IEC 61511-2

Edition 2.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

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

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.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 61511-2

Edition 2.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 13.110; 25.040.01

ISBN 978-2-8322-3227-9

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD....9
INTRODUCTION....11
1 Scope....13
2 Normative references....13
3 Terms, definitions, and abbreviations....13
Annex A (informative) Guidance for IEC 61511-1....14
A.1 Scope....14
A.2 Normative references....14
A.3 Terms, definitions and abbreviations....14
A.4 Conformance to the IEC 61511-1:–....14
A.5 Management of functional safety....14
A.5.1 Objective....14
A.5.2 Guidance to "Requirements"....14
A.6 Safety life-cycle requirements....23
A.6.1 Objectives....23
A.6.2 Guidance to "Requirements"....23
A.6.3 Guidance to "Application program SIS safety life-cycle requirements"....24
A.7 Verification....25
A.7.1 Objective....25
A.7.2 Guidance to "Requirements"....25
A.8 Process hazard and risk assessment (H&RA)....27
A.8.1 Objectives....27
A.8.2 Guidance to “Requirements"....27
A.9 Allocation of safety functions to protection layers....30
A.9.1 Objective....30
A.9.2 Guidance to "Requirements of the allocation process"....30
A.9.3 Guidance to "Requirements on the basic process control system as a protection layer"....32
A.9.4 Guidance to "Requirements for preventing common cause, common mode and dependent failures"....35
A.10 SIS safety requirements specification....36
A.10.1 Objective....36
A.10.2 Guidance to "General requirements"....36
A.10.3 Guidance to "SIS safety requirements"....36
A.11 SIS design and engineering....40
A.11.1 Objective....40
A.11.2 Guidance to "General requirements"....40
A.11.3 Guidance to "Requirements for system behaviour on detection of a fault"....47
A.11.4 Guidance to “Hardware fault tolerance"....47
A.11.5 Guidance to "Requirements for selection of devices"....50
A.11.6 Field devices....53
A.11.7 Interfaces....53
A.11.8 Guidance to "Maintenance or testing design requirements"....55
A.11.9 Guidance to "Quantification of random failure"....56
A.12 SIS application program development....62

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

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

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

G.4 Predictability of mathematical or logical result 190
G.5 Robustness 191
G.5.1 General 191
G.5.2 Controlling use of diversity 191
G.5.3 Controlling use of exception handling 192
G.5.4 Checking input and output 193
G.6 Traceability 194
G.6.1 General 194
G.6.2 Controlling use of built-in functions 194
G.6.3 Controlling use of compiled libraries 194
G.7 Maintainability 194
G.7.1 General 194
G.7.2 Readability 195
G.7.3 Data abstraction 198
G.7.4 Functional cohesiveness 199
G.7.5 Malleability 199
G.7.6 Portability 199
Bibliography 201

Figure 1 – Overall framework of IEC 61511 series 12
Figure A.1 – Application program V-Model 25
Figure A.2 – Independence of a BPCS protection layer and an initiating source in the BPCS 34
Figure A.3 – Independence of two protection layers allocated to the BPCS 35
Figure A.4 – Relationship of system, SIS hardware, and SIS application program 39
Figure A.5 – Illustration of uncertainties on a reliability parameter 60
Figure A.6 – Illustration of the 70 % confidence upper bound 61
Figure A.7 – Typical probabilistic distribution of target results from Monte Carlo simulation 62
Figure B.1 – Process flow diagram for SIF 02.01 83
Figure B.2 – Process flow diagram for SIF 06.02 84
Figure B.3 – Functional specification of SIF02.01 and SIF 06.02 85
Figure B.4 – SIF 02.01 hardware functional architecture 85
Figure B.5 – SIF 06.02 hardware functional architecture 86
Figure B.6 – Hardware specification for SOV extracted from piping and instrumentation diagram 86
Figure B.7 – SIF 02.01 hardware physical architecture 87
Figure B.8 – SIF 06.02 hardware physical architecture 87
Figure B.9 – Hierarchical structure of model integration 91
Figure B.10 – Hierarchical structure of model integration including models of safety properties and of BPCS logic 93
Figure B.11 – State transition diagram 94
Figure B.12 – SOV typical block diagram 95
Figure B.13 – SOV typical model block diagram 96
Figure B.14 – Typical model block diagram implementation – BPCS part 98
Figure B.15 – SOV application program typical model implementation – SIS part 99

Figure B.16 – Complete model for final implementation model checking 101
Figure D.1 – Example of P&ID for an oil and gas separator 104
Figure D.2 – Example of (part of) an ESD cause & effect diagram (C&E) 105
Figure D.3 – Example of (part of) an application program in a safety PLC function block programming 106
Figure F.1 – Simplified flow diagram: the PVC process 112
Figure F.2 – SIS safety life-cycle phases and FSA stages 114
Figure F.3 – Example of the preliminary P&ID for PVC reactor unit 123
Figure F.4 – SIF S-1 Bubble diagram showing the PFD_{avg} of each SIS device 139
Figure F.5 – S-1 Fault tree 140
Figure F.6 – SIF S-2 Bubble diagram showing the PFD_{avg} of each SIS device 141
Figure F.7 – SIF S-2 fault tree 142
Figure F.8 – SIF S-3 Bubble diagram showing the PFD_{avg} of each SIS device 143
Figure F.9 – SIF S-3 fault tree 144
Figure F.10 – P&ID for PVC reactor unit SIF 145
Figure F.11 – Legend *(1 of 5)* 146
Figure F.12 – SIS for the VCM reactor 160

Table B.1 – Modes of operation specification 88
Table B.2 – State transition table 93
Table F.1 – SIS safety life-cycle overview 115
Table F.2 – SIS safety life-cycle – Box 1 117
Table F.3 – Some physical properties of vinyl chloride 119
Table F.4 – What-If/Checklist 125
Table F.5 – HAZOP 126
Table F.6 – Partial summary of hazard assessment for SIF strategy development 127
Table F.7 – SIS safety life-cycle – Box 2 129
Table F.8 – Tolerable risk ranking 131
Table F.9 – VCM reactor example: LOPA based integrity level 132
Table F.10 – SIS safety life-cycle – Box 3 133
Table F.11 – Safety instrumented functions and SILs 133
Table F.12 – Functional relationship of I/O for the SIF(s) 134
Table F.13 – SIS sensors, normal operating range & trip points 134
Table F.14 – Cause and effect diagram 137
Table F.15 – MTTFd figures of SIS F.1 devices 138
Table F.16 – SIS safety life-cycle – Box 4 151
Table F.17 – SIS safety life-cycle – Box 5 162
Table F.18 – List of instrument types and testing procedures used 166
Table F.19 – Interlock check procedure bypass/simulation check sheet 178
Table F.20 – SIS safety life-cycle – Box 6 178
Table F.21 – SIS trip log 179
Table F.22 – SIS device failure log 179
Table F.23 – SIS safety life-cycle – Box 7 181

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61511-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

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

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

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

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

A list of all parts in the IEC 61511 series, published under the general title *Functional safety – Safety instrumented systems for the process industry sector*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

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

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

The SIS logic solvers addressed include Electrical (E)/Electronic (E)/ and Programmable Electronic (PE) technology. Where other technologies are used for logic solvers, the basic principles of this standard can be applied to ensure the functional safety requirements were met. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series has been developed as a process sector implementation of the IEC 61508 series. The IEC 61511 series is process industry specific within the framework of the IEC 61508 series.

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used. The objective of this part of IEC 61511 is to provide guidance on how to comply with IEC 61511-1:2016.

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

In most situations, safety is best achieved by an inherently safe process design whenever practicable, combined, if necessary, with a number of protective systems which rely on different technologies (e.g., chemical, mechanical, hydraulic, pneumatic, electrical, electronic, thermodynamic (e.g., flame arrestors), programmable electronic) which manage any residual identified risk. Any safety strategy considers each individual SIS in the context of the other protective systems. To facilitate this approach, IEC 61511-1:2016:

- requires that a H&RA is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety functions and related safety systems, such as the SIS(s), is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.
- addresses relevant SIS safety life-cycle stages from initial concept, through design, implementation, operation and maintenance and decommissioning;
- enables existing or new country specific process industry standards to be harmonized with this standard.

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

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

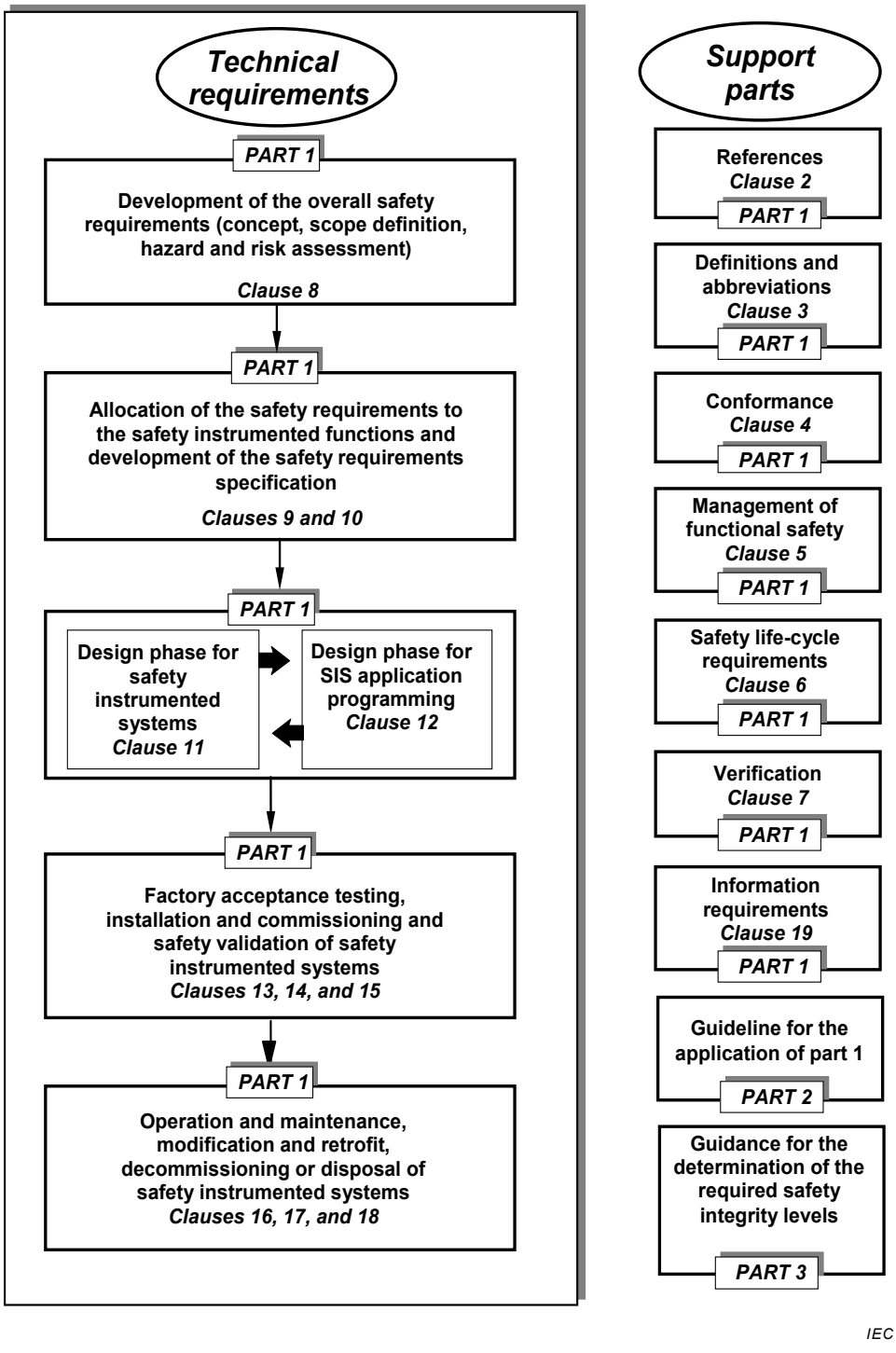


Figure 1 – Overall framework of IEC 61511 series

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

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

1 Scope

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

NOTE 1 Annex A (informative) has been organized so that each clause and subclause number therein addresses the corresponding clause and subclause number in IEC 61511-1:2016 except for being preceded by “A”.

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

NOTE 3 To achieve maximum use of this guideline;

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

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

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

2 Normative references

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

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

3 Terms, definitions, and abbreviations

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

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.

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).

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”. Devices of a SIS may be used by more than one SIF.

A.4 Conformance to the IEC 61511-1:–

No further guidance provided.

A.5 Management of functional safety

A.5.1 Objective

No further guidance provided.

A.5.2 Guidance to "Requirements"

A.5.2.1 General

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 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 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 61511-1:2016does not endorse any particular methodology. 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.

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 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 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 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 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) 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 from the project team is to increase objectivity in the assessment. The need for someone of senior stature (e.g., experience, position) 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;
- 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 and revision

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:

- inspections;
- safety visits (e.g., plant walk about and incident review);
- SIS surveys (via questionnaires).

A distinction 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 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.

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 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, 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:
   - 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 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 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 Subclauses 5.2.6.3, 5.2.6.4 and 5.2.6.5 of IEC 61511-1:2016 reinforce 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.

A.5.2.7 SIS configuration management

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 part of the AP which together constitute a specific version of a complete 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 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;
- 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.

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).

See examples of techniques and measures in A.12.6.2.

A.6.3.3 No further guidance provided.

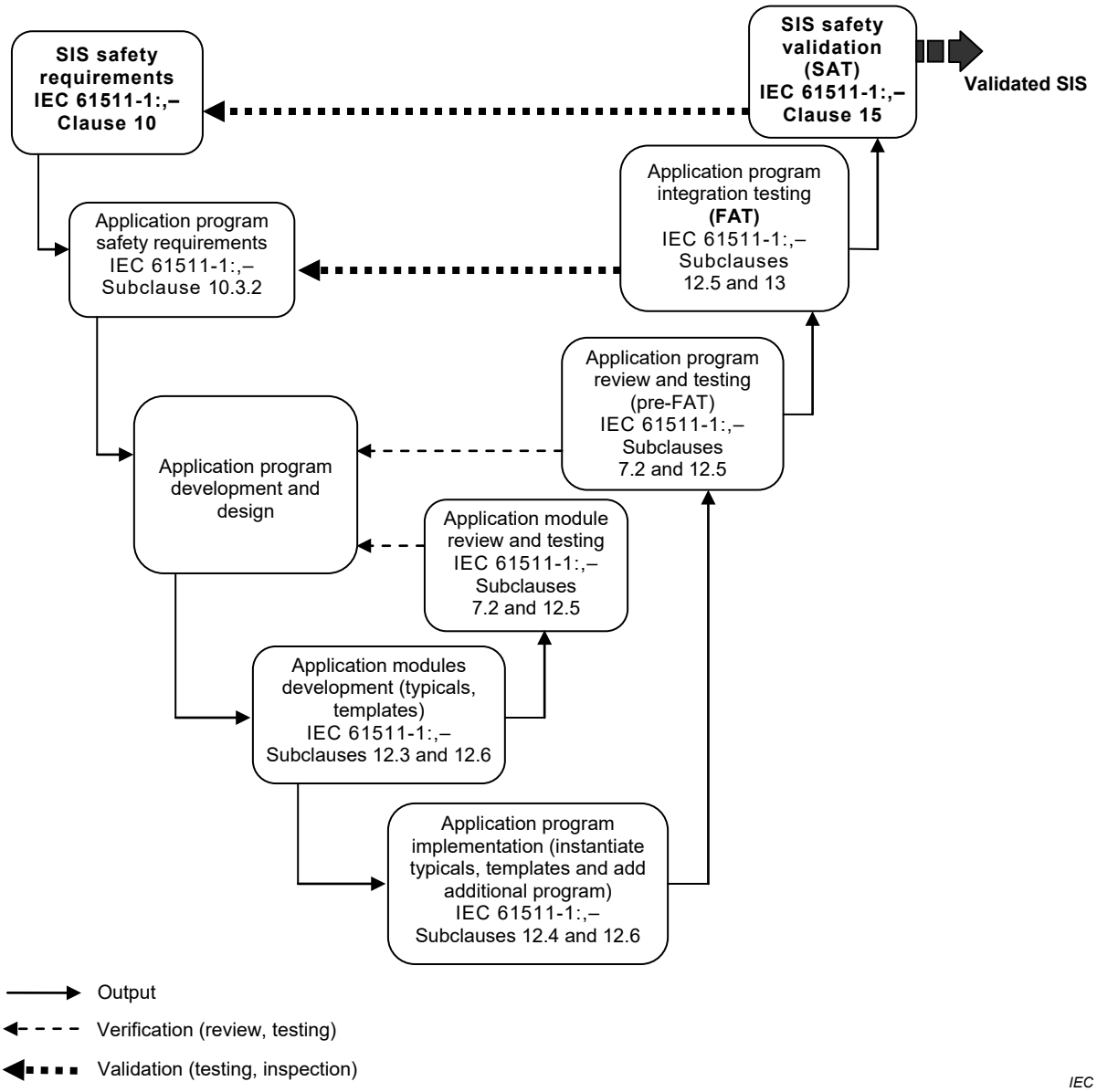


Figure A.1 – Application program V-Model

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 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 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.

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 and associated 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 protection layers so that failure of a single layer will not lead to or allow a harmful consequence. Typical 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. 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 target failure measures.

A H&RA should identify and address the 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 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 hazardous events may be introduced as detailed design proceeds. A final H&RA may therefore be necessary once the 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 protection layers as designed are adequate to manage the risks of the plant. During this final analysis it is necessary to consider whether failures of the protection layers (or successful activations of protection layers) introduce any new hazardous events or demands. If any new hazardous events are established at this stage, it may be necessary to define new safety functions. Another more likely outcome is that additional causes are identified that lead to 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 target failure measure requirements that were determined in the original analysis is needed.

The approach used to identify 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 rigorous approach may be necessary (e.g., 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 hazardous event, all possible outcomes, and the frequency of the hazardous event as it contributes to each outcome, should be considered. No credible outcome should be ignored or discarded. 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 should be consulted. They 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 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 hazardous event may occur during start-up when staff are 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.

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 should be made on when operator errors are to be included as initiating causes of the identified hazardous events and the frequency to be used for such events. Care is also needed where credit is taken for reduction in demand frequency due to operator action. The credit is limited by human factor issues such as how quickly action can be taken and the complexity of the tasks involved. 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 abnormal situation. It should be noted that a risk reduction of ≤ 10 might be claimed without the need to comply with IEC 61511. Where such claims are made, the human factor issues 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 means of risk reduction by reducing the demand rate on the SIS, 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 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 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 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;

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, 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 SIF and specify its associated safety integrity requirements, it is important to consider the planned (or installed) protection layers and how much risk reduction they provide. If a SIS protection layer is needed, a determination should be made on the SILs of each SIF allocated to the SIS.

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

A.9.2.1 The requirement is to identify the protection layers to be used and to allocate risk reduction to the SIF. In practice, safety functions are 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 instrumented systems rather than more traditional approaches such as relief valves 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 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 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 low demand mode or high demand/continuous mode. 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 an increasing number of applications operating in high demand mode where it is more appropriate to consider the application as continuous mode because the 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 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} 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 average frequency of dangerous failures to perform the SIF. This 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 SIL requirements.

The targets for average probability of failure on demand or frequency of dangerous failures 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 association with a specific SIF. However, 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 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 should be done to ensure that 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 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 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).

A.9.2.5 No further guidance provided.

A.9.2.6 Multiple SIFs may be utilized in order to achieve higher levels of risk reduction (e.g., greater than 10^3). When using multiple SIFs to achieve higher risk reduction, it is important that each of the SIFs is independently able to carry out the safety function and that there is sufficient independence between the SISs.

Furthermore, where multiple 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 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 SIF with a PFD_{avg} of $3{,}05 \times 10^{-4}$. This SIF achieves a risk reduction of approx. $3{,}3 \times 10^{3}$.

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 is also 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 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.

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:—.

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.

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.

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 ≤ 10 may be claimed from 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 BPCS protection layers to the requirements of IEC 61511-1:2016.

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 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.

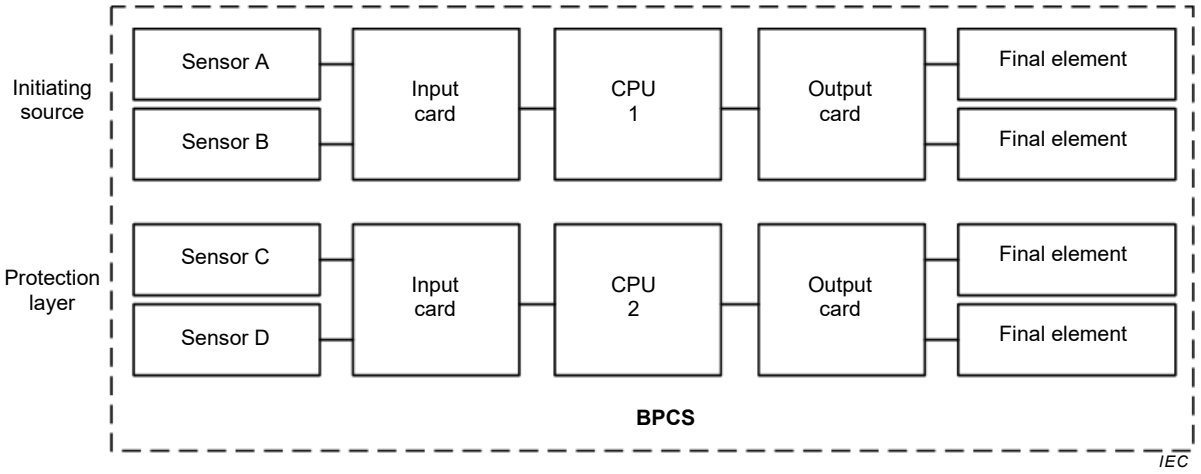


Figure A.2 – Independence of a BPCS protection layer and an initiating source in the BPCS

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.

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 $\times$ $\leq 10^{-1}$ = $\leq 10^{-6}$/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., $\leq 1/10 \times \leq 1/10 = \leq 1/100$). 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.

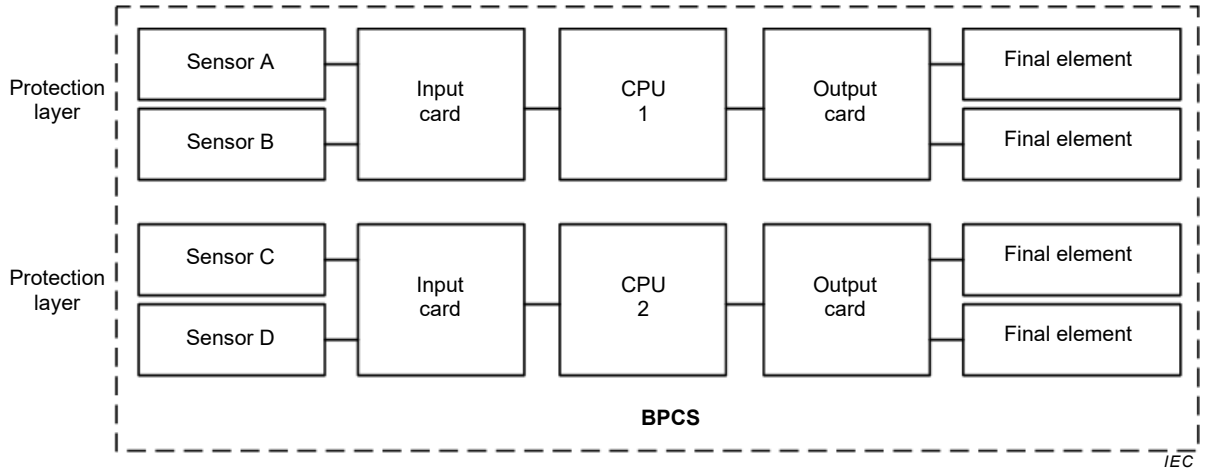


Figure A.3 – Independence of two protection layers allocated to the BPCS

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.

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.

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 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. 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"

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 should be defined early in a project to ensure the SIF provides the desired protection.

Some considerations with respect to the SRSs are as follows:

a) The first items that 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 topics:

   - Which process parameters should be monitored to detect the hazardous conditions.

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

   - The actions that should be taken and when they should be taken to prevent the hazardous 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 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 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 can also be identified. In defining the final elements, consideration 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 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;
   - 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 should be specified. Any requirement for independence of manual shutdown switches from the SIS logic solver also should be defined.

e) All requirements for restarting the process after a shutdown 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 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 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 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 corrective actions. 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 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.

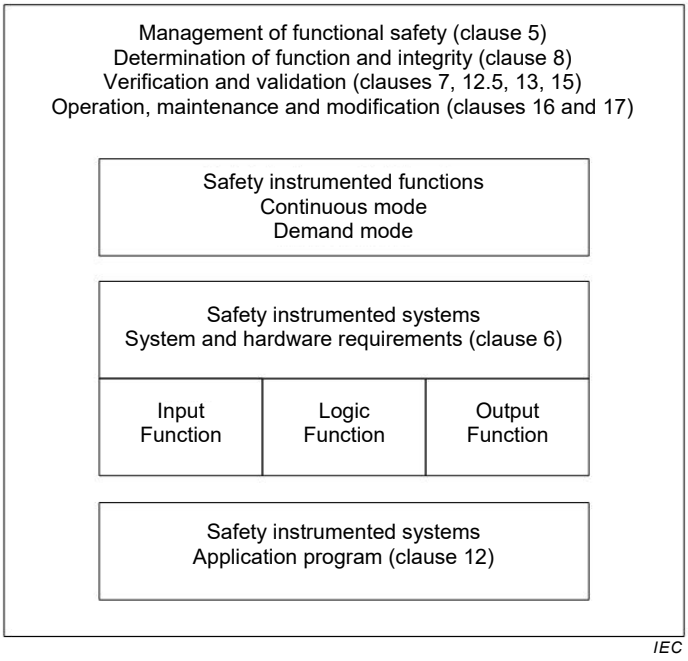


Figure A.4 – Relationship of system, SIS hardware, and SIS application program

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.

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 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 For AP guidance see A.12.2.4. .

A.11.2.3 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 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 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 affecting multiple channels at the same time and/or from the same cause and hence reduces correlated failure of multiple channels.

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 devices are to be selected which 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 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.

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 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.

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 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.

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

Similar to the sensors, using a single 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.

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 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 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 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.

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

- 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 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 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.

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 should be given to adding fire protection to the cable trays in fire risk areas.

A.11.2.5 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 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 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 (2009), ISBN 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 hazard that may be created if a SIS automatically restarts the process immediately after the trip condition is corrected. Each SIF 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 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.

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.

A.11.2.10 IEC 61511-1:2016 provides cautionary guidelines on using a common device for both the BPCS and the SIS. "Sufficiently low" in the note to 11.2.10 in IEC 61511-1:2016 means the dangerous failure rate of the shared equipment combined with the probability of failures of other protection layers (other than the SIF) meets corporate risk criteria.

A.11.2.11 In the case of final elements which on loss of power do not fail to the safe state (e.g., energize to trip systems) consideration should be given to the provision of local manual means to achieve the safe state.

A.11.2.12 No further guidance provided.

A.11.2.13 The purpose of the safety manual is to document all the necessary information related to how a device, SIS subsystem, or system can be safely applied.

NOTE 1 The safety manual is intended to cover information from the manufacturer as well as from the end user, and may be sectioned as appropriate, e.g., into hardware, firmware and AP.

NOTE 2 For IEC 61508 compliant items the manufacturer's input is the safety manual per the requirements of IEC 61508-2:2010, Annex D.

The safety manual should include, but not be limited to, the following information:

a) A brief description of the item and its topology (schematics), including hardware and software;

   NOTE 3 Any reduction or increase in the hardware fault tolerance according to IEC 61511-1:201611.4.4 can be justified in the safety manual.

b) Identification of revision and the constraints related to the AP;

   NOTE 4 Clause 12 in IEC 61511-1:– can be reviewed for more details on relevant information related to application programming.

c) Identification of hardware and firmware revisions;

d) Operational description, including the definition of the safe state, and the fail-safe operation;

   NOTE 5 Different modes of operation can be considered, such as start-up, normal operation, degraded operation, and demand mode.

e) List of all assumptions in relation to operations, maintenance, and testing;

   NOTE 6 Assumptions can include use conditions, preventive maintenance, how to perform proof testing, and follow-up of diagnostic faults.

f) List of all limitations and restrictions related to the safety function(s) of the item;

NOTE 7 Limitations and restrictions include, but not be limited to, configuration setting, environmental and process limitations.

g) Failure modes and the corresponding failure rates of the device(s);

NOTE 8 The failure rates can come from the manufacturer or from field experience.

h) Other parameters that are needed for reliability analyses such as useful lifetime, repair times, and if applicable, common cause failure rates;

i) Response(s) to or behavior in response to detected faults and warnings;

j) Manufacturer operating and maintenance instructions, and if applicable, recommendations to proof test intervals;

k) Measures taken to avoid and control systematic failures including software failures and, if applicable, common cause failures;

l) Information about how each failure mode may be revealed by regular functional test and diagnostics, including the diagnostic test interval;

m) The safety manual should include the restrictions on the use of the device, which include details related to its configuration, interfaces, installation, diagnostics, mean time to repair, fault response, and testing interval and AP language constraints.

A.11.2.14 No further guidance provided.

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

A.11.3.1 No further guidance provided.

A.11.3.2 No further guidance provided.

A.11.4 Guidance to “Hardware fault tolerance"

A.11.4.1 The traditional approach to safety system design is to ensure that no single fault would result in loss of intended function. System architectures such as 1oo2 or 2oo3 have a fault tolerance of 1 because they are able to function on demand even in the presence of one dangerous fault. Such systems are employed as a standard approach for safety systems to ensure they were sufficiently robust to be able to withstand random hardware failures. Fault tolerant architectures also provide protection to the range of systematic faults which do not arise at the same instant of time (mainly in hardware).

IEC 61511-1:2016 recognizes that the process industry needs more than one level of performance from safety systems and has adopted the concept of safety integrity levels with increasing performance depending on the required risk reduction for the specific hazardous event. Because of the different levels of performance it is no longer appropriate to expect all safety integrity levels to be fault tolerant. In selecting the architecture to use for a specified integrity level it is however important to ensure that it is sufficiently robust for both random hardware faults and systematic faults. To ensure robustness against random hardware faults this standard requires that a reliability analysis be carried out.

The requirements of 11.4.1 of IEC 61511-1:2016 are targeted at ensuring that architectures have the necessary fault tolerance for random hardware faults and some systematic faults. In deciding the extent of fault tolerance needed there are a number of factors that should be taken into consideration as follows:

a) the complexity of the devices used within the SIS or SIS subsystem;

b) a device will be less likely to suffer from systematic faults during operation if the nature of its faults are understood and taken into account in the selecting of the device, installing and configuring the device, and defining its operation and maintenance practices;

c) the failure data from field experience;

d) the safety integrity level requirement for the application involved;

e) the extent to which faults lead to a safe condition or can be detected by diagnostics so that a specified action can be taken;

f) the spurious actions due to safe failures which generally increase when the fault tolerance increases and which may, in turn, create a new hazard or be an additional cause for an existing hazard or may become unacceptable with regard to the target spurious failure frequency;

g) the common cause failures and the systematic failures which may drastically reduce the benefit expected from the fault tolerance;

h) the fault tolerance really achieved which may be reduced to none when the restoration of the dangerous failures takes too much time (e.g., a 2oo3 whose faults are not corrected in less than 0,8 MTTF is worse than a 1oo1 architecture);

i) the feasibility of the redundancy which may not be practicable for all functions;

j) the various SIFs in which the SIS (or its subsystems) is involved.

NOTE 1 The SIS subsystems can be required to operate under low or high demand depending on the operating mode. A SIF can be specified to close a valve in response to specified process deviations. Whether manual or automatic reset, the SIS can maintain the valve in the safe state until it is commanded to do otherwise. The hardware fault tolerance requirements for the SIS's operation in response to a hazardous event can be determined according to the low demand mode and its operation while in shutdown according to high demand mode.

NOTE 2 The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in SIF design that can result due to the number of assumptions made in the design of the SIF, along with uncertainty in the failure rate of devices used in various process applications.

A.11.4.2 A good understanding of the concept of SIS subsystem (see IEC 61511-1:2016, 3.2.78) is necessary to apply hardware fault tolerance requirements.

The requirements for hardware fault tolerance apply to the whole SIS or to the SIS subsystems required to perform a SIF, not to individual devices within a subsystem. For example, in the case of a sensor SIS subsystem comprising a number of redundant sensors, the fault tolerance requirement applies to the sensor SIS subsystem in total, not to individual sensors.

A.11.4.3 The IEC 61508 considered the factors described in 11.4.1 above and specified the extent of fault tolerance required in IEC 61508-2:2010 by the use of two different routes called 1_H and 2_H. In preparing this sector-specific standard for the process sector it was considered that route 2_H was better adapted for process sector. Therefore the requirements for fault tolerance in IEC 61511-1:2016 are based on IEC 61508-2:2010 route 2_H. The IEC 61508-2:2010 route 1_H could be applied as an alternative. It should be noted that SIS subsystem designs may require more device redundancy than what is stated in IEC 61511-1:2016 Table 6 in order to satisfy process availability requirements (e.g., spurious failure frequency target).

A route 1_H assessment for IEC 61511 compliance should take into account the intended operating environment. For field devices, the operating environment often has significant impact on the demonstrated failure rate, which may also effect the distribution of safe and dangerous failures.

A.11.4.4 The fault tolerance can be provided by non-identical redundant devices (e.g., when diversified redundancy is implemented). The hardware fault tolerance of a SIS is actually given by the shortest combination of independent device faults leading to an overall dangerous fault of this SIS. If the SIS has been split into independent SIS subsystems, its hardware fault tolerance is equal to the minimum value of the hardware fault tolerance of its SIS subsystems.

The hardware fault tolerance requirements may be relaxed while the SIS is being repaired on-line. However, the key parameters relating to any relaxation should have been previously evaluated (e.g., MTTR or test duration compared to the probability of a demand during repair or tests). This has to be included in the calculation of the probability measurements (PFD_{avg}, PFH) related to the SIL claim.

Depending on the selected architecture, the reduction in hardware fault tolerance may result in an increased risk of the hazardous event. The risk of continuing operation with a known fault should be assessed to determine the need for compensating measures.

Certain single failures/faults may be excluded when they clearly have a very low probability by virtue of properties inherent to design and construction (see 3.2 of IEC 61511-1:2016): that is, the contribution to the target failure measure of the sum of the dangerous failures of serial devices, on which fault exclusion is being claimed, should not exceed 1 %. Any such failure/fault exclusions should be justified and documented. Then, it would not normally be considered necessary to constrain (on the basis of hardware fault tolerance) the safety integrity of any SIF bearing those single failures/faults.

NOTE 1 In the case of field wiring, it is common to assume that the field device data includes the field wiring from the field device to the termination, because the field wiring has a much lower dangerous undetected failure rate than the field device. In general, hardware fault tolerance is provided for the wiring only when hardware fault tolerance is needed for the field device. With other forms of signal communication, it can be necessary to determine the hardware fault tolerance for the signal transmission means separately due to a higher dangerous undetected failure rate in the operating environment. For these forms of communication, the signal communication means can require more hardware fault tolerance than required for the field device.

NOTE 2 The devices of the system that perform unique functions that are not typically required for the SIS to operate successfully (e.g., operator interfaces, engineering stations, maintenance management systems, and data recorders) which have a low likelihood of impacting the ability of the SIS to operate as required, are not typically considered in the analysis.

When certain faults can be excluded (according to the criteria noted above) then the minimum HFT may be reduced (see 11.4.6 of IEC 61511-1:2016).

A.11.4.5 Table 6 of IEC 61511-1:2016 defines the minimum fault tolerance for SISs or SISs' subsystems. The fault tolerance requirement depends on the required SIL of the SIF being implemented by the SIS. In establishing the hardware fault tolerance it is acceptable to assume that the SISs or SIS subsystem has been properly selected for the application and is adequately installed, commissioned and maintained such that early life failures and age related failure may be excluded from the assessment. Human factors may be excluded when determining hardware fault tolerance.

A.11.4.6 Fault tolerance is the preferred solution to gain the required confidence that a robust architecture has been achieved. When IEC 61511-1:2016, 11.4.6 applies, the purpose of the justification is to demonstrate that the proposed alternative architecture with reduced hardware fault tolerance provides an equivalent or better solution (e.g., with the use of other verifiable means such as certification or similar). It should provide evidence that:

a) compliance with the hardware fault tolerance requirements specified in IEC 61511-1:2016, 11.4.5 might introduce additional failures that would lead to a decrease in the overall safety; and

b) if the hardware fault tolerance is reduced to zero, the failure modes identified in the SIS performing the SIF may be excluded because the dangerous failure rate(s) of the identified failure mode(s) are very low compared to the target failure measure for the SIF under consideration.

NOTE 1 Examples to implement reduced hardware fault tolerance include: back-up arrangements (e.g., analytical redundancy (replacing a failed sensor output by physical calculation results from other sensors outputs); using more reliable items of the same technology (if available); changing for a more reliable technology; decreasing common cause failure impact by using diverse technology; increasing the design margins; constraining the environmental conditions (e.g., for electronic components); decreasing the reliability uncertainty by gathering more field feedback or expert judgment, etc.

NOTE 2 Hardware fault tolerance is only effective when there is a high probability to detect and repair the failure of one part before the failure of the other redundant parts. When dealing with systems in remote or hostile locations (e.g., subsea SIS) where maintenance is difficult (if not completely impossible) the benefit of hardware fault tolerance is reduced and, in these situations, the design of SIS can be failure robust, i.e., rely on the intrinsic components reliability rather than on hardware fault tolerance.

NOTE 3 The overall process safety may be reduced if an additional industrial combination full voltage motor starter (i.e., combination fused switch and contactor with control transformer and pilot relay, also providing overload and short circuit protection used for connecting and disconnecting power to three phase reversing or non-

reversing motor) is installed for fault tolerance reasons. This is due to the increase of the number of components when utilizing multiple motor starters versus a single motor starter resulting in more:

- spurious trips;
- complexity of design (e.g., overload and short circuit protection coordination) and difficulties to get a full knowledge about the behavior and the failure modes of redundant motor starters:
- maintenance, inspection and testing;
- exposure to high voltage;
- phase to phase fault due to lack of synchronization (typically caused by wiring error) between multiple combination full voltage motor starters;
- exposure to electrical arcs;
- re-starts required.

Further justification for the use of a single industrial combination full voltage motor starter in lieu of redundancy is provided by the following considerations:

- the failure modes of all components are well defined;
- the behavior of the motor starter under fault conditions can be determined;
- industrial manual starters or industrial combination full voltage motor starters do not rely on software to perform their specified function;
- there is sufficient dependable failure data to show that the claimed failure rates for detected and undetected dangerous failures allow quantification of random hardware failure;
- the low MTTFdu value of industrial combination full voltage motor starters;
- the use of quantitative procedures to verify that the use of a single industrial combination full voltage motor starter is justified.

A.11.4.7 No further guidance provided.

A.11.4.8 No further guidance provided.

A.11.4.9 No further guidance provided.

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

A.11.5.1 Objectives

No further guidance provided.

A.11.5.2 Guidance to "General requirements"

Considerations when migrating from non-programmable technologies to PE technologies are given in Annex C.

A.11.5.2.1 There are some considerations for selecting devices and subsystems to be used in a SIS. The first option is that the devices be designed in accordance with IEC 61508-2:2010 (requirements for electrical/electronic/programmable electronic safety-related systems) and IEC 61508-3:2010 (software requirements). The second option is to use devices and SIS subsystems that are known to be reliable through extensive use in similar service and in a similar environment during its useful lifetime. The useful lifetime is the period of time, in which the failure rate of a device is extensively constant. The probabilistic calculation of the overall PFD_{avg} of the SIS (which should satisfy the SIL requirement for each SIF implemented by the SIS) is based on these failure rates. After the end of the useful lifetime the failure rates can rise gradually, e.g., by aging.

Whichever option is chosen, it has to be demonstrated that the device or SIS subsystem:

a) is reliable enough to achieve the overall target PFD_{avg} or target dangerous failure rate of the SIF;
b) meets the architectural constraint requirement;
c) has a sufficiently low likelihood of systematic faults;

d) in case of electrical devices, that they have an appropriate failure rate or are based on prior use.

The requirement of c) can be satisfied either by compliance with IEC 61508-2:2010 and IEC 61508-3:2010 or are based on prior use requirements in IEC 61511-1:2016, 11.5.3.

A practical approach for the selection of devices used in safety applications is to use a combination of evidence of compliance with IEC 61508-2:2010 and IEC 61508-3:2010 and operational experience. This approach ensures that the devices selected are designed, manufactured, and managed for safety applications and operate successfully in the intended application (e.g., application induced failures are accounted for).

Procedures for demonstrating that a device complies with IEC 61508-2:2010 and IEC 61508-3:2010 do not include consideration of potential dangerous failure modes of the process interfaces, installation, power supplies, or communication interfaces, may not include the full device boundary and are sometimes restricted to the E/E/PE portion of the device. Failures associated with the process interfaces are very prominent in sensors, including plugged process lines, frozen lines, corrosion and gas permeation, and in valves, including seat damage, plugging, deposition, and corrosion (including stem buildup). For this reason, devices developed according IEC 61508-2:2010 and IEC 61508-3:2010 should be evaluated to ensure that the device operates in its intended applications. This may include the gathering of prior use information or simulated testing of statistical samples.

When selecting devices, the user also should consider how to protect against systematic failure. For a device developed according to IEC 61508-2:2010 and IEC 61508-3:2010 there are a large number of techniques and measures that should be implemented by the manufacturer during the development of the device to reduce the potential for systematic failures. On the other hand, prior use history based on significant documented experience with a given product in a given application can be used to demonstrate that there are sufficiently low dangerous systematic failures concerning the intended application and therefore adequate protection against them.

A.11.5.2.2 No further guidance provided.

A.11.5.3 Guidance to "Requirements for the selection of devices based on prior use"

A.11.5.3.1 Many users have devices that are approved for use in their facility. Sensors and valves that have had a history of not performing as desired have been eliminated as approved devices.

The assessment of these devices should include considerations of the version of the device and be supported by documented monitoring of field performance. In addition, the manufacturer should have a modification process which evaluates the impact of reported failures and modifications.

ISA TR84.00.04:2015, and NAMUR recommendation NE130 (“Prior use”-devices for SISs”) give guidance how to qualify field devices, how to keep them under the control of management of change and how to observe and document their performance. The results can be collected in a device approval form.

If such a form does not exist, then users and designers should conduct an assessment on the sensors and valves to ensure that they are satisfied and the device will perform as desired. This may require discussions with other users or designers to see what they are using for similar applications.

A.11.5.3.2 It should be noted that for more complex devices, it may become more difficult to show that the experience gained in an application is relevant. As an example, experience gained by using a PLC in an application involving the use of simple ladder logic may not be relevant if the equipment was to be used for complex calculations or sequences.

In general, the relevant aspects of the operating profile of field devices are different from those of a logic solver.

For field devices the following points contribute to the operating profile:

- functionality (e.g., measurement, action);
- operating range;
- process properties (e.g., properties of chemicals, temperature, pressure); and
- process connection.

For logic solvers, the following points contribute to the operating profile:

- version and architecture of hardware;
- version and configuration of embedded software;
- AP;
- I/O configuration;
- response time; and
- process demand rate.

For all devices, the following points contribute to the operating profile:

- EMC; and
- environmental conditions.

A.11.5.3.3 No further guidance provided.

A.11.5.4 Guidance to "Requirements for selection of FPL programmable devices (e.g., field devices) based on prior use"

A.11.5.4.1 No further guidance provided.

A.11.4.4.2 No further guidance provided.

A.11.5.4.3 No further guidance provided.

A.11.5.4.4 Explains additional requirements when trying to qualify a FPL programmable device to a SIL 3 capability.

A.11.5.5 Guidance to "Requirements for selection of LVL programmable devices (e.g., logic solvers) based on prior use"

A.11.5.5.1 No further guidance provided.

A.11.5.5.2 No further guidance provided.

A.11.5.5.3 No further guidance provided.

A.11.5.5.4 No further guidance provided.

A.11.5.5.5 No further guidance provided.

A.11.5.5.6 No further guidance provided.

A.11.5.6 Guidance to "Requirements for selection of FVL programmable devices (e.g., logic solvers)"

No further guidance provided.

A.11.6 Field devices

A.11.6.1 No further guidance provided.

A.11.6.2 No further guidance provided.

A.11.6.3 No further guidance provided.

A.11.7 Interfaces

A.11.7.1 Guidance to "General"

User interfaces to a SIS are operator interfaces and maintenance/engineering interfaces. The information or data which is communicated between the SIS and the operator displays can be either SIS related or informative.

If an operator action is part of the SIF, everything needed to perform this action should be considered as part of the SIF. This would include, for example, an alarm indicating that the operator has to shutdown the process. In this example, the shutdown switch (the means of implementing the shutdown action) should be considered as part of the SIF.

Data communication which is not part of the SIF (e.g., display of the actual value of a SIF sensor if the trip function is realised within the SIF) may be displayed in the BPCS if it can be shown that the SIF are not compromised (e.g., read-only-access in the BPCS).

A.11.7.2 Guidance to "Operator interface requirements"

The operator interfaces used to communicate information between the operator and the SIS may include:

– displays;
– panels containing lamps, push buttons, and switches;
– annunciator (visual and audible);
– printers (should not be the sole method of communication);
– any combination of these.

a) video displays

   BPCS video displays may share SIS and BPCS functions provided the displayed data is for information only. Safety critical information is additionally displayed via the SIS (e.g., if the operator is part of the safety function).

   When operator action is needed during emergency conditions, the update and refresh rates of the operator display should be carried out in accordance with the SRS.

   Video displays relating to the SIS should be clearly identified as such, avoiding ambiguity or potential for operator confusion in an emergency situation.

   The BPCS operator interface may be used to provide automatic event logging of SIF and BPCS alarming functions.

   Conditions to be logged might include the following:

   – SIS events (such as trip and pre-trip occurrences);
   – whenever the SIS is accessed for program changes;
   – diagnostics (e.g., discrepancies, etc.).

It is important that the operator be alerted to the bypass of any portion of the SIS via an alarm and/or operating procedure. For example, bypassing the final element in a SIS (e.g., shutoff valve) could be detected via limit switches on the bypass valve that turn on an alarm on the panel board or by installing seals or mechanical locks on the bypass valve that are managed via operating procedures. It is generally suggested to keep these bypass alarms separate from the BPCS.

b) panels

Panels should be located to give operators easy access. The location of any panels should be considered in regard to the areas affected by any potential hazards.

Panels should be arranged to ensure that the layout of the push buttons, lamps, gauges, and other information is not confusing to the operator. Shutdown switches for different process units or equipment, which look the same and are grouped together, may result in the wrong equipment being shut down by an operator under stress in an emergency situation. The shutdown switches should be physically separated and their function labelled. Means should be provided to test all lamps.

c) printers and logging

Printers connected to the SIS should not compromise the SIF if the printer fails, is turned off, is disconnected, runs out of paper or behaves abnormally.

Printers are useful to record the sequence in which events occur, diagnostics and other events and alarms, with time and date stamping and identification by tag number. Report formatting utilities should be provided.

If printing is a buffered function (information is stored, then printed on demand or on a timed schedule), then the buffer should be sized so that information is not lost, and under no circumstances should SIS functionality be compromised due to filled buffer memory space.

The operator should be given enough information on one display to rapidly convey critical information. Display consistency is important and the methods, alarm conventions and display devices used should be consistent with the BPCS displays.

Display layout is also important. Layouts with a large amount of information on one display should be avoided since they may lead to operators misreading data and taking wrong actions. Colours, flashing indicators, and judicious data spacing should be used to guide the operator to important information so as to reduce the possibility of confusion. Messages should be clear, concise and unambiguous.

The display should be designed such that data can be recognized by colour blind operators. For example, conditions shown by red or green colours could also be shown by filled or unfilled graphics.

A.11.7.2.1 No further guidance provided.

A.11.7.2.2 No further guidance provided.

A.11.7.2.3 No further guidance provided.

A.11.7.2.4 No further guidance provided.

A.11.7.2.5 No further guidance provided.

A.11.7.2.6 No further guidance provided.

A.11.7.2.7 No further guidance provided.

A.11.7.3 Guidance to "Maintenance/engineering interface requirements"

A.11.7.3.1 No further guidance provided.

A.11.7.3.2 No further guidance provided.

A.11.7.3.3 Maintenance/engineering interfaces consist of means to program, test and maintain the SIS. Interfaces are devices which are used for functions such as:

a) system hardware configuration;

b) AP development, documentation, and downloading to the SIS logic solver;

c) access to AP for changes, testing, and monitoring;

d) viewing SIS system resource and diagnostic information;

e) changing SIS security levels and access to AP variables.

Maintenance/engineering interfaces should be capable of displaying the operating and diagnostic status of all SIS devices (e.g., input/output modules, processors) including the communication between them.

Maintenance/engineering should provide means for copying APs to storage backup media.

A personal computer connected to a SIS for maintenance/engineering purposes, should not compromise safety functions if the personal computer fails, is turned off or is disconnected.

A.11.7.3.4 No further guidance provided.

A.11.7.4 Guidance to "Communication interface requirements"

A.11.7.4.1 It is acceptable for the two interfaces to look the same as long as the maintenance/engineering interface cannot be used to manipulate the process. The maintenance/engineering software should not be used as the operator interface.

A.11.7.4.2 No further guidance provided.

A.11.7.4.3 No further guidance provided.

A.11.7.4.4 No further guidance provided.

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

A.11.8.1 The design of the SIS should take into consideration, how the system is going to be maintained and tested. If the SIS is to be tested while the process is running, the design should not require the disconnection of wires, applying jumpers or forcing software registers (e.g., inputs, outputs) since using these techniques may jeopardize the integrity of the SIS. The system design should address the technical and procedural requirements for testing of the SIS in order to accomplish full system testing of sensors, logic solvers and final elements safely.

It is important to define how a SIS is going to be maintained while the process is running. For example, if a transmitter or valve should be worked on, consideration should be given on how the maintenance department will work on these instruments without causing a nuisance trip while maintaining the safety of the process.

It should be noted that any limit on the testing period of final elements should be taken into account in the calculation of the PFD_{avg} of the SIF.

A.11.8.2 No further guidance provided.

A.11.8.3 Bypasses may reduce the level of safety in a SIS. This reduction in safety may be overcome by:

- using passwords and/or key locked switches. Some designs may incorporate locked cabinets containing the appropriate bypasses;
- clear identification of piping bypasses may be accomplished by either sealing valve positions or installing safety signs indicating importance of the appropriate position;
- clear procedures or facilities (e.g. master bypass removal switch) for the control of bypass application and removal;
- using bypasses that have a time limiting function that will automatically remove the bypass – such a feature reduces the risk of bypasses being left active on completion of testing or maintenance.

For example, for a 1oo2 sensor configuration, some users like to bypass both sensors at one time but others like to have a separate bypass for each sensor. If both sensors are bypassed, it will be necessary to put measures in place to ensure that risk remains tolerable. Either can be possible, but this should be addressed early in the design.

Likewise, some process operations do not support the valve being moved while the process is running or installing a bypass around the valve may be impractical. In these cases, the design should allow for testing the SIS as far as practical, i.e., at least through the solenoid valve. In this case, some type of bypass around the solenoid can be included in the design with the usual alarming or procedural controls for this bypass.

A.11.8.4 Timers may be provided within the SIS, that limit the duration of the by-pass, e.g. by automatic reset and/or alarm to operator; logic may be provided in the SIS that automatically allows reset of any inhibits or overrides, e.g. lack of pressure during pump start up.

A.11.8.5 No further guidance.

A.11.8.6 Forcing of inputs and outputs in PE SIS should not be used as part of the AP. For example uncontrolled forcing of inputs and outputs through on-line editing of the memory within the logic solver using a programmers tool whilst the program is running is frequently used during program development to explore proposed modifications to the AP. However, this practice should not be used on-line as it will mask the ‘’real’’ input status of variables from the plant and/or feed false outputs to plant devices. In either event, the logic solver will not be controlling the plant in the predicted fashion. Moreover, such small modifications to the application programme can easily be overlooked, remaining in the program when no longer required.

A.11.9 Guidance to "Quantification of random failure"

A.11.9.1 Users and designers should refer to IEC 61511-3: –, Annex J; IEC 61508-6:2010, Annex B; ISO 12489; ISA TR84.00.02:2002; IEC 61508-3:2010, Annex B; IEC 61025 (Fault trees); IEC 61078 (Reliability block diagrams); IEC 61165 (Markov graphs); IEC 62551(Petri nets); IEC 62502 (Event trees) for guidance in techniques available to ensure SIS design satisfies performance relating to random hardware failures.

During proof tests intervals, the probability of a dangerous failure on demand, PFD(t), increases continuously when the time elapses. Therefore after it has crossed its average value it will remain consistently above it until the end of the proof test interval. In some cases it may even cross the upper SIL boundary corresponding to this average value and remain consistently above it. Therefore when high safety integrity is required the average values alone may give a false sense of safety and verification should be made, e.g., verification that the risk corresponding to the peak values is consistent with the risk criteria of the user organisation.

A SIF acting on demand mode of operation (e.g., closure of a valve to prevent an overpressure) is often immediately followed by another SIF implying the same components but acting in continuous mode of operation (e.g., preventing the opening of the valve as long as the overpressure is present upstream the valve). Therefore for SIF acting on demand mode of operation, the hazard frequency associated with failure of the SIS not retaining the process in a safe state should be considered.

A.11.9.2 The estimated failure rates can be determined by a quantified failure-mode analysis of the design by using failure data from a recognized industry source or from experience of the previous use in the same environment as for the intended application. For the sake of conservativeness, the 70 % upper confidence limit of input data may be used in calculations.

It has to be noted that the overall undetected failure rate of fault tolerant items are time dependent and increase during proof test intervals. Fault tolerant items may have time dependant failure rates.

EXAMPLE An item made of two similar components A and B with the same undetected failure rate λ, has an overall undetected failure rate A which increases from 0 to λ when the time increases.

When quantifying the effect of random hardware failures of a SIS (or of its SIS subsystem), having a hardware fault tolerance of 0, and which is implementing a SIF operating in high demand mode or continuous mode, credit should only be taken for diagnostics if:

- the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or
- in high demand mode, the ratio of the diagnostic test frequency to the demand frequency equals or exceeds 100.

The proof test procedure and the reliability analysis of the proof test facilities includes, for example:

- the durations of the proof tests;
- the state of the process (running or stopped) during proof tests;
- the state of the tested device during the proof tests (on line or off line); if the tested device is off line (i.e., unavailable) during proof tests this may be an important contributor to its PFD_{avg};
- the proof test coverage when the proof tests are not 100 % effective. This implies the identification of the failures which, inherently, can never be detected by proof tests;
- the failure which may be caused by the proof tests themselves (e.g., failure due to the change of state needed for testing purpose);
- the possible staggering of the proof tests for similar redundant devices in order to de-correlate the proof tests;
- the possibility for the proof test to return an incorrect result about the health of the SIS:
  - proof test affected by a fault associated with the proof test itself;
  - the human error during proof tests (e.g., no detection of an actual failure, omission of a test, proof tested or repaired device remaining off line after proof test or repair completion, etc.).

If the proof test interval is not explicitly modelled for the probabilistic calculation, then the MTTR of individual detected dangerous failures can be calculated as half the proof test interval plus the MRT of the considered failure.

Most of the techniques in A.11.9.1 require some quantification of the diagnostic coverage of the SIS. Diagnostics are tests performed automatically to detect faults in the SIS that may result in safe or dangerous failures.

A particular diagnostic technique cannot usually detect all possible faults. An estimate of the effectiveness of the diagnostics used may be provided for the set of faults being addressed (see Annex C of IEC 61508-2:2010 and Annex C of IEC 61508-6:2010 for examples of how diagnostic coverage is calculated).

Improving the diagnostic coverage of the SIS may assist in satisfying the SIL requirements. In this case, both the diagnostic coverage and the period between diagnostic tests (the diagnostic test interval) should be taken into account when calculating the probability of failure (demand mode) or frequency of failure (continuous mode) of the SIS. For further guidance, refer to IEC 61508-2:2010, Annex C or ISA TR84.00.02:2015.

In situations where the SIS is the only layer of protection and is used for a safety function operating in the continuous mode of operation, then the diagnostic test interval should be such that faults in the SIS are detected in time to ensure the integrity of the SIS and to allow action to be taken to ensure a safe state in the event of a failure occurring in the process or the basic process control system.

To achieve this, the sum of the diagnostic test interval and the reaction time to achieve a safe state should be less than the “process safety time”. According to 3.2.52.1 in IEC 61511-1:2016, the process safety time is defined as the time period between a failure occurring in the process or the BPCS (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed.

Critical and potentially critical faults to common devices (such as faults to CPU/RAM/ROM) typically inhibit nearly the entire processing of data and are therefore more far reaching than a fault of a single output point. Failure modes that carry a high failure probability have to be detected with more confidence. Furthermore, the detectability of failure modes should be taken into account.

For each diagnostic implemented, testing interval and resulting action on fault detection should meet the SRS.

Where these diagnostics are not “built in” the vendor supplied equipment, externally configured diagnostics may be implemented at the system or application level in order to meet the SIL for the SIF.

Diagnostics may not be capable of detecting systematic errors (such as software bugs). However, appropriate precautionary measures to detect possible systematic faults may be implemented.

Diagnostics may be accomplished using a variety of, or a combination of, methods including:

a) Sensors
   1) Diagnostic alarms could be provided to detect a sensor that has completely failed upscale or downscale. One way this can be accomplished is by use of an out of range alarm. For example, in a high temperature trip application with redundant temperature sensors, a low out of range alarm could be added to diagnose a sensor failure or loss of sensor signal.
   2) If redundant sensors are used, comparison of the analogue values detects anomalies that may occur during normal operation. If three sensors are used, the middle of the three readings can be used (mid-value selection – see note below). Significant deviations between readings may be created by:
      – plugging or freezing in the impulse leads;
      – reduction in purge supply pressure;
      – process coating of thermowells;
      – grounding or power supply problems;

– non-response of a sensor transmitter that has an output value that is no longer changing.

NOTE 1 Mid value selection is advantageous over comparison to the average because the average is skewed by the device that is not functioning properly. Nevertheless mid-value selection does not work if two transmitters are giving false readings and so common-mode failures can be considered.

3) If either “2)” is applied or comparison is made between analogue sensors in the SIS and comparable process parameter readings by other sensors in systems such as BPCS then the potential improvement of the diagnostic coverage will depend on specific applications and has to be analyzed, evaluated and documented. If a diagnostic coverage higher than 90 % is claimed then the sources of common cause failures (CCF) between collaborate sensors should be analyzed and documented.

NOTE 2 To take credit for comparison any discrepancy can, at least, automatically generate an alarm. Such discrepancy alarm threshold can be set according to a documented deviation of the related process variable. Such comparisons detect both the failure of the SIS sensors and of the non-SIS sensors. Then, false alarms or spurious trips generated by non-SIS sensors failures can be analyzed before implementing such a solution.

NOTE 3 The improvement of diagnostic coverage provided by this type of comparison can be used to increase the proof test interval.

4) Time delays may be provided to prevent nuisance alarms due to variations in sensor response to process changes caused by sensor location or sensor technology. For example, some redundant flow sensors may have 1 to 2 s delays. There are a number of software packages available from vendors to monitor redundant sensor readings and calculate the standard deviation in order to initiate the diagnostic alarms.

5) Another method of sensor diagnostics is comparison of related variables (e.g., flow totalizers versus tank level changes or pressure and temperature relationship).

b) Final elements

1) Comparison of the feedback from the final element (such as limit switches or position transmitters) to the requested state may be performed to verify that the expected actions have been taken. Sufficient time delays should be used to filter the alarm for valves in transition (e.g., from fully opened to fully closed). This comparison of the feedback from the final element to the requested state can only be considered to be a diagnostic if the valve periodically changes to the safe state as part of normal operation (e.g., batching operation).

2) Some valves, actuators, solenoids, and/or positioners may provide diagnostic capability.

c) Logic solvers

Safety-configured or IEC 61508 series compliant PE logic solvers typically include diagnostics which detect various faults. The types and diagnostic coverage will generally be described in the safety manual.

d) Externally configured diagnostics

Examples of these include watchdog timers and end-of-line monitors.

The confidence in the reliability data used to perform the target measure calculations should also be taken under consideration. Using the 70 % upper confidence bounds of the input reliability parameters ensure to perform conservative calculations and this is discussed in 11.9.4 of IEC 61511-1:2016.

A.11.9.3 No further guidance provided.

A.11.9.4 The reliability data values used when quantifying the effect of random hardware failures are always only known with numerical uncertainties. Therefore assessing the impact of these uncertainties on the target measures is useful to consolidate the SIL claims.

The uncertainty (see Note 1) of a given reliability parameter (e.g., failure rate) can be evaluated by:

a) statistical analysis,

b) the exercise of expert judgment and, where needed,

c) the undertaking of specific tests.

As a general law the numerical uncertainties decrease when the amount of available field feedback increases.

Therefore a reliability parameter is not a perfectly known deterministic value but a random variable with a distribution more or less scattered around its mean value as illustrated in Figure A.5.

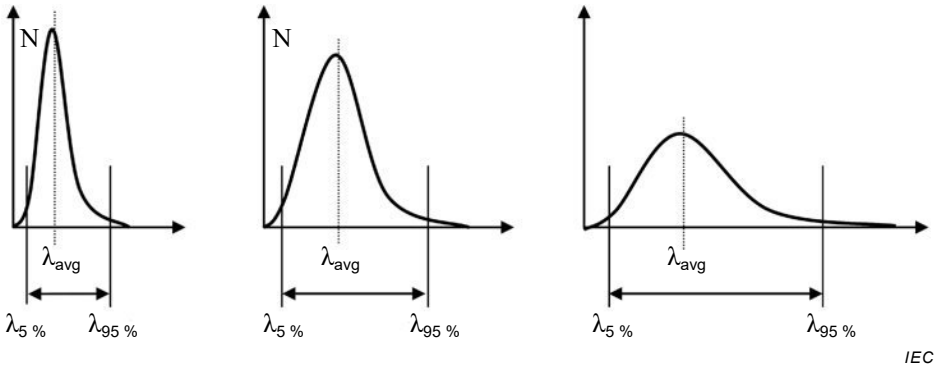


Figure A.5 – Illustration of uncertainties on a reliability parameter

The sharper the distribution, the less uncertain is the parameter. The uncertainty increases from the left to the right in Figure A.5.

At the limit, if the parameter was perfectly known the curve would be a simple vertical straight line (i.e., a Dirac distribution).

As illustrated in Figure A.5 the uncertainty of a reliability parameter λ can be evaluated by its confidence interval at, e.g., 90 %: the actual average value of λ has a probability of 90 % to belong to the interval [$\lambda_{5\ \%}$, $\lambda_{95\ \%}$] where λ has a probability of 5 % to be better than $\lambda_{5\ \%}$ and a probability of 5 % to be worse than $\lambda_{95\ \%}$.

On a pure statistical basis, the average of a reliability parameter can be estimated by using the "maximum likelihood estimate" and the confidence bounds [$\lambda_{5\ \%}$, $\lambda_{95\ \%}$] be calculated by using the χ^2 (Chi-square) function which is tabulated in statistical books.

A sample of n failures observed over a cumulated observation time T provides an average equal to n/T and a 90 % confidence interval equal to $[\frac{1}{2T}\chi^2_{0,95,2n}, \frac{1}{2T}\chi^2_{0,05,2(n+1)}]$. The width of this interval squeezes, i.e., the accuracy improves, when the cumulated observation time and/or the number of observed failures increase (from the right to the left in Figure A.5).

The Bayesian approach may also be used to handle statistical observations, expert judgement and specific test results. This can be used to fit relevant probabilistic distribution functions for further use in Monte-Carlo simulation.

When the confidence interval is wide (i.e., in the case of sparse field feedback) a reliability data collection process should be implemented as soon as possible and the probabilistic predictions of the target probabilistic measures should be periodically updated by using the collected reliability data.

NOTE 1 The IEC 61511 standard involves probabilistic calculations which need accurate reliability data to be performed. It cannot be properly implemented without reliability data collection from users. When a lack of

reliability data is identified, it is an opportunity to launch a specific reliability data collection to fill this gap. If it is not useful for the present SIS, it will be useful for the next one.

The first approach to handle the uncertainty described above is to use pessimistic input reliability data. This ensures that, in spite of the lack of accuracy, the evaluation of the target measure (PFD_{avg} or PFH) is not optimistic. This can be done by using for the input reliability parameters some confidence upper bounds higher than the conventional average values. The use of 70 % upper bounds (e.g., $\lambda_{70\ \%} > \lambda_{avg}$) is generally considered to provide a reasonable confidence level. This is illustrated in Figure A.6 which shows that the conservativeness of input data decreases when the accuracy increases (the difference $\lambda_{70\ \%} - \lambda_{avg}$ decreases).

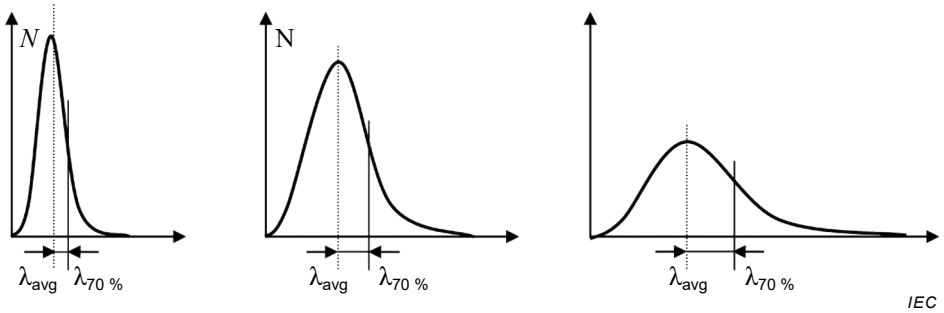


Figure A.6 – Illustration of the 70 % confidence upper bound

NOTE 2 From a sample of n failures observed over a cumulated observation time T the confidence upper bound can be calculated by using the χ^2 function: For example $\lambda_{70\ \%}$ can be evaluated by $\lambda_{0,7} = \frac{1}{2T}\chi^2_{0,3,2(n+1)}$ and there are 70 % chances that the actual value is lower (i.e., better) than that. This confidence upper bound exists even when no failure has been observed. It is always pessimistic compared to λ_{avg} but it is less and less pessimistic when T and/or n increase (see Figure A.6).

NOTE 3 The calculations performed with the 70 % confidence upper bounds of input parameters do not provide the 70 % confidence upper bound of the overall result (e.g., PFD_{avg}). Calculations done in this way only ensure that the result is conservative.

The previous approach implies only one calculation of the probabilistic target (i.e., PFD_{avg}) but the level of conservativeness is not known. Therefore another approach may be used if this level of conservativeness has to be known. This consists in using the whole distributions of the input reliability parameters instead of only single values like $\lambda_{70\ \%}$. The so-called "Monte Carlo" simulation can be used for doing that:

a) using random numbers to simulate the probabilistic distributions of the values of the input reliability parameters; and

b) achieving several (e.g., 100) calculations of the probabilistic target which different sets of random numbers.

This provides a statistical sample (i.e., a histogram) of the target result (e.g., PFD_{avg}) which may be processed to obtain the corresponding probabilistic distribution and the corresponding average and confidence levels (see Figure A.7).

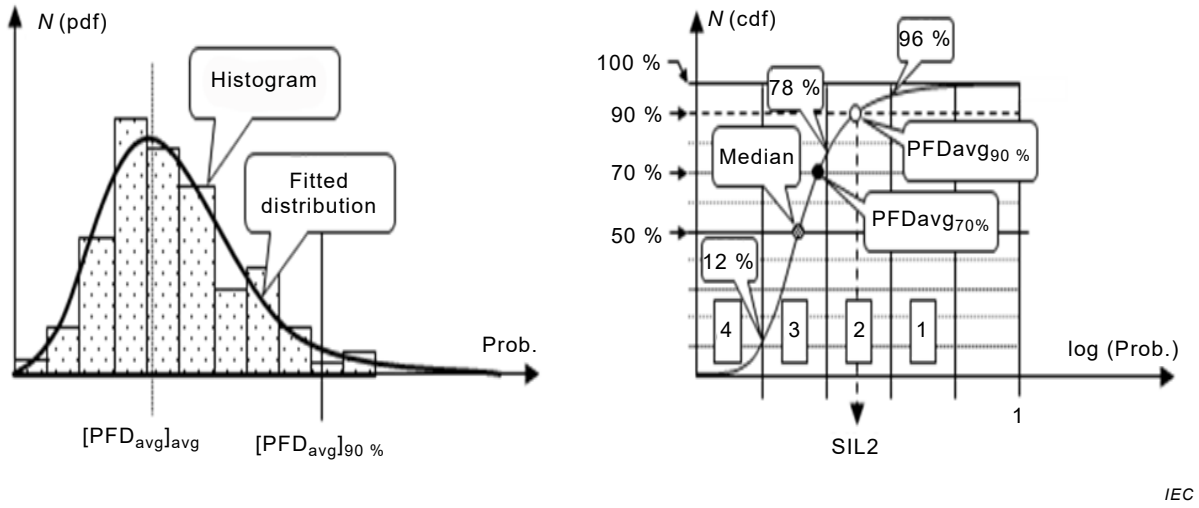


Figure A.7 – Typical probabilistic distribution of target results from Monte Carlo simulation

Figure A.7 illustrates the probabilistic density function (pdf) and the corresponding cumulative distribution function (cdf) which can be obtained from a Monte Carlo simulation. This shows the distribution of PFD_{avg} around its average value $[PFD_{avg}]_{avg}$.

NOTE 4 PFD_{avg} is a random variable in itself because of the underlying probabilistic laws used to make the calculations. The above calculation provides only the distribution intrinsically due to the uncertainties of the input reliability parameters.

$[PFD_{avg}]_{avg.}$ can be used instead of the classical PFD_{avg} but its conservativeness cannot be proven. It is likely to be close to the median value (i.e., 50 % chances that the actual value is better than (PFD_{avg}) 50 % and 50 % that the actual value is worse).

The cdf curve in Figure A.7 shows that PFD_{avg} has 12 % chances to be in the range related to SIL 4 (88 % chances to be in the range of SIL 3 or worse), 78 % chances to be in the range of SIL 3 or better (22 % chance to be in the range of SIL 2 or worse), 96 % chances to be in the range of SIL 2 or better (4 % chance to be in the range of SIL 1 or worse), etc.

For the sake of conservativeness a 90 % confidence level may be chosen. As $[PFD_{avg}]_{90\ \%}$ lies within the SIL 2 bounds this leads to SIL 2 for this example. Note that with a 70 % confidence level the same example give SIL 3.

A.11.9.5 No further guidance provided.

A.12 SIS application program development

A.12.1 Objective

See Clauses B.1 and F.20 for example(s) of how to define the development of an AP for one or several SIFs in a SIS.

A.12.2 Guidance to "General requirements"

A.12.2.1 Clause 12 in IEC 61511-1:2016 is suitable for the development and modification of APs with requirements of up to SIL 3. Experience shows that there is little difference in the development methods SIL 1, SIL 2 or SIL 3 when using LVLs in an IEC 61511-1:2016 compliant logic solver in accordance with the corresponding safety manual.

There may be differences between SIL 1, SIL 2 and SIL 3 for test and verification techniques for different SILs. See A.7.2.2.

A.12.2.2 For example, the application programmer should review the information in the logic description (e.g., Clauses F.15 and F.17) versus the sequence instructions as part of the process to detect deficiencies and to ensure the application programmer understands the intended requirement.

A.12.2.3 This standard is limited to the requirements for APs developed using LVL "AP development" is interpreted as the design and implementation of the application safety logic using a PE selected according to IEC 61511-1:2016, 11.5.

A.12.2.4 This standard also addresses the application of devices using Fixed Program Languages (FPL), for example control over the inputting of parameters in smart sensors – see for example Annex C and Table F.13.

A.12.2.5 Separate areas of the AP should be used for non-safety and SIF.

One way to demonstrate adequate independence could be to comply with all of the following:

a) SIF in the AP are clearly labelled as SIF application code;

b) non SIF in the AP are clearly separated;

c) all variables used in the implementation of SIF are labelled;

d) all AP implementing non-safety-instrumented functions are labelled as non-safety instrumented function code;

e) all AP using non safety variables and SIF variables meet the following conditions:

f) the non safety AP (including all functions and function blocks) do not write into any SIF variables used in the safety AP; and

g) the safety AP does not depend on any non safety variables in the implementation of SIF.

h) all safety AP (including variables and data) is protected against any non-safety AP changes; and

i) if safety and non-safety AP share the same resources (e.g., CPU, operating system resources, memory, buses), then the SIF (e.g., response time) of the safety AP is never compromised.

A.12.2.6 See guidance on A.11.2.8. If the AP does not include a manual reset then this should be identified in the SRS.

Addresses the hazard that may be created if a SIS loses power and on power restoration fails to maintain the process safe state. See also A.11.2.8 and 12.2.5 in IEC 61511-1:2016. In the case of energise to trip see also IEC 61511-1:2016, 11.6.2.

A.12.2.7 No further guidance provided.

A.12.2.8 Helps to minimize AP complexity and ensures all inputs and outputs are addressed on every scan. See also ISA TR84.00.09. It also helps to ensure response time requirements are achieved – see IEC 61511-1:2016, 10.3.2.

A.12.2.9 Ensures the appropriate AP is in use. Consideration should be given to secure storage and retrieval as well as to the length of time for which old versions should be stored, taking into account operational and regulation requirements. Consideration should also be given to retaining hardware and embedded software necessary to run old versions of the AP. Prior to implementing any modification to the AP it should be verified that the AP running in the machine is identical to the master copy. Prior to restoration of user data it should be verified that the user data is the appropriate version. See 5.2.7.

A.12.2.10 No further guidance provided.

A.12.3 Guidance to "Application program design"

A.12.3.1 Operating modes may include operating functions such as manual, semi-automatic, automatic, start-up, batch, test, and maintenance. See Clauses F.14 and F.27.

A.12.3.2 For examples of the inputs to the AP design see Clause F.13. For an example of the SRS for the SIS see step F.3. Example of the methods and tools for developing the AP design is in Clause F.20 and step F.3.

There may be a need to discuss the inputs to the AP design between the application programmer and the SIS designers.

A.12.3.3 In order to facilitate the FSA the AP should be traceable back to the specification of the safety requirements of the SIS. For example it should be structured in such a way that it shows how the SIF(s) are implemented and identifiers should reflect the practical installation – by using ‘’real world’’ input/output tag names. The AP should also be annotated to reflect the process functions. See also 5.2.6 of IEC 61511-1:2016 and the examples in Figure F.11. The AP design should describe the device and SIS subsystems of the AP, how they are interconnected, and how the required attributes, particularly safety integrity, are achieved. Examples of AP devices include application functions which are replicated throughout the program (e.g., pump control sequences), information interchange with the plant I/O and the communication modules, any AP level functions that interact with the underlying PE devices (e.g., use of multiple SIS to achieve redundant functions and/or behavior on error detection, and/or start up / shut down sequences).

Conducting a FSA of the AP will help to identify errors at an earlier stage, as well as to ensure the AP is robust to failure. FSA of an AP may include:

a) confirmation that the AP complies with the safety manual constraints and any specific application coding standards and safe programming practices;

b) failure analysis of the AP behavior; this involves identification of the functions carried out by the AP, their potential functional deviations (e.g. as in a chemical HAZOP – too large/small, too early/late, opposite/not present/none etc.), assessment of the effect of failure of each application function and identification of any mitigations that protect against functional failure.

NOTE Many AP functions are SIFs and the failure analysis may be carried out as part of the system failure analysis; however additional functions may have been identified in the AP, or may be identified during the functional failure analysis itself, to protect against failure of the SIF (e.g. control of pumps, voting on process inputs such as fire and gas voting or temperature and pressure voting, action to be taken on failure).

A.12.3.4 Examples of the techniques for application programme design are given below:

a) See Figure F.11, sheet 4, line 1.

b) See AP examples in Clause F.20 (Table F.8 through F.14 inclusive); the AP structure should be consistent with the structure of the process. (E.g., in a chemical plant the AP for each process unit should be grouped together and within each process unit separation is provided between equipment for ease of understanding and maintenance);

c) The proper execution order of the networks and logic should be defined both within each program and also the execution sequence and desired execution rates of all the APs. The execution rates of the APs should be confirmed to be consistent with the required process response times from the AP SRS;

d) Examples of description of standard library modules can be found in Figure F.11, sheet 1;

e) Examples of description of specific library modules can be found in B.4.1; any custom functions and function blocks should be developed and designed; custom designed function blocks are desirable since repetitive operations can be programmed, tested and used repeatedly; I/O modules and memory variable data areas should be configured;

f) Memory allocation is typically done automatically when performing application programming in PLCs; memory allocation is achieved by partitioning various parts of the AP (e.g., alarms, inputs, outputs, safety logic, non-safety logic, blank spaces for future growth) into their own individual ladders rungs – see Figure F.11 for an example; if partitioning has to be done manually, care should be taken in memory management by:

   – distributing equivalent variables in dedicated pages in order not to mix constants with variables, inputs with outputs, physical variables with intermediate variables;

   – segregating variable types in order not to e.g. mix real with integer with binary;

   – avoiding multiplexing simple variable types in more complex variable types, such as nesting several binary variables in integers or in bytes, by adhering to the rule of one memory address per variable;

g) An example of an application global variable could be a safety alarm such as a high temperature alarm that is changed depending on the batch constituents under process; another example could be a high combustible gas alarm limit used in fire and gas protection systems – for example, 20 % lower explosion limit (LEL); an example of integrity protection could be the functionality of the underlying logic solver which might constrain the global variable to being overwritten only by one AP instruction; additional considerations on the use of global variables can be found in G.3.4.3, G.3.4.4, G.7.2.4, G.7.3.1 and G.7.3.2;

h) It is desirable to separate the safety and non-safety functions into separate programs so that the emphasis can be placed on the safety programs and so that non-safety functions can be readily demonstrated not to interfere with safety functions; Figure B.13 provides an example of analysis of SIF vs non-SIF independence; the SRS should specify which SIF and other functions will be included within a given program; its also desirable to limit the size of the safety programs to a few functions so that the highest level of integrity need only be applied to the essential safety functions;

i) Figure F.11 sheets 1 and 2 provide an example input and output description; the tag names for all the I/O and memory variables should be developed;

j) Figures B.6 and B.12 provide examples SIS HMI specification;

k) The communication variables to systems peripheral to the SIS should be defined; if the variables are memory variables they will have to be assigned to appropriate data areas so they can be accessed by the SIS communication subsystem; variables that can be modified by other systems external to the SIS should be defined with care and are typically placed in a special read/write area of memory; Figure B.13 illustrates an example of data exchanges between SIS and BPCS;

l) The sensor and final element diagnostics and the periodic testing philosophy needs to be defined and will be dependent on the sensor and final element redundancy; the testing philosophy needs to be defined carefully and should include the appropriate alarming during the test period; Figure F.11 sheet 3 lines A1 to A6, sheet 4 lines 4, 6, 8 and 10, sheet 5 lines 17 to 20 are examples of implementation of diagnostics;

m) The handling and recording of alarms need to be addressed with care, together with their impact on risk reduction; further the approach to maintenance overrides needs to be identified; some users will require switches wired through digital input points to initiate maintenance override whereas others will use controlled data input to the SIS from a display station; in either case secure procedures are required to avoid unintended overrides/bypasses; see Figure F.11 sheet 3 for typical examples of an alarm diagram; see Clause F.14 and Table F.13 for alarm prioritization; see Figure F.11, sheet 2 lines DI1, DI2, and DI3 for typical examples of operator interfaces;

n) Examples of application data integrity checking and sensor validation include:

   – out of range I/O data checks, e.g., an out of range transmitter;

   – validation of application communications data, e.g., external watchdog timer, external cyclic redundancy check (CRC) algorithms; and

   – comparison of sensors values and deviation alarming;

o) System configuration checks can be carried out through structural testing (see 12.5.3 b for a detailed description of structural testing); in addition care is required to ensure tag names etc. are unique including between controllers;

p) One example of control of complexity is given in B.3.2.2.1 where the complexity of an AP is limited by using a hierarchical organization of three layers of modules (see also Figure B.9);

q) Figure F.11 sheet 3 lines D01, D02 and D03, sheet 4 lines 1 and 2 and sheet 5 lines 12 and 16 to 20 show an example of management of SIS and SIS sub-systems I/O faults;

r) An example of on-line test with automatic inhibition would be partial stroke testing of the physical output – see also A.16.3.1.2 and A.16.3.1.3;

s) Figures B.6 provides an example of interface to maintenance switches for off-line testing;

t) Modifications to the SIS should be done offline – the safety of the modification process usually relies on:

   – preventing on-line modification of the AP in the logic solver; this is normally achieved by inhibiting editing of the logic solver code through hardware switches and passwords;

   – preventing access to the AP download link;

   – the intrinsic characteristics of the AP workbench and its embedded safety features, including syntax control, consistency checks, traceability and version control;

u) The AP safety requirement specifications are usually contained in a document, or a set of documents, organized hierarchically in order to provide a progressive refinement of the requirements ranging from the SRS to the most detailed implementation specifications, such as memory mapping. The AP documentation provided by the logic solver is not an adequate SRS for the SIS.

A.12.3.5 Consideration for proper application programming design include:

a) See Clauses F.17 and F.27.

b) The implemented AP should realize all the functionalities described in the AP safety requirement specifications and all other non specified behaviors should be identified and should not impair the safety integrity.

c) See A.12.6 and Annex G for guidance to avoid ambiguity. The AP should be implemented in a way that assists the operators and maintainers to understand and interact with the SIS (where required). For example, the presentation of alarms, the response times required, operator workloads, etc. Functions should support the maintenance activities including the use of over-rides and bypasses.

d) See A.12.6 for guidance to achieve freedom from design faults.

A.12.4 Guidance to "Application program implementation"

A.12.4.1 Wherever possible, the AP should be based on well-proven AP modules that may include user library functions and well-defined rules for linking the AP modules (See B.4.3.3.1, B.4.3.3.2.1 and B.4.3.4.1, and Figure B.9). In Figure F.11, sheet 1 an example is given of a part of an AP using supplier provided and safety assessed library function blocks.

A.12.4.2 See the following references to illustrate how each requirement of Part 1 may be implemented.

NOTE Annex F is an example based on the second edition of IEC 61508 and IEC 61511.

a) the AP originator – bottom of Figure F.11 – title block;

b) a description of the purpose of the AP; Clauses F.1, F.2, F.3, F.4, as well as F.5.1 and F.5.2;

c) no further guidance provided;

d) no further guidance provided;

e) traceability to the AP SRS – Table F.12;

f) identification of each SIF and its SIL – Table F.11;

g) identification and description of the symbols used, including logic conventions, standard library functions, application library functions – Figure F.11, sheet 1;

h) for identification of the SIS logic solver input and output signals see Tables F.9 and F.10;

i) where the overall SIS utilizes communications, a description of the communications information flow – see Figure F.12;

j) a description of the program structure, including a description of the order of the logical processing of data with respect to the input/output SIS subsystems – see Clause B.1 – and for typical limitations imposed by scan times;

k) if required by the SIF specification, the means by which the correctness of field data and data sent over a communication link is ensured – see Figure F.11, sheet 5, lines 17, 18, 19, 20; and

l) for version identification and a history of changes, see bottom of each sheet in Figures F.4, F.5, F.6, F.7, F.8, F.9, F.10 and F.11.

A.12.4.3 The re-use of AP library functions should demonstrate the satisfactory operation in a similar application, including evidence that the same library functions have demonstrated satisfactory operation in similar conditions of use. An example of a previously developed AP library function utilized in many process facilities is an AP module that performs the start, stop, and seal-in functions found in a momentary 3-wire motor control function.

A.12.4.4 To build a robust and reliable AP some thought should be given to its structure. This could include the way in which application level redundancy is added to the underlying logic solver design, functions are shared between several I/O (such as valve control are structured) and the order of processing of input and output variables.

A.12.5 Guidance to "Requirements for application program verification (review and testing)"

A.12.5.1 No further guidance provided.

A.12.5.2 Competence in this context means that the person has a professional technical background and education (e.g. bachelor or master degree or equivalent), that he/she is familiar with the used program language and design and implementation tools, that he/she is an experienced application programmer. Further he/she should have knowledge on functional safety, especially for the process industry. He/she should be able to recognize inherently unsafe logic (e.g., OR-gates or inversions in De-energize to Safe state applications or AND-gates in Energize To Safe state applications). See Clause F.28.

A.12.5.3 During testing, all areas of the AP should be exercised to ensure correct operation and to ensure that one area of the application does not adversely interfere with another part of the program. Data should be checked throughout the fully allowed range to ensure that the system will operate correctly when in range. Out of range checks should also be carried out to ensure that out of range data is detected and the appropriate action is taken. Tests should also be carried out to confirm that the AP does not perform unintended functions that jeopardize its safety requirements.

AP review should include such techniques as inspections, walk-through, and formal analysis. It should be used in conjunction with simulation and testing to provide assurance that the AP satisfies its associated specification.

Testing may be ‘’black box’’ (testing conducted without knowledge of the internal structure of the AP) for example functional testing or ‘’white box’’ (testing using knowledge of the internal structure of the AP. In both cases it is important to demonstrate the test results against the requirements, but in the case of white box testing ‘’unexpected’’ behavior may be more readily identified.

AP testing may take place initially on a simulator and then on the logic solver hardware against the specifications produced in the design and requirements specification stages. The purpose of the initial testing phases (simulation and testing against the design specifications) is:

a) to demonstrate that the AP modules provided the necessary functionality and are incapable of any prohibited behavior;

b) to subject the AP to a wide range of conditions and sequences to show that it is resilient to unexpected behavior;

c) structural testing encompasses three critical phases of AP development and testing (unit, integration, and system levels of testing).

AP structural testing is meant to challenge the decisions made by the AP with test cases based on the structure and logic of the design. Complete structural testing exercises the AP's data structures (such as configuration tables, typicals, subroutines, functions) and its control and procedural logic at the test levels discussed below.

Structural testing should be done at the unit, integration, and system levels of testing. As used herein, a "unit" is the smallest separately compliable – or equivalent – device of code, such as a procedure, subroutine, class, method, or database table. Structural testing assures the AP's statements and decisions are fully exercised by code execution. For example, it confirms that AP loop constructs behave as expected at their data boundaries. For configurable AP, the integrity of the data in configuration tables is evaluated for their impact on program behavior. At the unit level, structural testing also includes the identification of "dead code," which is code that cannot be reached for execution by any code pathway.

Integration structural testing should be performed after all verification testing of the units involved and before system-level structural testing. AP verification confirms that the output of each phase of AP development is true to (i.e., is consistent with) the inputs to that phase. Performance testing confirms the final AP product, running in its intended hardware and environment, is consistent with the intended product as defined in the product specifications and AP requirements.

- Unit level structural testing

  The unit is compiled and linked with a driver and stubs, as needed. The driver is a substitute for any actual unit that will eventually call the unit-under-test, and if the driver passes data to the unit-under-test, it is set up to pass test case variable values such as maximum, minimum, and other nominal and "stress-test" values. The stubs are substitutes for any units called by the unit-under-test. As with the driver, if the stubs return data to the unit-under-test, they also pass "stress test" and nominal data values, as appropriate. The interface of the drivers and stubs, including their names, are the same as the true units' interfaces, allowing the set of units to be linked without altering the unit-under-test.

  Unit-level structural tests can be conducted on the actual target hardware, on an emulator or simulator of the actual hardware, or, if the situation requires, on a totally different processor. The latter case may occur, e.g., if the actual hardware has no provision for determining the results of a unit's tests, but where the code is written in a higher order language. Thus, the higher order AP can be compiled and linked to run on another logic solver that supports reading the test results where the target logic solver could not support the tests.

  Structural testing (a.k.a. white-box testing) is performed with the item-under-test, in this case the unit, being viewed internally for purposes of determining how the item should behave – for example, in determining all possible code branches. The primary purpose of unit-level structural testing is to verify the AP complies with the design, including logic, algorithms' correctness, and accuracy (versus parallel AP or hand calculations), and the correctness of the data's engineering units. This requires, for each unit, complete branch tests, complete AP tests (including verifying there is no dead code), and stress tests (to detect, e.g., overflow and underflow conditions as well as nominal and maximum loop-control data values). The detailed design is used to develop the acceptance criteria.

- Environment for integration-level and system-level structural tests

It is best to set up the integration and system structural tests using the actual hardware and environment to the extent practical. There are several reasons for this, but the two most significant are (a) the AP may have subtle conditions, both good and bad, that will only show up when running on the actual hardware, and (b) the final SIS, including the intended hardware and AP, should be validated running on that hardware, and the structural tests should advance the AP development towards that end. However, there are also good and sufficient reasons to perform structural tests partially or wholly in a simulated environment. In considering establishing simulation capabilities, the two most common configurations are to both emulate the logic solver and simulate the environment, or to simulate both the logic solver and the environment. The principal advantages, then, in using a simulation of the environment and, at times, the logic solver includes the following:

– the ability to set up absolutely known input values, such that the results can be predetermined to establish the acceptance criteria of each test;

– a simulator makes it easy to establish inputs that are over, under, and at the exact limits of critical data values;

– it is easy to set up illegal inputs to test all error and failure conditions;

– the results of each test can be readily seen.

- Integration level structural testing

  Integration structural testing combines functionally cohesive units of verified AP parts (which includes unit-level structurally tested AP parts) by compiling and/or assembling and linking these parts, along with any drivers and stubs needed. The structure is then loaded into the actual or simulated environment for execution. This allows the tester to focus on that one functional package to confirm its correct operation, including all internal and external interfaces. Following completion of each functional package's test, the next functional package may be either separately tested or added to (i.e., linked with) the previously tested package(s). Regression testing (i.e., running a selected subset of previous, successfully run test cases) should be performed on the previously tested packages to confirm they are not adversely affected by the newly introduced functional package.

- Incremental approach

  The incremental approach to integration-level structural tests is the best for AP developers (as opposed to third party, validation testers – see below), especially if the AP is large or complex. In this approach, selected small, functionally cohesive portions of the AP are compiled, linked, and tested. This approach is used regardless of the AP life-cycle development method, including any of the following three methods. In the waterfall method, all of the requirements are developed, then the design is completed, and, finally, selected "threads" are coded and structurally tested. In the spiral method, a major device of the AP system is discussed and then the requirements, design, and code are developed, and the device's structural test is performed prior to going on to discuss and develop the next major device. Finally, in the incremental AP development method, all of the specifications and requirements may be developed, but the design and implementation are developed one function at a time.

  In any case, if the operating system was uniquely developed for the system-under-test, that operating system should be structurally tested first. This portion of the code itself should be broken down into functionally cohesive packages if it is large and/or complex; otherwise, it can be structurally tested as an entity. The second portion of the AP to be tested is normally the unique input/output section. If there are diverse input/output devices, these may be structurally tested separately. But it is often best to select a thread that includes both the ability to input data and to see the resulting output for each structural test. The third step is to select and structurally test a functionally cohesive portion of the application and the utilities needed to support that application. Then, select the next functionally cohesive portion of the AP and associated application utilities for the next structural test, and so on. All previously tested functions should be regression tested, as appropriate.

During the review the data format in the AP should be verified for:

- completeness; (e.g., all safety functions have been implemented and all states for each safety function have been considered);
- self-consistency; (e.g., the same consistency has been used throughout the program and ensure that the safety logic is clear, self explanatory and visually segregated from non SIF logic such as status reporting etc.);
- protection against unauthorized alteration; (e.g., two levels of protection should be applied, one level at the application programming station to ensure that the application source code is not modified without the appropriate authority and the second level to ensure that an AP cannot be downloaded to the SIS without the appropriate authority);
- consistency with the functional requirements: (e.g., ensure that each functional requirement has been interpreted correctly);
- consistency with the data structures: (e.g., ensure that data structures are readable and the same format is used throughout the AP);
- compatibility with the underlying embedded software (e.g., sequence of execution, run-time);
- correct data values; (e.g., the correct data types have been used such as integer or floating point, Boolean, etc.);
- operation within a known safe boundary; (e.g., range checking within the application to ensure that values stay within the range expected and tested);
- having the capacity for safe modification.

The AP should also be verified to ensure that modifiable parameters are protected against:

- invalid or undefined initial values; (e.g., ensure that all modifiable values that can be entered have a default value to ensure that the AP is kept in range if no value is entered by the user);
- erroneous values; (e.g., provide an alarm or shut down if a value goes outside the range tested or expected by the process);
- unauthorized changes; (e.g., ensuring that unauthorized changes cannot be made by a user or that a value cannot be changed by a fault in another system);
- data corruption. (e.g., ensure that data cannot be corrupted by any non safety task or system).

Communications, process interfaces and associated AP should be verified for failure detection, protection against message corruption data validation, unless previously addressed through an IEC 61508 compliant device.

The application response time should be checked for all safety functions to ensure that the data route through the application is such that the process safety time can be met. For example, the logic layout may mean that the AP should go though several cycles before the safety function is resolved.

A.12.5.4 No further guidance provided.

A.12.5.5 From the start of the formal testing, all changes to AP functions and configuration data should be implemented strictly in accordance with a defined modification procedure.

A.12.5.6 No further guidance provided.

A.12.6 Guidance to "Requirements for application program methodology and tools"

A.12.6.1 See IEC 61508-3:2010, Annex D and ISA TR84.00.09 for further guidance. See also Annex G for additional considerations. The programmer should not make any assumptions beyond those defined in the safety manual, for example, to use compiler

capabilities which are omitted from the safety manual. Ideally, the compiler would have been configured to enforce these restrictions.

For some PE systems the full range of configuration functions may include general control functions that depend on algorithms that are difficult to prove always respond in a predictable manner – for example functions which make use of algorithms which do not reliably terminate (e.g., recursion) or which could result in exceptions in the program execution (e.g., 'tan 90 degrees'). For this type of system the manufacturer will normally supply a 'PE Manual' which defines which functions can be used for safety applications. Further, where general purpose PE systems are used it may be necessary to limit the way the tools are used to avoid tools which are known to have faults in their operation (often this can be found on user discussion forums) as well as to limit the complexity of the programming functions to those which have been proven to behave in a dependable manner. In this case it will be necessary to supplement any PE manual provided with the PE system with additional procedures to constrain the way the tools are used (e.g., to specify good programming practice, identify any unsafe features (e.g., undefined language features, non-terminating algorithms), identify checks to detect faults in the configuration and specify procedures for documentation of the AP which are aimed at ensuring the predictability of the AP. If the architecture of the SIS is not defined in the PE Manual the procedures should also include the way fault tolerance will be handled, for example redundancy and diversity. Consideration should be given to whether any extra AP constraints – such as watchdogs, data checking etc. should be defined.

Instructions and examples to enable a group of programmers to produce programs of similar format and style may also be provided either as part of the safety manual or as an application specific document. These instructions should include details of specific algorithms or functions that are not to be used in the programs, since the algorithms or functions may result in unexpected behavior which might affect safety.

Typical sections of the PE safety manual are:

a) safety integrity levels for which the device or system is suitable;

b) the expected behavior of each library function (i.e., to ensure well-defined syntax and semantics of the programming language used);

c) rules and constraints aimed at restricting the use of "unsafe" features of the application language and toolset.

d) requirements for, and limitations of, tools and programming languages;

e) use of embedded watchdogs;

f) guidance to the programmer on how to use the programming tools to check the correct use of data variables. Other features to address may include memory mapping, checks on status flags and validity checks on input values.

A.12.6.2 The set of methods and techniques used to develop the AP should be identified and the rationale for their choice should be justified.

A typical toolset that supports application programming is given in Clause E.1.

The methods and techniques should be selected to minimize the risk of introducing faults into the AP during development. This may include the consideration of:

- well-defined syntax and semantics;
- suitability for the application;
- understandability by personnel involved in the development, maintenance and use of the system;
- guarantee of properties important to the SIF (e.g., worst case execution time);
- evidence of successful use in similar applications;

- rules and constraints aimed at restricting the use of “unsafe” features of the method – for further guidance see Clauses E.2 and E.3;
- a deterministic order of execution and updating of data items

Methods and techniques for removing faults include, review, simulation testing, analysis and analytical proof – see also 12.5 of IEC 61511-1:2016.

To ensure that the faults remaining in the AP will not lead to unacceptable results, the following could be considered:

- on-line checking techniques and exception handling;
- use of vendor offsite databases and global fault reporting;
- monitoring of SIS failure reports and of process issues and their impact on the SIS;
- mirroring of key SIS functionality in other systems;
- use of a duplicate of the SIS AP during the training process.

Methods and tools for managing modifications include configuration and version control, requirements management databases, update of as-built documents, document control and change management, traceability and tracking of responsibility for change, automatic test suites.

Tools should be selected to implement the methods and techniques so as to reduce human error in their practical application. This may include the consideration of:

- familiarity with tools by the appropriate members of the development team;
- evidence of successful use of the tools in similar applications;
- rules and constraints aimed at restricting the use of “unsafe” features of the tools;
- documented list of the precise version of all tools and the SIS;
- compatibility between the different tools and with the SIS;
- ability to generate AP documentation;
- the predictability of the behavior of the SIS subsystem;
- compatibility of the fault tolerant architecture between the AP design and the hardware;

The PE application development environment and language should comply with IEC 61508-3:2010, Table A.3.

Where it is decided to use tools which have not been provided as part of the PE system, consideration should be given to how the following attributes can be achieved:

- simplicity in the AP arrangement;
- provision of comments embedded in the AP to explain its functions and expected behavior;
- how test coverage can be maximized and demonstrated;
- guarantee of properties important to the SIF (e.g., worst case execution time);
- suitable commentary and natural language support;
- compartmentalization to reflect the application;
- commonality of style with other related AP.

Other methods, techniques and tools that could be considered include metrics measurements (e.g., test coverage) and use of different tools to enhance verification of a function(s) (e.g., back-to-back tools).

The availability of tools (not necessarily those used during initial system development) to supply the relevant services over the whole lifetime of the SIS should be considered.

For further details on the characteristics of the programming environment and tools, see Annex E.

A.13 Factory acceptance testing (FAT)

A.13.1 Objectives

The purpose of the factory acceptance test (often including an AP integration test) is to show that the SIS can implement all of the required SIFs within the required response time, meets other functional requirements of the SRS and is free from foreseeable undesirable behaviors.

A.13.2 Guidance to "Recommendations"

A.13.2.1 A FAT can be recommended for those logic solvers implementing SIFs having fairly complex application logic or redundancy arrangements (e.g., 1oo2, 1oo2D, 2oo3, etc.).

A.13.2.2 The most important part of the FAT is to have a well defined, well written and well structured test procedure that defines how to test the application logic and what to look for after each step.

Personnel that will be operating the process should attend the FAT since it will give them some early training on the operation of their SIS. Often, they can also provide good suggestions or enhancements to the test procedure that were not foreseen during the design.

A.13.2.3 No further guidance provided.

A.13.2.4 No further guidance provided.

A.13.2.5 During the FAT, interfaces should be tested (e.g., communications between the BPCS and SIS).

A.13.2.6 No further guidance provided.

A.13.2.7 No further guidance provided.

A.14 SIS installation and commissioning

A.14.1 Objectives

A.14.2 Guidance to "Requirements"

A.14.2.1 No further guidance provided.

A.14.2.2 The SIS should be installed per the design and installation plan. Any deviations from the design should be properly reviewed with the project team to ensure all of the design requirements are still satisfied. After the SIS has been properly installed, it should be fully commissioned and validation activities should be initiated.

A.14.2.3 While IEC 61511-1:– has addressed commissioning as a single phase, it is recognized that the application, the experiences of the project team, and project needs may require commissioning to be accomplished in several phases. Instrument configuration includes settings which ensure the instrument performs properly according to the SRS or safety manual (e.g., dampening, linearization, etc.).

A.14.2.4 Documentation that shows compliance with required configurations (I.e., requirements per SRS or safety manual) should be produced.

A.14.2.5 No further guidance provided.

A.15 SIS safety validation

A.15.1 Objective

The objective of the SIS safety validation is to validate that the SIS achieves the requirements stated in the SRS. Validation activities should be completed prior to the placing of the SIS into operation.

A.15.2 Guidance to "Requirements"

A.15.2.1 No further guidance provided.

A.15.2.2 The AP validation plan should be included as part of the overall SIS or SIS subsystem validation plan.

A.15.2.3 No further guidance provided.

A.15.2.4 If the SIS has already been through a factory acceptance test (FAT), this may be taken into consideration during the validation. The validation team should review the results of the FAT to ensure that the entire AP was successfully tested and all problems found during the FAT have been corrected.

It will be very important to ensure that there has been no shipping/storage/handling damage, that all sensors and final elements are correctly connected to the logic solver, that the SIF perform properly and that the operator interface provides the necessary information.

A.15.2.5 No further guidance provided.

A.15.2.6 The final stage of testing, i.e., demonstration that the integrated system worked correctly in its intended environment, with the intended physical devices and interfaces and with the defined operating procedures, can only be fully completed after the whole system installation and during commissioning.

A.15.2.7 No further guidance provided.

A.15.2.8 Forcing of inputs and outputs in PE SIS should not be used as a part of AP operating procedure(s).

Forcing of inputs and outputs without taking the SIS out of service should not be allowed unless supplemented by plant approved procedures and access security. Any such forcing should be announced or set off an alarm, as appropriate.

Maintenance overrides should be announced.

A.16 SIS operation and maintenance

A.16.1 Objectives

No further guidance provided.

A.16.2 Guidance to "Requirements"

A.16.2.1 A SIS maintenance plan should be established. The maintenance plan should describe all of the potential degraded modes of the SIS caused by SIS failure or maintenance. The compensating measures associated with these degraded modes should be identified and maintenance plans developed. All maintenance action should be recorded.

A.16.2.2 In the case of a failure and/or bypass of a SIF while the process is in operation, the likelihood of an unsafe process state is increased. Thus, procedures should be in place for:

- diagnosing failures situation, especially failures model, causes to make related risk reduction measures, while warning to operators;
- identifying compensating measures allowing continued operation at a tolerable safety level;

  NOTE 1 An example of a means for testing diagnostics is to insert an artificial fault.

  NOTE 2 Failure mode and effect analysis are important tools for risk analysis and their use is recommended.
- bypass due to functional proof testing.

Strict operation procedures and risk mitigation measures should be applied to the start-up and the removing of the bypass (e.g. the approval before applying the bypass, warning to operators whilst the bypass is in place, loop inspection prior to return to the full operational state). Proper training should be given to operators.

– the methods and procedures which are used to test the diagnostics. If fault insertion testing is used, the negative impact should be considered to ensure that the SIF and the SIL of the system still meet the functional safety requirements after returning to the full operational state.

If the diagnostics indicate a failure by means of the fault insertion testing, proper analysis to determine the reason and effect of this failure to the SIF and its SIL should be performed, and action taken:

g) according to the maintenance procedure to deal with the random hardware failure (e.g., maintain or change the device); or

h) return to the relevant life-cycle phase and proceed according to management of change process to deal with the system failure (e.g., undetected designing error).

A.16.2.3 The following can be addressed:

- causes of demand requiring compensating measures;
- instruction for use of compensating measures; and
- which manner the compensating actions will bring the process to a safe state, response time and consequence on failure of the compensating measure;
- strict operation procedures and risk mitigation measures should be applied to the start-up and the removing of the bypass (e.g., the approval before applying the bypass, warning to operators while the bypass is in place, loop inspection prior to return to the full operational state). Proper training should be given to operators.

A.16.2.4 No further guidance provided.

A.16.2.5 No further guidance provided.

A.16.2.6 No further guidance provided.

A.16.2.7 No further guidance provided.

A.16.2.8 No further guidance provided.

A.16.2.9 No further guidance provided.

A.16.2.10 No further guidance provided.

A.16.2.11 Proof test procedures for sensors and final elements should include fully testing their interface to the process gas/fluid. The test carried out by remote access should influence the performance of the SIF.

NOTE An on-line test may be possible when using a local smart device.

A.16.2.12 No further guidance provided.

A.16.2.13 Assumptions made during SIL determination may influence the SIL of the system.

Operations management should review and verify assumptions made during SIL determination including occupancy, probability of avoidance, procedures to avoid or reduce demand, and procedures to be applied on alarm.

A new risk analysis should be performed if these assumptions deviate from the actual condition.

A.16.3 Proof testing and inspection

A.16.3.1 Guidance to "Proof testing"

A.16.3.1.1 The proof test interval should be selected to achieve the average probability of failure on demand as required in the SRS.

A.16.3.1.2 Proof tests of the SIS have to reflect the real operating conditions as accurately as possible. Proof testing should be performed before any regular maintenance activity that is likely to distort any representative test results.

Proof testing of the SIS is preferably to be carried out as an integral test, i.e., the entire SIS loop should be tested together. The proof test can either be performed as an end-to-end (i.e., full loop) integrated test, or by using a segmented approach (series of overlapping device level tests, i.e., sensors, logic solvers, and final elements). Proof testing should include, but not be limited to, verification of following conditions:

a) operating logic sequences, e.g., as given by cause & effects diagrams;
b) operation of all input devices including field sensors and SIS input modules;
c) logic associated with each input device;
d) logic associated with combined inputs;
e) trip initiating values (set-points) of all inputs;
f) alarm functions;
g) speed of response of the SIS when necessary;
h) operation of SIS output modules and all final elements;
i) computational functions performed by the SIS;
j) timing and speed of output devices;
k) functioning of manual actions bringing the process to its safe state;
l) functioning of user-initiated diagnostics;
m) the SIS is operational after testing, e.g., reset of any inhibit or override.

If a SIS loop test is not possible due to safety or operational reasons, a partial test may be performed for devices or subsystems part of the SIS loop. Some items may be tested under

process operating conditions by providing inhibit of the input signal or override of an output action. Items such as process valves, which cause process shutdown, may therefore be tested during planned shutdown periods.

For those applications where partial testing is applied, it is imperative that the test procedures are written to ensure that all loop items are included:

- testing the final element during unit shut down;
- testing the SIS by exercising the output(s) as far as practical (e.g., output trip relay, shut down solenoid, partial valve movement) during on-line testing;
- any limitation of the testing period of the final elements should be taken into account in the calculation of the PFD_{avg} of the SIF.

All paths through redundant architectures should be proof tested to demonstrate that all channels are working correctly and not just sufficient channels to initiate the output. This often requires special provisions to be made to facilitate the testing.

A complete SIS loop test should be performed at predetermined intervals.

Parts not covered by the tests should be proven by other means, e.g., if dangerous failures cannot be detected by the proof testing such item should be overhauled at predetermined intervals.

For valves, partial stroke test may be treated as a functional test which covers a fraction of the possible failures, and not as self test with diagnostic coverage. The fraction detected should be properly documented through a failure modes, effects, and diagnostic analysis (FMEDA) or similar.

A.16.3.1.3 The frequency of proof tests should be consistent with applicable manufacturer's recommendations and good engineering practices, and more frequently, if determined to be necessary by prior operating experience.

There are a number of strategies being used to select the proof test interval for a SIF.

For example, some users like to make this proof test interval as long as possible to minimize maintenance cost and the potential impact of testing. In this case, the SIS design may include more redundancy in equipment, increased diagnostic coverage and robust devices. After completion of the design, a calculation may then be performed on the design to determine the maximum test interval allowed to achieve the SIL performance defined for the SIF. The negatives to this design philosophy are that each system in a plant will have a different test interval and may require more rigorous compliance tracking. It also may encourage designing the performance toward the low end of the performance curve (e.g., $PFD_{avg} = 10^{-1}$ for SIL 1 systems and $PFD_{avg} = 10^{-2}$ for SIL 2 systems).

It should be noted that the PFD_{avg} is a time dependant probability which increases when the time increases. Therefore for large proof tests intervals, it can become very large even if in average the SIL target is reached, and it may become a very poor indicator of the risk. This may be unacceptable, but staggering tests, to some extent, reduce the impact of this problem.

Other users may wish to standardize on the basis of a defined test interval and test all systems in a manufacturing plant at the same test interval. For example, they may wish to test each SIF annually so they design each SIS accordingly. By pre-selecting a proof test interval prior to beginning the design, user companies can then pre-select architectures, devices and diagnostic coverage that will satisfy the SIL for most applications. By having these features already defined in their corporate standards, it reduces the design engineering cost for most applications. In this case, a calculation should be performed on the SIS to ensure the required SIL performance is satisfied with the pre-selected proof test interval.

In addition, shutdowns due to actual demand on the SIS during operation may be given credit as proof tests (fully or partial) under given conditions such as:

- the shutdown documents equivalent information as registered during corresponding proof testing;
- the shutdown covers all parts of the SIS, and if not, the devices or SIS subsystems not activated should be tested separately;
- the shutdown occurs within a predetermined maximum time window before the next planned proof test which then can be cancelled.

If these conditions are fulfilled, the next planned proof test may be skipped.

In the choice of a proof test interval, considerations should be given to the demand rate for demand mode systems, the failure rate of each device being tested, and the overall system performance requirements.

A.16.3.1.4 No further guidance provided.

A.16.3.1.5 No further guidance provided.

A.16.3.1.6 No further guidance provided.

A.16.3.1.7 No further guidance provided.

A.16.3.2 Guidance to "Inspection"

As stated in IEC 61511-1:2016, inspecting the SIS is different from proof testing. Whereas a proof test is ensuring the SIS will operate properly, a visual inspection is required to validate the mechanical integrity of the installation.

Normally, the inspection is done at the same time as the proof test but it may be done at a more frequent interval if desired.

NOTE 1 The inspection may detect incipient failures, which proof testing does not find.

NOTE 2 A SIS component, sub-system or system in poor condition is likely to have a higher failure rate (λ) than that assumed in the PFD_{avg} and residual risk calculations. Poor condition of any such items can be remedied.

A.16.3.3 Guidance to "Documentation of proof tests and inspection"

It is important to document the results of the proof test and inspection for a record of what was found. There are no specific requirements for how long these results should be retained but generally a sufficient number are retained to allow for re-examination of previous results to see if there is a history of device failure.

For example, if a sensor failed a proof test, it is good practice to review the results of previous proof tests to see if this sensor had failed a similar proof test within the past few tests. If the history indicates repeating failures, consideration should be given to redesigning the SIS using a different type of sensor.

A.17 SIS modification

A.17.1 Objective

Modification applies primarily to changes occurring during the operational phase of the SIS.

A.17.2 Guidance to "Requirements"

A.17.2.1 Every change to the SIS (subsystem or components) is a modification unless a replacement in kind is performed. Such modifications may include issues related to:

- new proof test interval or procedures;
- components with different characteristics, e.g., replacing obsolescent components;
- changes of set-point;
- changes in operating conditions;
- changes in operating procedures;
- changes to application software or firmware;
- correction of systematic failures;
- a failure rate higher than desired;
- increased demand rate.

A.17.2.2 No further guidance provided.

A.17.2.3 Wherever possible, on-line modifications to a SIS AP should be avoided. If on-line modifications are required, the complete procedure should be documented and approved according to the safety planning.

A.17.2.4 No further guidance provided.

A.17.2.5 No further guidance provided.

A.17.2.6 No further guidance provided.

A.17.2.7 No further guidance provided.

A.17.2.8 No further guidance provided

A.18 SIS decommissioning

A.18.1 Objectives

No further guidance provided.

A.18.2 Guidance to "Requirements"

A.18.2.1 No further guidance provided.

A.18.2.2 No further guidance provided.

A.18.2.3 No further guidance provided.

A.18.2.4 No further guidance provided.

A.18.2.5 No further guidance provided.

A.19 Information and documentation requirements

A.19.1 Objectives

For examples of documentation structure, see IEC 61508-1:2010 Annex A and, for more details, IEC 61506. The documentation can be available in different forms (e.g., on paper, film or any data medium to be presented on screens or displays). A variety of different examples of documentation are provided in the annexes for illustration only.

A.19.2 Guidance to "Requirements"

A.19.2.1 The list of the information and documentation that may be used to implement a SIS, includes:

a) results of the H&RA;

b) protection layer allocation;

c) assumptions used when determining the integrity requirements;

d) SRSs;

e) application logic;

f) design documentation;

g) modification information and/or documentation;

h) records of verification and validation;

i) commissioning and SIS validation procedure(s);

j) SIS operating procedures;

k) SIS maintenance procedures;

l) proof test procedures;

m) results of assessments and audits.

A.19.2.2 SISs should be identified and documented in a manner that clearly distinguishes them from other non-safety related systems, such as BPCS.

A.19.2.3 No further guidance provided.

A.19.2.4 No further guidance provided.

A.19.2.5 No further guidance provided.

A.19.2.6 No further guidance provided.

A.19.2.7 No further guidance provided.

A.19.2.8 See Clause F.26 for a typical list of documents provided with SIS design.

A.19.2.9 No further guidance provided.

Annex B
(informative)

Example of SIS logic solver application program development using function block diagram

B.1 General

The following example describes:

- A method of organizing the activities related to AP development satisfying IEC 61511-1:–, 6.3;
- The generation of the AP SRSs on the basis of the SRSs thus answering to IEC 61511-1:–,10.3.2;
- The development and implementation of two shutdown functions in an AP satisfying 7.2.2, 11.5.2.3, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6 and 15.2.2 of IEC 61511-1:2016.

B.2 Application program development and validation philosophy

An efficient development methodology is required to help the AP engineers to design the SIFs with predictable performance and the requested safety integrity (i.e., SIL 3).

Traditionally the AP design engineers are able to do a complete test of the AP design only in the later part of the design effort when the actual hardware architecture is available. This is a highly inefficient method as on discovering an error at this stage they have to go back to the relevant design phase to correct the errors and come out with a new release resulting in a drastic increase in the time and money involved in developing the final product.

The traditional text based approach of safety AP specification is not efficient enough to handle the advanced, complex safety requirements commonly found in SIF specifications.

The most efficient tool to address these challenges is the Model-based design (MBD). MBD is a mathematical and visual method of addressing the problems associated with designing complex safety systems, and is being used successfully in many applications. It provides an efficient approach to overcome the difficulties of the development phase of the safety life-cycle. This approach and this example include the following steps:

- Modeling the AP SRS by:
  - identifying the concerned SIS elements,
  - describing their behavior with an appropriate modeling language;
- Analyzing and synthesizing the behavior of the foreseen implementation of the AP SRS with respect to their fulfilment;
- Demonstrate the compliance of the AP implementation with the SRS in order to document the validation process and contribute to satisfy IEC 61511-1:2016 12.5 and 15.

This allows to locate and to correct errors early in AP design, where the time and financial impact of AP modification is minimised. Design reuse is facilitated with MBD, both for AP upgrading and for derived APs development with expanded capabilities. MBD provides a common design environment for all developers, facilitating general communication, data analysis, and AP verification between different development groups.

Text specification and simulation have been in use for a very long time, but they are highly inefficient and inadequate to deal with the advanced and complex features of SIFs since these tools are totally non-graphical in nature and are not providing mathematical proofs

supporting assessment. Because of the limitation of graphical tools design engineers used to heavily rely on traditional text-based programming and mathematical models. And this used to be a major cause of concern to guarantee safety integrity since developing models in text-based programs isn't just difficult and time consuming but also highly prone to errors. Debugging the model and correcting the errors used to be a tedious process. It requires a lot of trial and error cases before a final fault free model can be created, as functional model used to undergo unseen changes during the translation of the model through the various design stages. These challenges are nowadays overcome by the use of dedicated graphical modelling tools supported by development software packages satisfying 12.6 of IEC 61511-1:2016 and covering the whole AP safety lifecycle of 6.3.1 of IEC 61511-1:2016. This allows to develop in a single repository both specifications and implementation with the benefit of being able to prove safety integrity properties at a very low cost compared to manual techniques. The general AP development philosophy of this example is to follow model based engineering practice.

- The following models will be sequentially realised, incrementally integrated and used, to support design and validation:
- Functional models:
  - Hardware functional architecture model
  - Hardware physical architecture model
  - AP functional architecture model
  - AP architecture model
- Safety properties models:
  - Time properties
  - Safety integrity properties
- Checking model.

These models are progressively integrated in order to sequentially demonstrate the compliance of the AP to the AP SRS.

These models are used for:

- Design as being the materialization of the specification of the functional and safety integrity detailed specification;
- Automatic compiled AP production;
- Semi-automatic testing through model checking in order to verify whether each AP module meets its functional and safety specifications;
- Validation by providing extensive description of test coverage and test results.

B.3 Application description

B.3.1 General

This example is based on a part of a SIS for an LNG plant.

B.3.2 Process description

The process supporting this example is a part of a liquid natural gas terminal. The aim of the plant is to receive LNG from ships, to store and prepare the LNG for injection in the gas grid.

B.3.3 Safety instrumented functions

B.3.3.1 General

The SIS for the above described process includes 7 SIL 3 SIF and 64 SIL 2 SIF. The example focuses on one SIL 3 SIF and one SIL 2 SIF. The information given below can be considered as being part of the SRS and used as input for the AP SRS.

B.3.3.2 SIF 02.01 – LNG unloading emergency stop

The process section concerned by this function is described in Figure B.1.

The aim of this SIL 2 function is to isolate the ship from the plant in case a High High Pressure is detected in one of the three LNG tanks.

The demand on the function occurs when a high high pressure is detected by a pressure switch (the sensors are not shown on Figure B.1) in any one of the three LNG tanks. The function then closes 3 valves (XV1008, XV2008 and XV3008). If the high high pressure is still present after a given delay, two additional valves (XV1014 and XV2014) are closed. The valves shall remain closed until reset even if the high high pressure signal disappears.

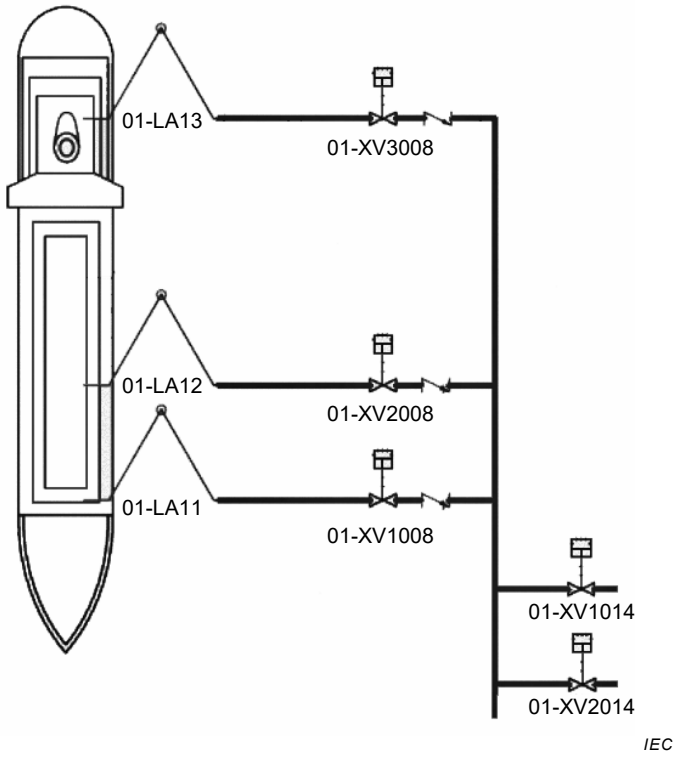


Figure B.1 – Process flow diagram for SIF 02.01

B.3.3.3 SIF 06.02 – ORV feed valve emergency closure

The process section concerned by this function is described in Figure B.2.

The aim of this SIL 3 function is to isolate each ORV by closing the feed valve XV1001 and the isolation valve XV1013 on detection of low low temperature (the sensors are not shown in Figure B.2) on the export pipe by a temperature switch. Only one valve shall be closed at a time in order not to trap gas in the circuit between the valves. The valves shall remain closed until reset even if the low low temperature signal disappears. The closure of both isolation valves leads to a dangerous state. Avoiding this dangerous state is rated SIL 2.

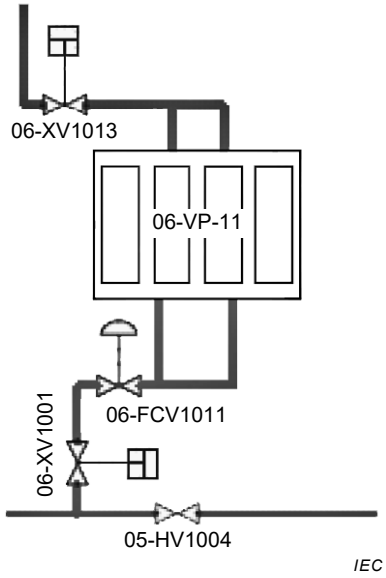


Figure B.2 – Process flow diagram for SIF 06.02

B.3.4 Risk reduction and domino effects

The risk analysis specifies that a demand on both SIF at the same time can be dangerous and shall not occur.

B.4 Application program safety life-cycle execution

B.4.1 General

Clause B.4 describes sequentially:

- the inputs necessary for AP SRS development extracted from the SRS;
- the AP SRS development (IEC 61511-1:2016, 10.3.2);
- the AP architecture design (IEC 61511-1:2016, Clause 12);
- the AP modeling, design and testing (IEC 61511-1—, 12.3 and 12.4);
- the AP integration modeling and testing (IEC 61511-1:2016, 12.4 and 12.5);
- the AP production;
- the contribution to the SIS validation (IEC 61511-1:2016, Clause 15).

B.4.2 Inputs to application program SRS development

B.4.2.1 General

The following are the inputs coming out of the previous life-cycle phases.

B.4.2.2 Functional specification

The functional specification arising from the refining of the requirements described in Figures B.1 and B.2 is described in Figure B.3 hereunder. These schematics describe the expected behavior of the SIFs prior to any decision on the future necessary hardware and application software for their implementation.

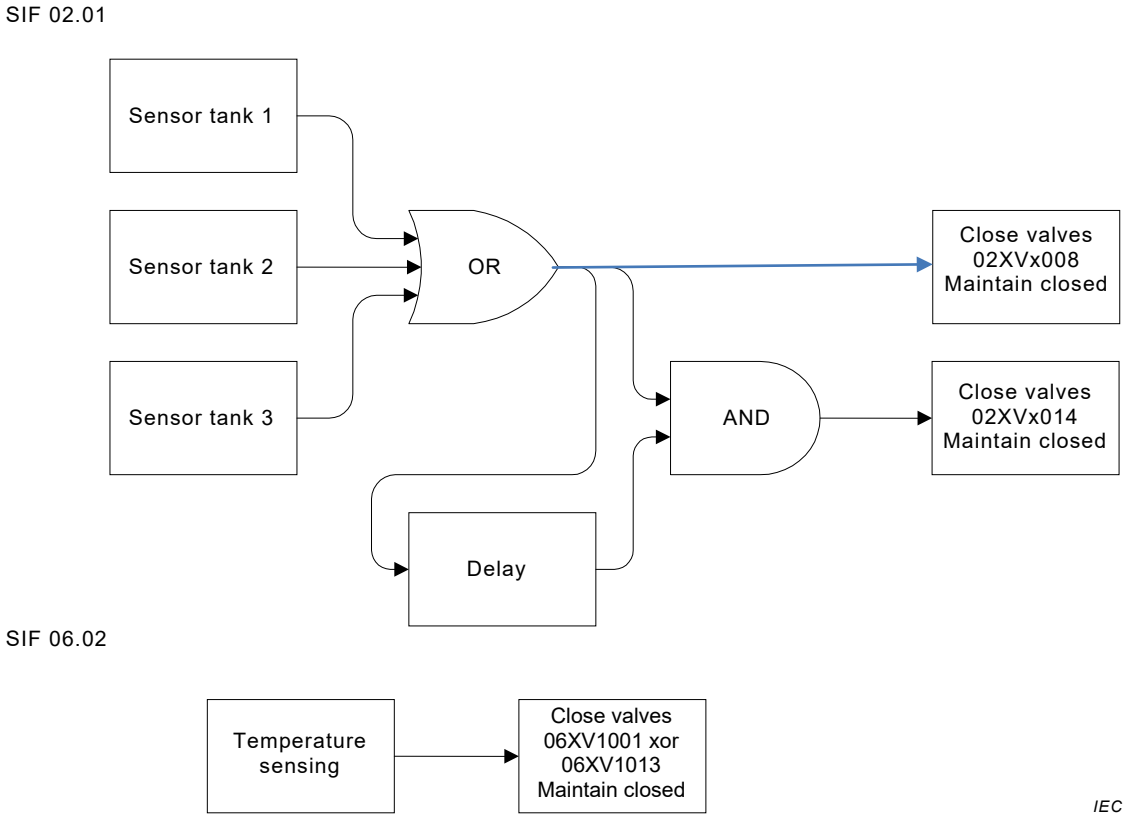


Figure B.3 – Functional specification of SIF02.01 and SIF 06.02

B.4.2.3 Hardware functional architecture

These diagrams show the hardware architecture necessary to implement the SIFs prior to the application of HFT constraints and any other requirement of the SRS.

SIF 02.01

The hardware functional architecture is illustrated in Figure B.4:

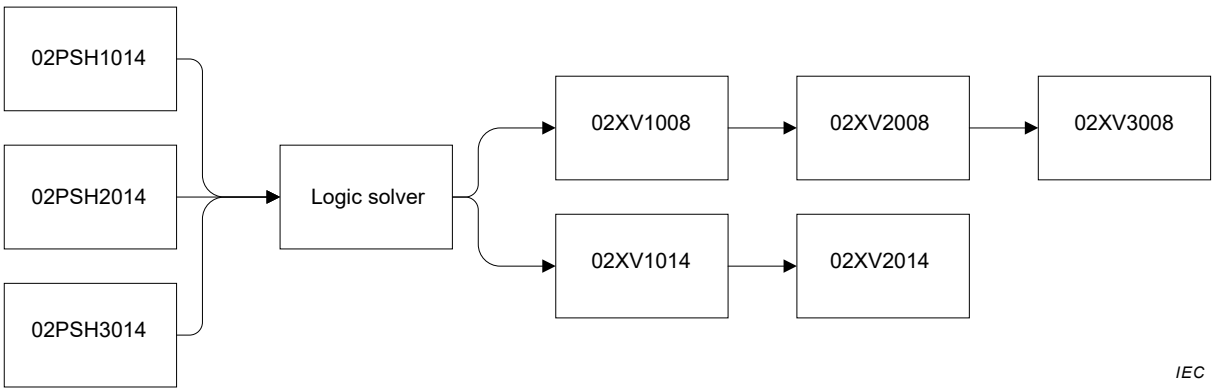


Figure B.4 – SIF 02.01 hardware functional architecture

SIF 06.02

The hardware functional architecture is illustrated in Figure B.5 as follows:

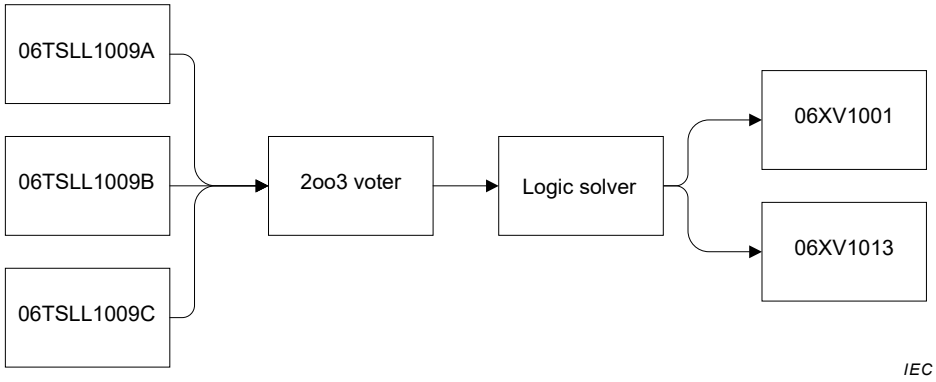


Figure B.5 – SIF 06.02 hardware functional architecture

B.4.2.4 Hardware typical specification for SOV/MOV

The piping and instrumentation diagram usually describes all the hardware and AP interfaces of a device. Figure B.6 describes the hardware and AP interfaces to be implemented for an SOV in both BPCS and SIS.

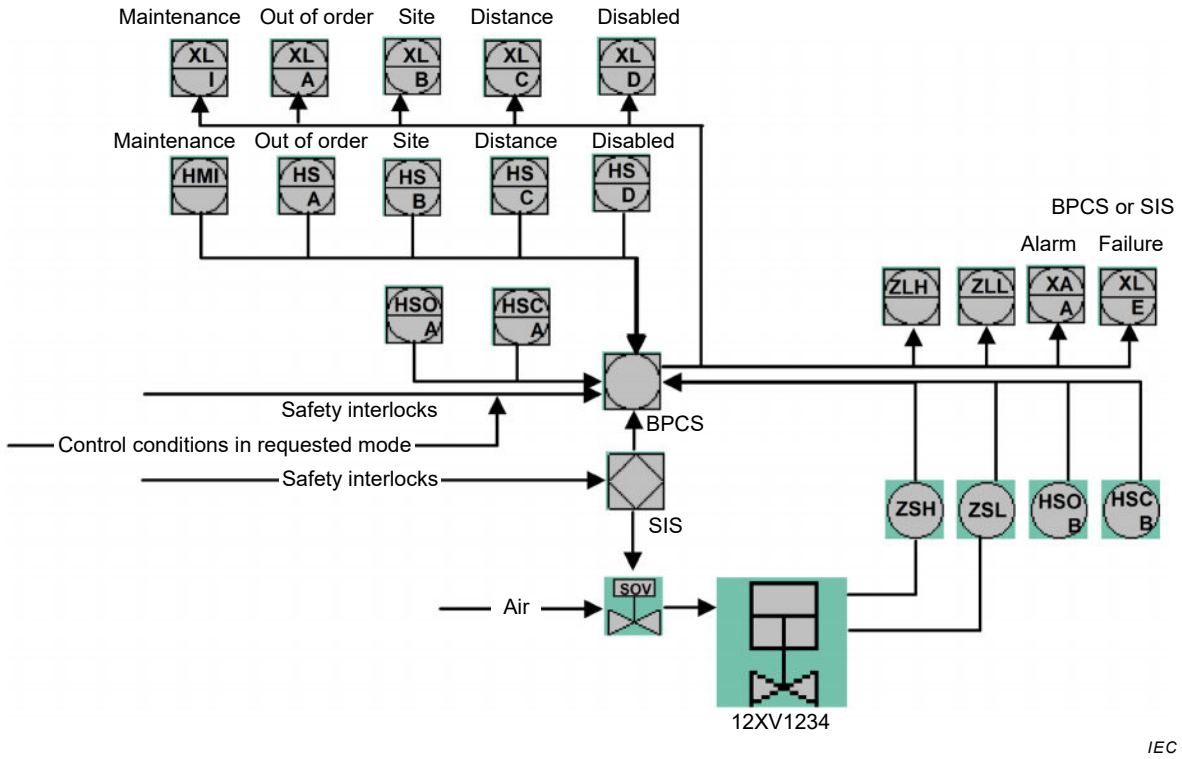


Figure B.6 – Hardware specification for SOV extracted from piping and instrumentation diagram

B.4.2.5 Hardware physical architecture specification

Refining the derived requirements described in Figures B.5 and B.6 leads to the definition of the actual hardware to be used and to its final architecture as described in Figures B.7 and B.8.

NOTE 1 The description of the application of hardware fault tolerance requirements coming out of IEC 61511-1:2016 Clause 11 requirements is not discussed hereunder.

NOTE 2 In this example the link between BPCS and SIS is discrete (hard wired).

SIF 02.01

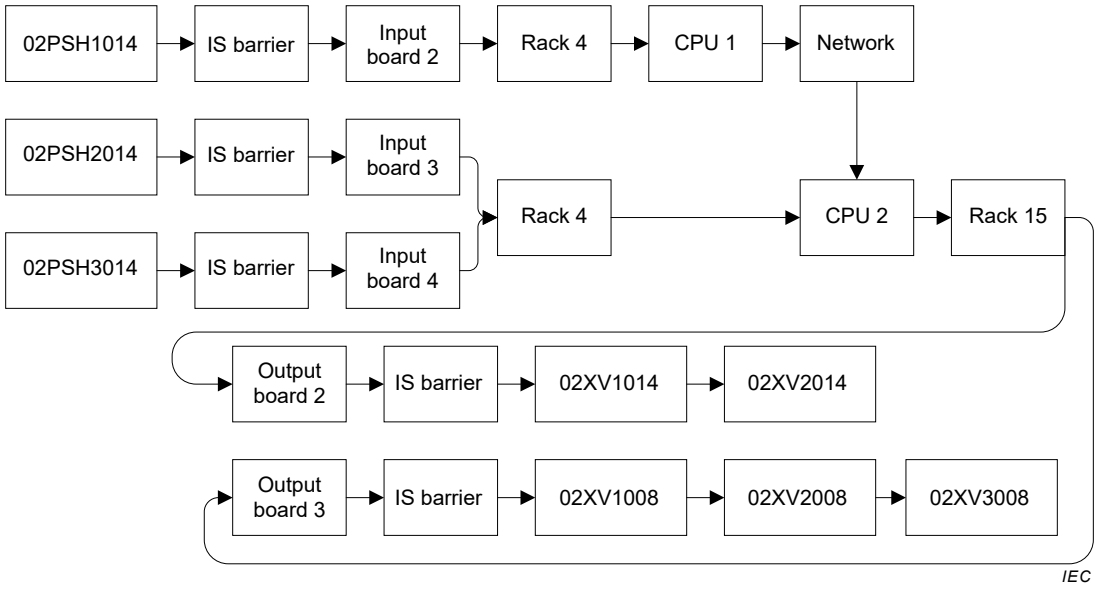


Figure B.7 – SIF 02.01 hardware physical architecture

SIF 06.02

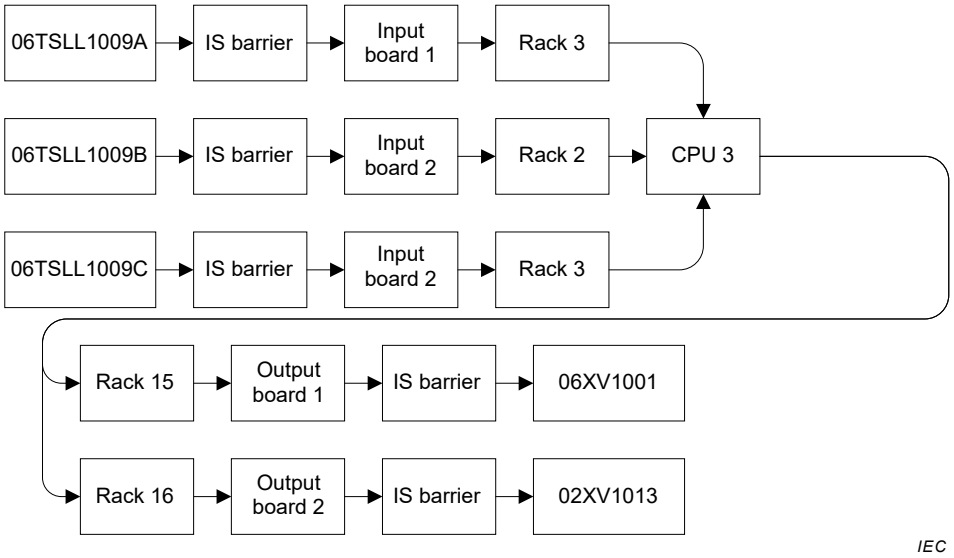


Figure B.8 – SIF 06.02 hardware physical architecture

B.4.3 Application program design and development

B.4.3.1 General

Subclause B.4 includes examples to describe the following steps:

- AP SRS development;
- AP functional architecture design;
- AP functional design, modeling and testing;
- AP integration modeling and testing.

B.4.3.2 Application program SRS

B.4.3.2.1 General

The AP SRS can be organised as following:

- Functional requirements corresponding to expected behaviors:
  - Requirements for the devices (sensors and actuators);
  - Requirements for each SIF interlocks;
  - Requirements for interlocks between SIFs;
- Safety integrity requirements corresponding to behaviors to be avoided:
  - At device level;
  - At SIF level;
  - At a higher level such as the plant level.

B.4.3.2.2 Application program functional requirements specification

B.4.3.2.2.1 Device functional requirements

The device functional requirements can be described per device type and organised in:

- generic device operating modes; and
- device functional specification.

Subclause B.4.3.2 provides an example for an SOV.

General actuators operating modes:

The state machine for the operating modes of a solenoid operated valve (SOV) is defined hereunder in Table B.1.

Table B.1 – Modes of operation specification

State Name	Description
Requested	When safety conditions generate a safety sequence, the valve is requested to be controlled from a higher level logic. This request has priority over any other operating mode. The device is then locked in requested mode. Its individual commands become unavailable, and the valve is only controlled by the higher level logic. When the logic releases the safety conditions, the operating mode is forced to DISTANCE mode, the operator is then free to change the operating mode.
Distance	The valve is controlled through the BPCS man machine interface open and close commands. This is the initial state.
Local	The valve is controlled through the local push buttons open and close commands located close to the valve.
Out of order	This mode is possible only if the valve is already in its safe position. All local and distance operator commands become unavailable. The control through the safety conditions remains active.
Maintenance	This mode is possible only if the valve is already in its safe position. The state is forced to Out of order and all alarms are inhibited.

SOV functional specification:

The device is an isolation solenoid operated valve controlled by the SIS and by the BPCS.

It is assumed that with respect to danger protected by the SIF, the SOV has a unique and non-variable safe position. This position is closed.

The SOV is an autonomous device: It has individual commands from the BPCS and can in particular circumstances be controlled by a higher level logic. The logic to control a device such as an SOV is called a “typical”.

The typical for this SOV allows the following to be realised:

- open and close command from the BPCS operator stations;
- local open and close commands from the site through the BPCS;
- move to safe position on SIS or BPCS initiation;
- cabling of the open and close commands from the SIS;
- selection of the operating mode from the BPCS operator stations by a software switch;
- realignment of the commands in the following cases:
  - commands realignment on limit switches information at initialization;
  - commands realignment on higher level logic interlocks in requested mode;
  - commands realignment on site commands in site mode;
  - commands realignment on safe state in case of safety action;
- handling of the maintenance state;
- valve status visualization from the two limit switch information;
- conflict alarm generation (at opening or at closure, simultaneous detection of both limit switches, limit switch failure). In order to avoid spurious conflict alarm generation, the limit switch information is delayed to allow an SIS command to be transmitted to the BPCS;
- BPCS and SIS failure detection;
- tuning and tuning parameters modification.

Parameters: conflict detection delay.

Access at maintenance level only.

B.4.3.2.2.2 SIF functional requirements

The functional requirements for each safety function are described in the SRS.

B.4.3.2.2.3 Interlocks between SIFs functional requirements

There are no functional requirements at this level.

B.4.3.2.3 Safety integrity requirements specification

B.4.3.2.3.1 Device integrity requirements

The device integrity requirements are the following:

- No combination of the interlocks shall prevent the device command going to its safe position when requested;
- No combination of the interlocks shall delay the SOV command by more than 100 ms;
- No combination of the interlocks shall result in an undefined or unstable state of the physical device command;
- All transition conditions of the state machines shall be complete and exclusive;
- The actions of each condition of the state machines shall be defined.

B.4.3.2.3.2 SIF integrity requirements

The SIF integrity requirements are the following:

- No combination of the interlocks shall prevent the function from issuing a request to the AP typical of the SOV when the inputs are valid;
- No combination of the interlocks shall delay a request to the SOV by more than 100 ms;
- No combination of the interlocks shall result in an undefined or unstable state of the physical device command.

B.4.3.2.3.3 Interlocks between SIFs integrity requirements

The SIF integrity requirements are the following:

- No combination of the interlocks or demands shall result in a simultaneous demand on SIF 02.01 and SIF 06.02.

B.4.3.3 Application program functional architecture design

B.4.3.3.1 Architecture design

The AP architecture design activity has to ensure:

- that the resulting architecture will comply with IEC 61511-1:201612.4.4;
- that the resulting architecture will not in any way degrade the systematic integrity of the hardware architecture described in the SRS;

The AP architecture will be based on a hierarchical structure. The following levels and AP modules are considered:

- AP typicals for the devices: in this example, we will consider solenoid valves; pressure and temperature sensors. These modules contain the logic relevant for: device control, input acquisition and handling, standard complex functions such as voting;
- SIF logic: interlocking of AP modules to realize the expected behavior of each SIF;
- Plant logic: interlocking of SIFs.

These AP modules are described by the means of the graphical language of the model checking workbench environment in models reflecting the expected behavior of the AP modules to be developed. All these modules represent the final AP to be produced for the SIF and can potentially be directly compiled and downloaded in the targeted logic solvers.

The list of the necessary modules (limited to this example) is:

- SOV typical;
- 2oo3 voting;
- network communication handling;
- sensor handling;
- SIF 02.01 logic;
- SIF 06.02 logic.

All the modules are integrated together according to the structure described in Figure B.9.

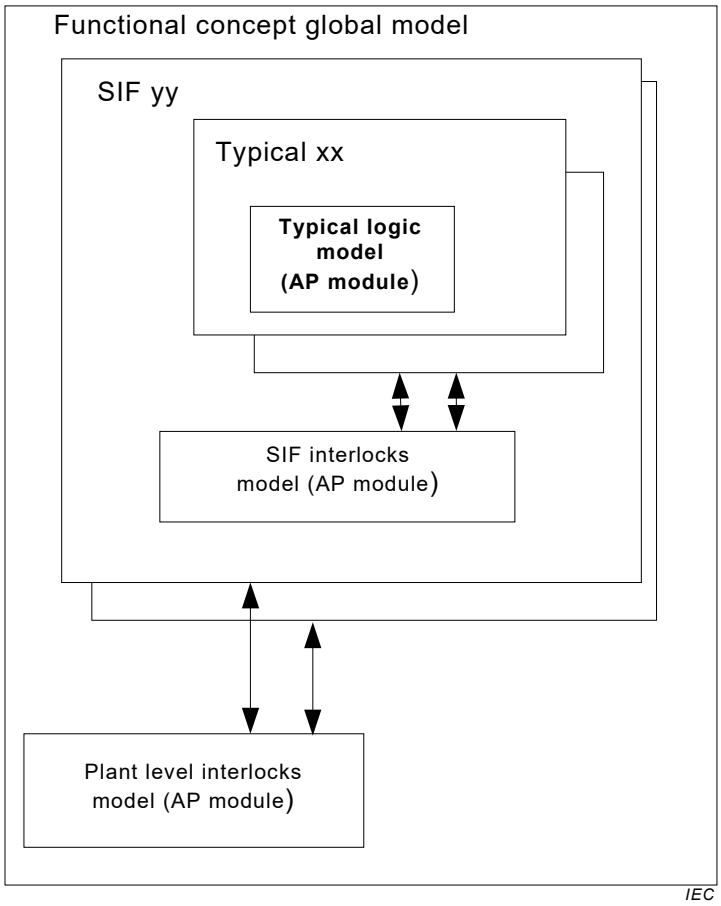


Figure B.9 – Hierarchical structure of model integration

B.4.3.3.2 Architecture derived safety integrity requirements

B.4.3.3.2.1 General

This architecture should not in any way jeopardize the systematic safety integrity of the physical hardware architecture defined in B.4.3.3.1.

This issue is not discussed more extensively here as it is directly dependent on the characteristics of the selected logic solvers. But as a minimum, it appears that for SIF 02.01, there will be the need for an analysis of the consequences of distribution of the AP modules between CPU 1 and CPU 2 on the systematic integrity of the SIF. This will request an analysis of the combinations of the failure modes of the hardware with those of the AP. This is usually done by the means of failure trees including the intrinsic failures of AP modules (independent of the hardware hosting them) aiming at determining if there exists a single point of failure undermining the HFT.

In addition, the definition of the AP architecture allows to define the derived AP SRS that have to be allocated to each AP module.

B.4.3.3.2.2 Device integrity requirements

Derived requirements:

- All transition conditions of the state machines shall be complete and exclusive.
- The actions of each condition of the state machines shall be defined.

B.4.3.3.2.3 Safety Instrumented function integrity requirements

Derived requirements:

- No combination of the dynamic value of the variables interfacing a SIF interlocks to its related modules shall result in an undefined or unstable state of a SIF.

NOTE This requirement is not repeating B.4.3.3.1 requirement. B.4.3.3.1 is related to the functional static behavior of the logic. This requirement is now related to the dynamic behavior of a logic spread over 2 CPUs and arises from the architecture design.

B.4.3.3.2.4 Plant level integrity requirements

No derived requirement.

B.4.3.4 Application program functional design, modelling and testing

B.4.3.4.1 Application program modules functional models design and testing

The necessary AP modules identified in the AP architecture are modelled in the model checking workbench development environment. In parallel, models are built to describe:

- the behavior of the physical devices;
- the behavior of the man machine interface;
- the required safety properties of the devices;
- the required safety properties of the SIFs;
- the required safety properties at the plant level;
- the plant physical behavior (interlocking by the process fluids);
- the BPCS part of the logic.

This is necessary to allow proving the required properties of the modelled SIFs in front of their functional and physical context.

All the AP modules are integrated together in a functional checking model according to the structure described in Figure B.10.

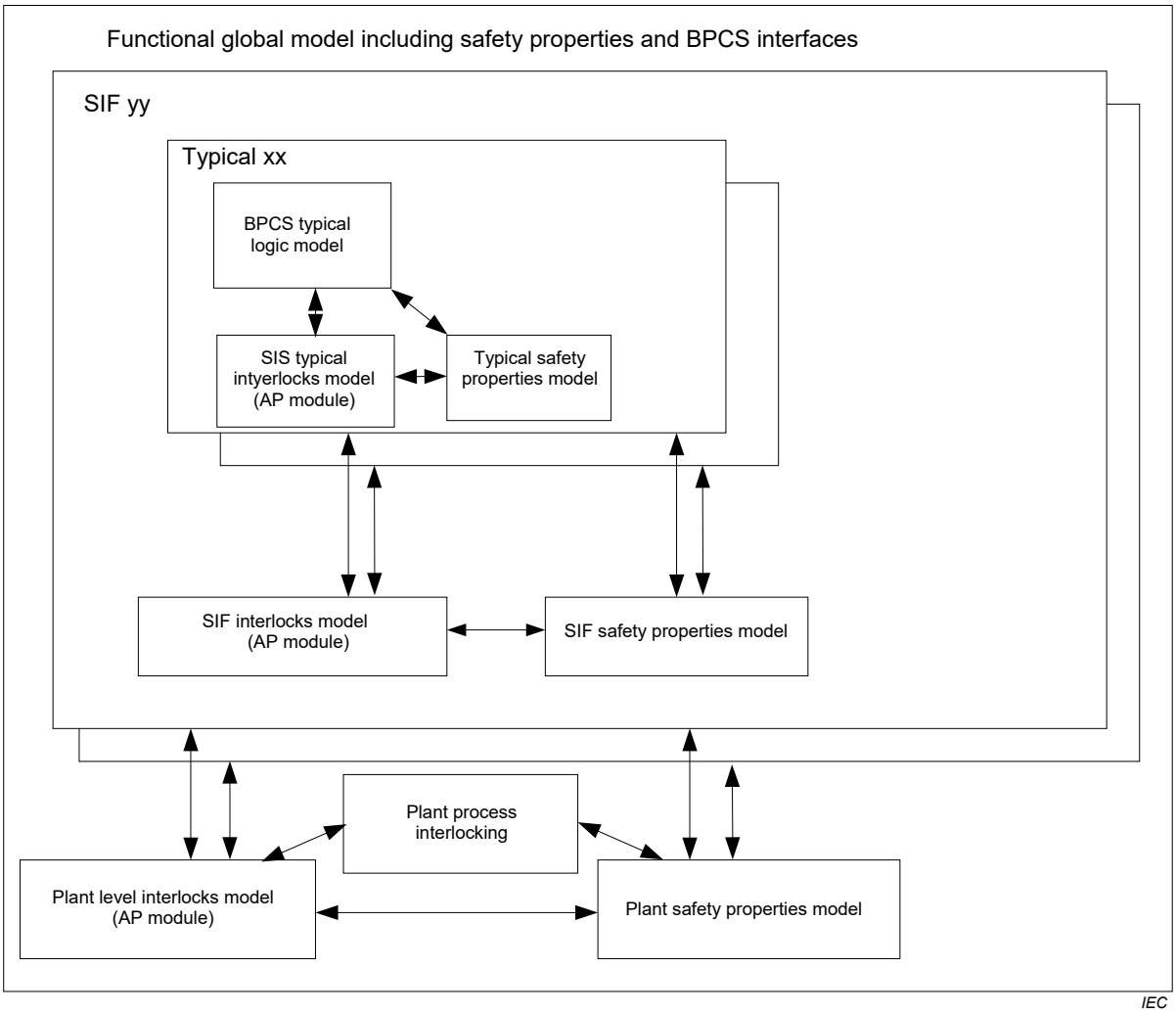


Figure B.10 – Hierarchical structure of model integration including models of safety properties and of BPCS logic

B.4.3.4.2 Models description

B.4.3.4.2.1 Application program typicals level

SOV BPCS control logic model:

The refining of the modes of operation of Table B.1 requirements results in the detail design of the SOV control logic specified by means of a state machine diagram.

An example of a state transition table is given in Table B.2.

Table B.2 – State transition table

States/Next states	Transition condition	Action
Requested		
Distance	!12HS1234D	
Distance		
Requested	12HS1234D	
Site	12HS1234B ∩ !12HS1234D	

States/Next states	Transition condition	Action
Disabled	12HS1234A ∩ !12HS1234D ∩ 12ZSL1234	
Site		
Requested	12HS1234D	
Distance	12HS1234C ∩ !12HS1234D	
Disabled	12HS1234A ∩ !12HS1234D ∩ 12ZSL1234	
Disabled		
Requested	12HS1234D	
Distance	12HS1234C ∩ !12HS1234D	
Site	12HS1234B ∩ !12HS1234D	

The state transition Table B.2 results in the state transition diagram Figure B.11.

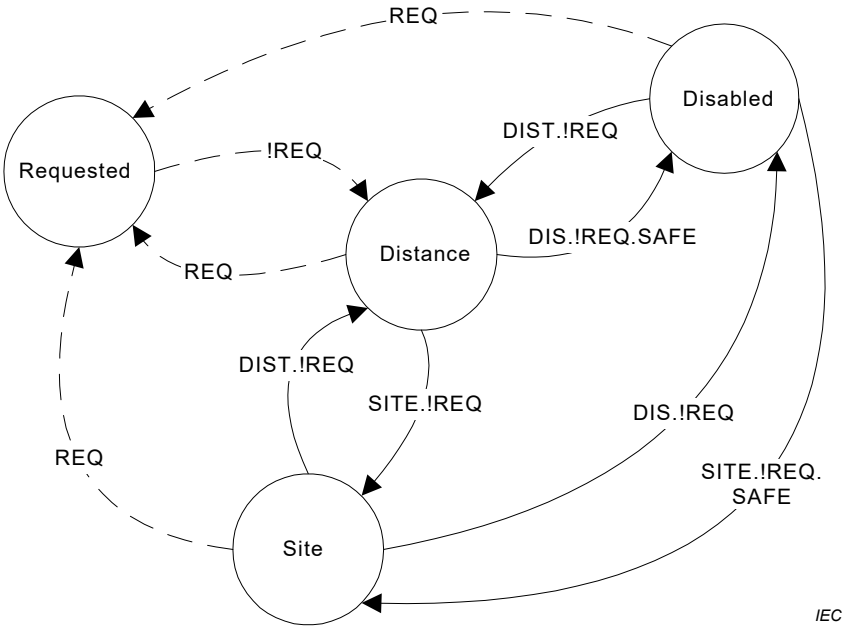


Figure B.11 – State transition diagram

The graphic specification of the behavior of the SOV in compliance with Figure B.6 interface requirements and with Figure B.11 results in the Figure B.12 function block description.

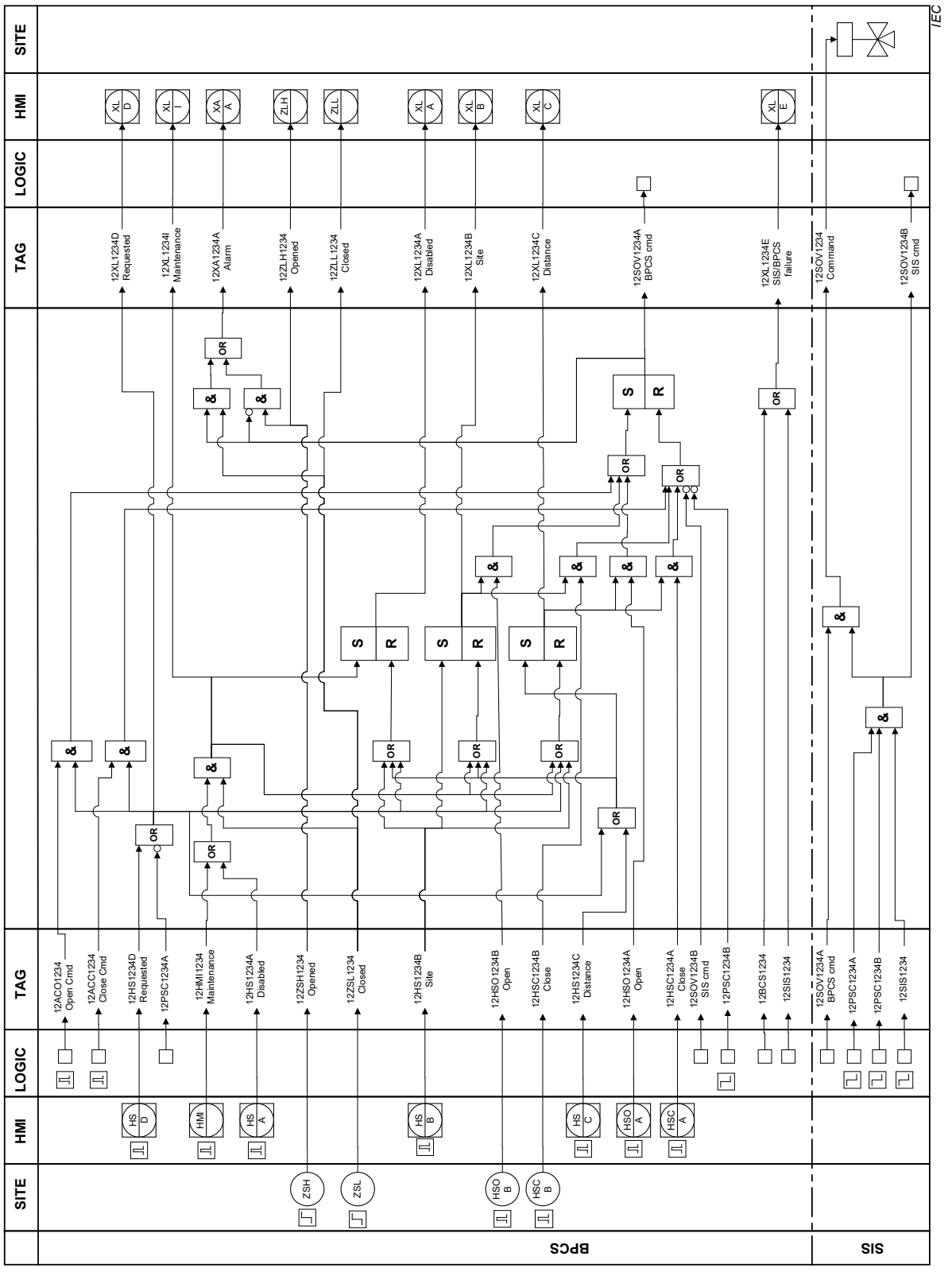


Figure B.12 – SOV typical block diagram

The HMI functions and interfaces need not be modelled as they are only outputs and will have no effect on the SOV behavior. Figure B.12 can thus be simplified in the Figure B.13 representation.

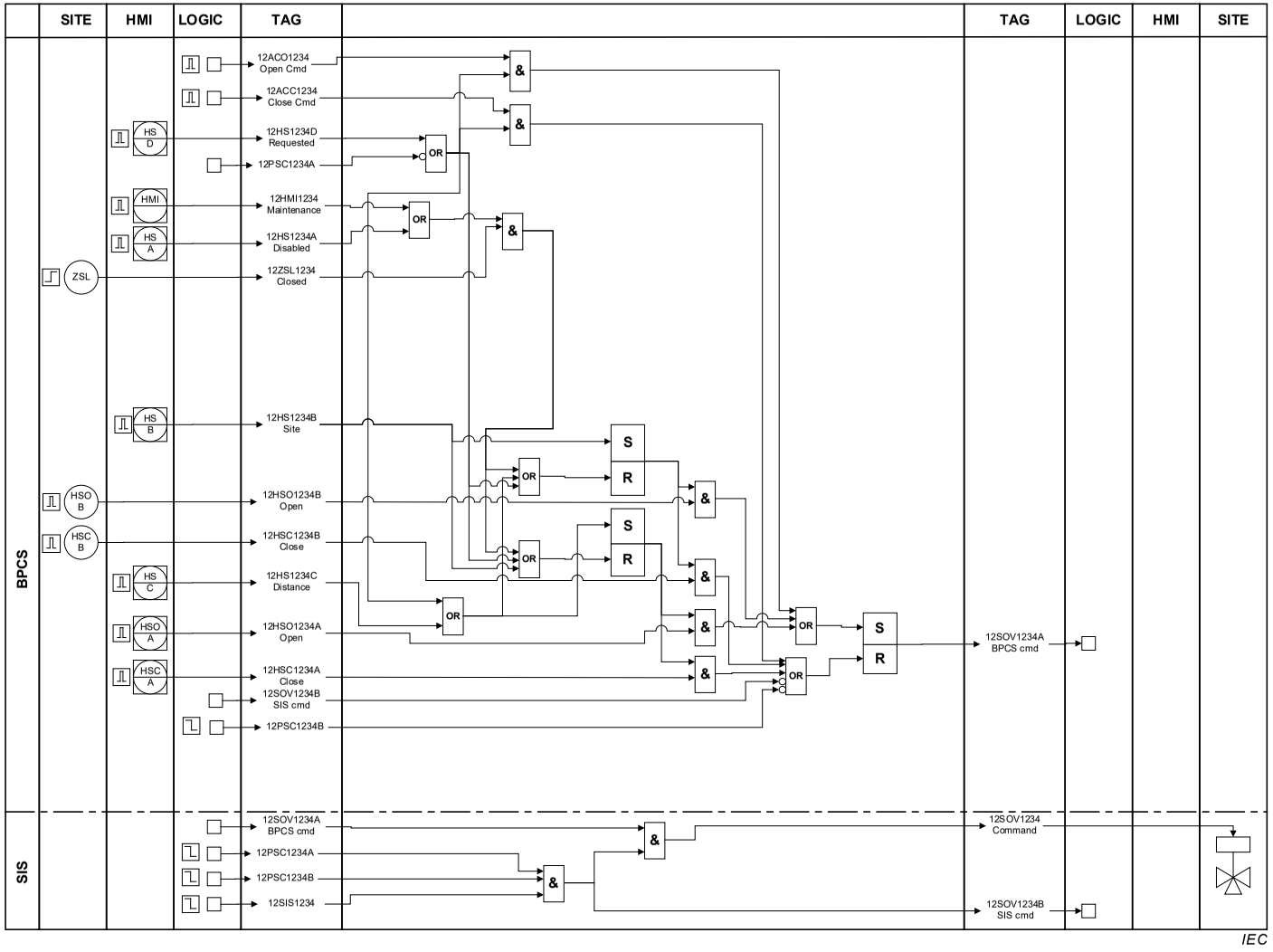


Figure B.13 – SOV typical model block diagram

Figure B.13 specification should be implemented in the graphical language of the model checking workbench environment. The implementation takes into account the need to segregate the part of the logic related to the BPCS and the part related to the SIS. This implementation results for instance in the one described in Figure B.14 for the BPCS part and in Figure B.15 for the SIS part. The modelling of the BPCS part is needed in particular when an interface exists between the BPCS and the SIS in order to prove the independence of the SIF from the BPCS and to prove safety integrity requirements such as the fact that in no case the BPCS can inhibit the SIF. Most of the model checking workbenches allow to directly realise the model implementation without the need of the step described in Figures B.12 and B.13 that were provided here for the clarity of the demonstration.

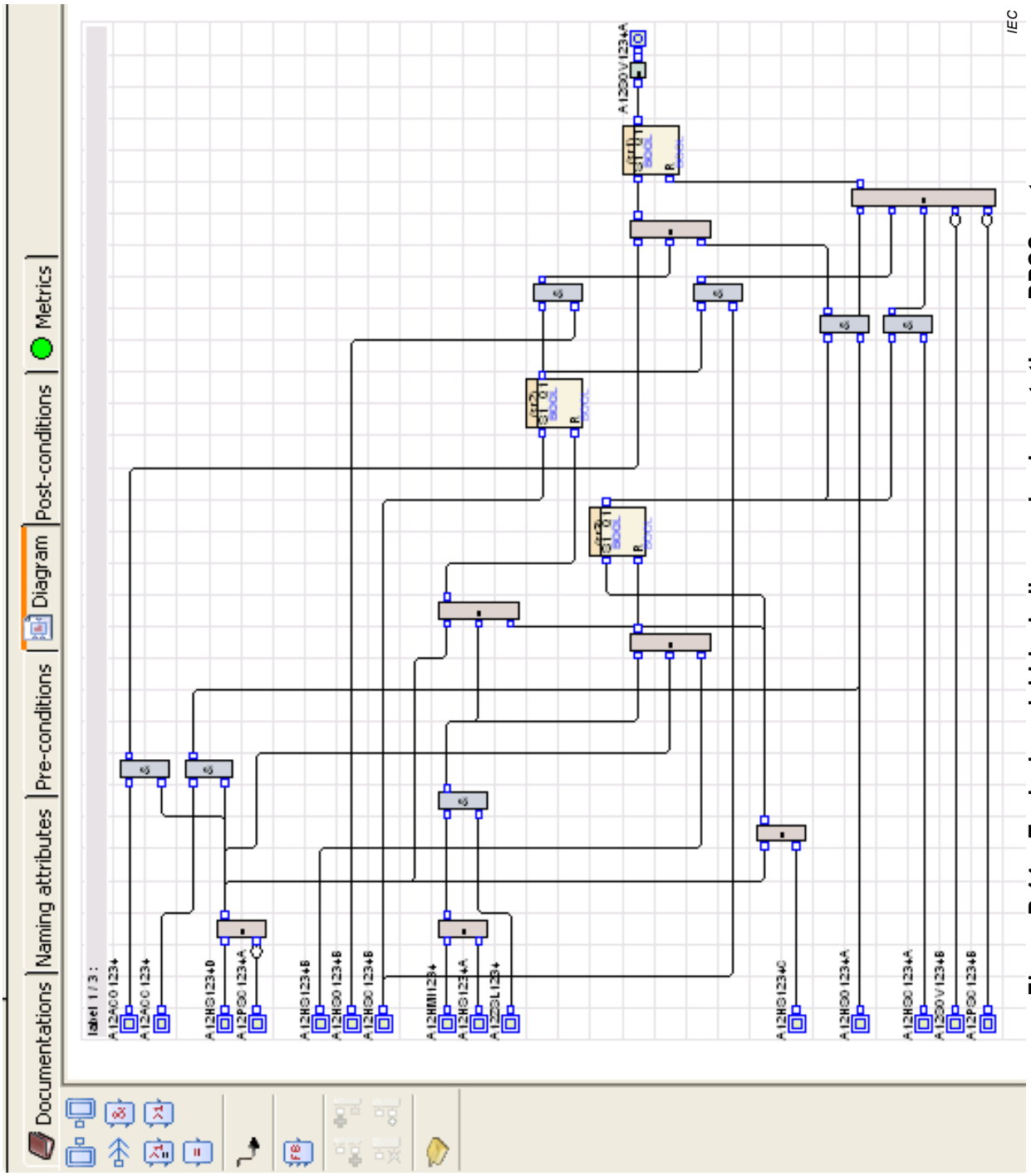


Figure B.14 – Typical model block diagram implementation – BPCS part

SOV SIS control logic model implementation

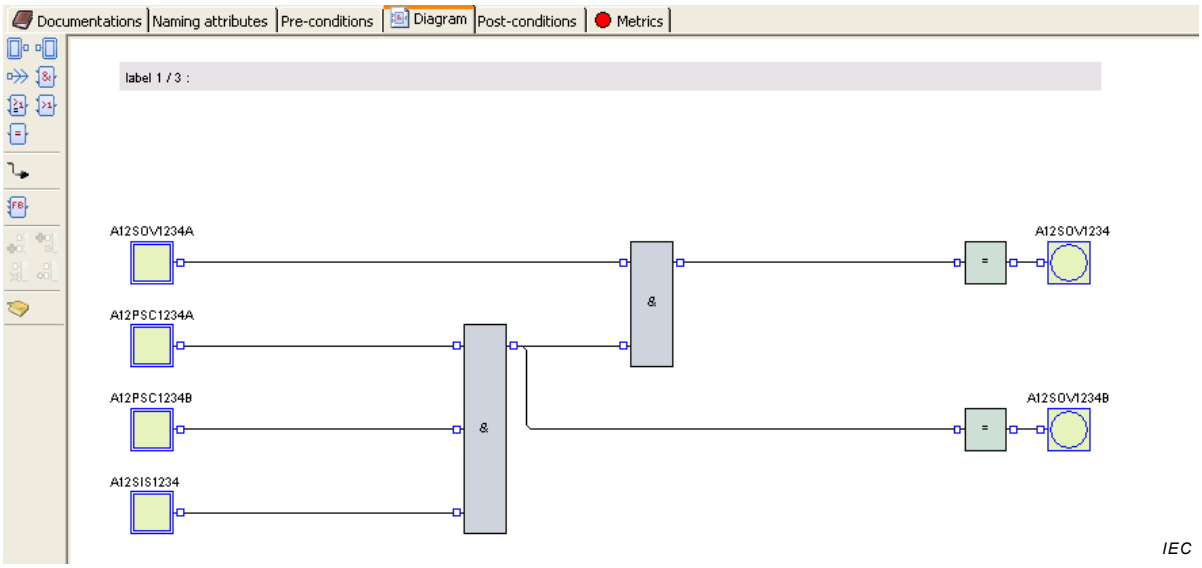


Figure B.15 – SOV application program typical model implementation – SIS part

Modelling continuation:

The same approach is followed to model:

- The safety properties of this SOV;
- The other necessary typicals that would be in this example:
  - 2oo3 voting;
  - 2oo3 safety properties;
  - network communication handling;
  - network communication safety properties;
  - sensor handling;
  - sensor safety properties.

B.4.3.4.2.2 Safety instrumented function level

The same approach applies at SIF level to model:

- SIF 02.01 interlocks model;
- SIF 02.01 safety properties model;
- SIF 06.02 interlocks model;
- SIF 06.02 safety properties model.

B.4.3.4.2.3 Plant level

The same approach applies at SIF level to model:

- plant interlocks model;
- plant safety properties model;
- plant model.

B.4.3.4.3 Models testing results and defect correction

The models are independently run by the model checking tool in order to detect safe behavior violations. If errors are found by the model checker the concerned models are corrected and run again until they are free from these systematic design faults.

B.4.3.5 Application program integration modelling and testing

The previous steps have enabled the AP engineer to:

- describe an AP architecture;
- describe the functional AP modules content;
- demonstrate that the architecture and the modules specifications were:
  - compliant with AP functional specifications;
  - compliant with AP safety integrity specifications.

This is not sufficient to demonstrate that the AP concept is viable when integrated on the targeted physical hardware architecture because the functional behavior of the AP will depend also on the characteristics of the physical hardware architecture.

This design phase consists in adding models describing the impact of the distribution of the AP in the targeted hardware physical architecture in order to check that the SRS are still met. If it is the not case, the AP modules and/or the AP architecture and/or even the physical architecture would be modified. The step of Figure B.10 can skipped if the physical hardware architecture is known early during AP development life-cycle.

The following models are developed and added to the checking model within the following structure as described in Figure B.16.

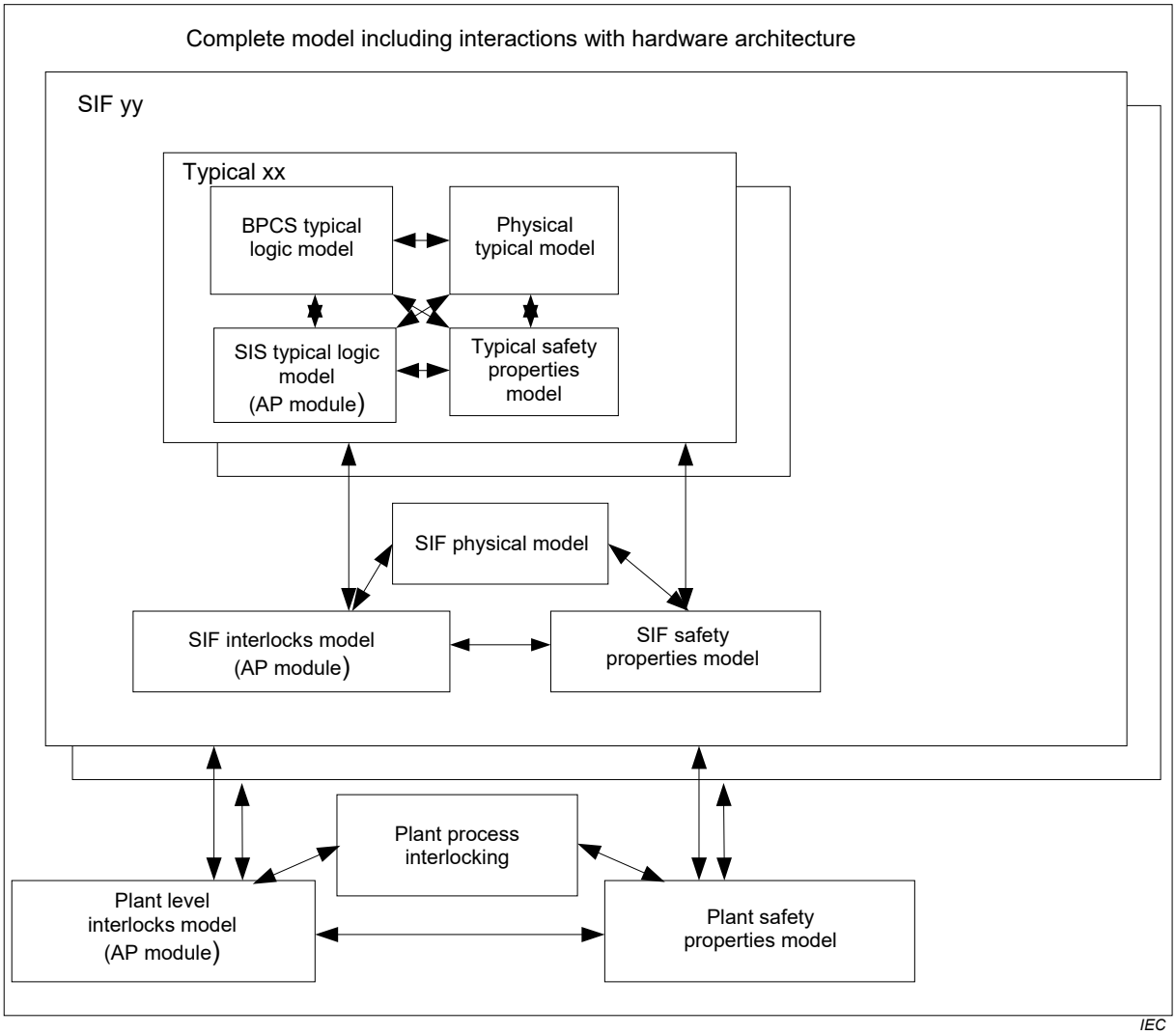


Figure B.16 – Complete model for final implementation model checking

B.4.4 Application program production

Some AP workbenches allow direct downloadable code generation from the models previously checked. Some are, in addition, IEC 61508 compliant.

B.4.5 Application program verification and testing

When it is not possible to automatically generate a downloadable code from an IEC 61508 compliant or prior use tool, the AP is manually generated and tested.

B.4.6 Validation

For an AP generated automatically from the models with a tool compliant with IEC 61511-1:201612.6, the validation consists in verifying through an analysis of the model checker documentation that all functional and safety integrity properties described in the AP SRS have actually been demonstrated.

For a manually generated AP, the validation consists in verifying that the implementation strictly follows the assumption of the models and that all functional and safety integrity properties described in the AP SRS have actually been demonstrated by the tests.

Annex C
(informative)

Considerations when converting from NP technologies to PE technologies

Many process sector facilities utilise electrical or solid state devices for their SIS design. These facilities may desire to capture the advantages offered with PE technology and as such plan on modification of, or addition to their SIS(s) with the use of PE devices. Some considerations that the facility may consider prior to and during this transition include:

a) PE devices for SISs should not be used unless the plant can successfully verify, validate, utilize, operate, and maintain PE devices in their BPCS;

b) PE devices for SISs should not be used unless the plant has the capability to utilize, design, modify, and maintain AP for PE devices;

c) A review should be carried out to determine what can be transferred from the existing plant application capability to the SIS AP, such as:

- skills and experience (e.g., programming experience, capability, availability); Portability of on-site AP skills to the SIS; management familiarity and involvement with PE support;
- security capability as it relates to allowing access (local and remote);
- application language use in existing facility;
- modules (e.g., existing control algorithms such as motor start/stop/try, comparison of actual position to position command status);
- real time response and delays moving from hardwired to PE systems;
- interfaces (e.g., existing, proven, reliable interfaces to DCS, HMI, networks, electrical interfaces, timing);
- documentation (e.g., capable of providing functionality to clearly describe the AP to maintenance personnel/operators);
- support to trouble-shoot the PE and AP 24/7;
- coverage (availability of support 24/7);
- response (e.g., time to problem resolution);
- simulator (e.g., for off-line AP analysis, modification, development, training);
- testing capability (e.g., plant testing approach and capability versus testing needs of the AP);
- operator experience (with PE and AP);
- plant bypass procedures (and their realization and control using application programming);
- conversion of the plant HMI solution from NP to PE technology;
- training (availability , coverage of application programming, HMI);
- tools (e.g., programming, development, testing); support for utility software;
- management support (existing, sufficient, awareness of need by all parties);
- management of change procedure, including control over modifications to the AP, secure storage and configuration management and provision for re-validation where changes have been made or can affect the AP;
- future enhancement/upgrade/obsolescence of the system(s);
- corporate/plant application programming standards and promulgation of industry codes of practice;

- compatibility with “sister” PE solutions for interchangeability of experience, processes, equipment etc.

Annex D
(informative)

Example of how to get from a piping and instrumentation diagram (P&ID) to application program

Annex D illustrates how an oil and gas separation process was evolved from a P&I diagram to an AP. Figure D.1 illustrates the P&I diagram. Figure D.2 illustrates the expression of the safety functions by means of a cause and effect diagram. Figure D.3 shows the conversion of the cause and effect diagram to the AP using function block programming.

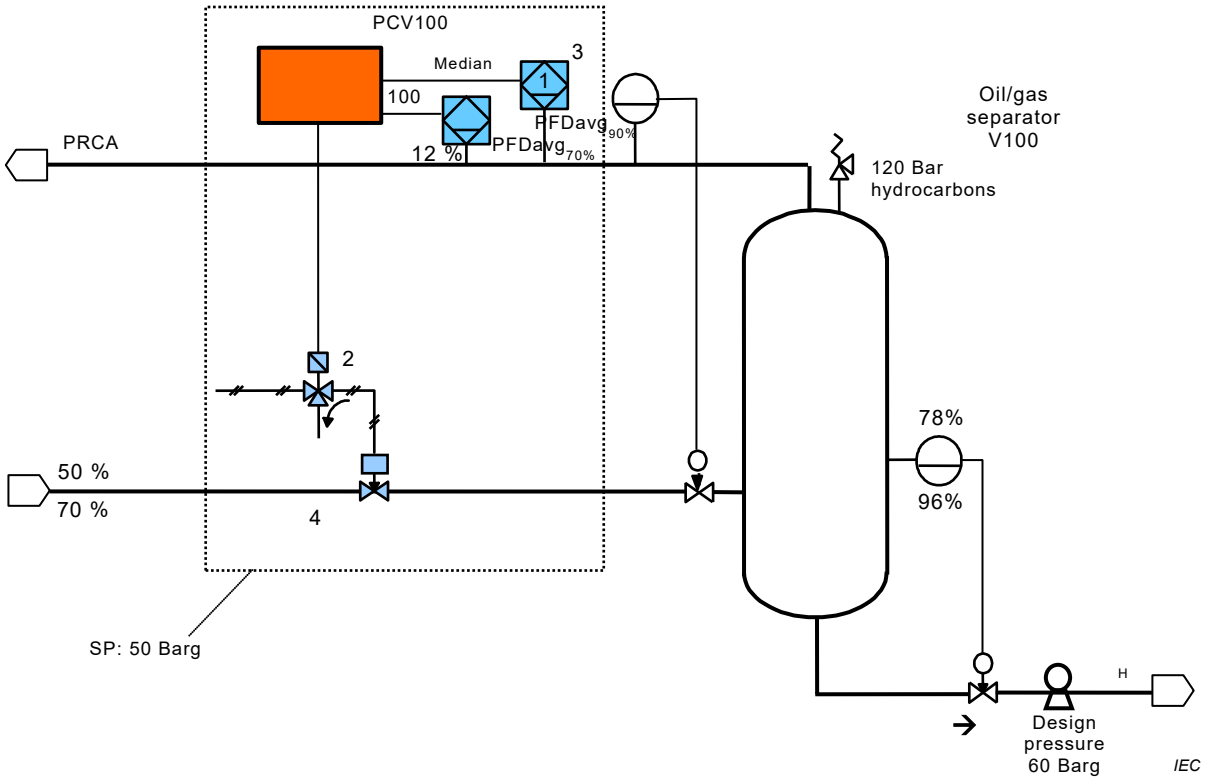


Figure D.1 – Example of P&ID for an oil and gas separator

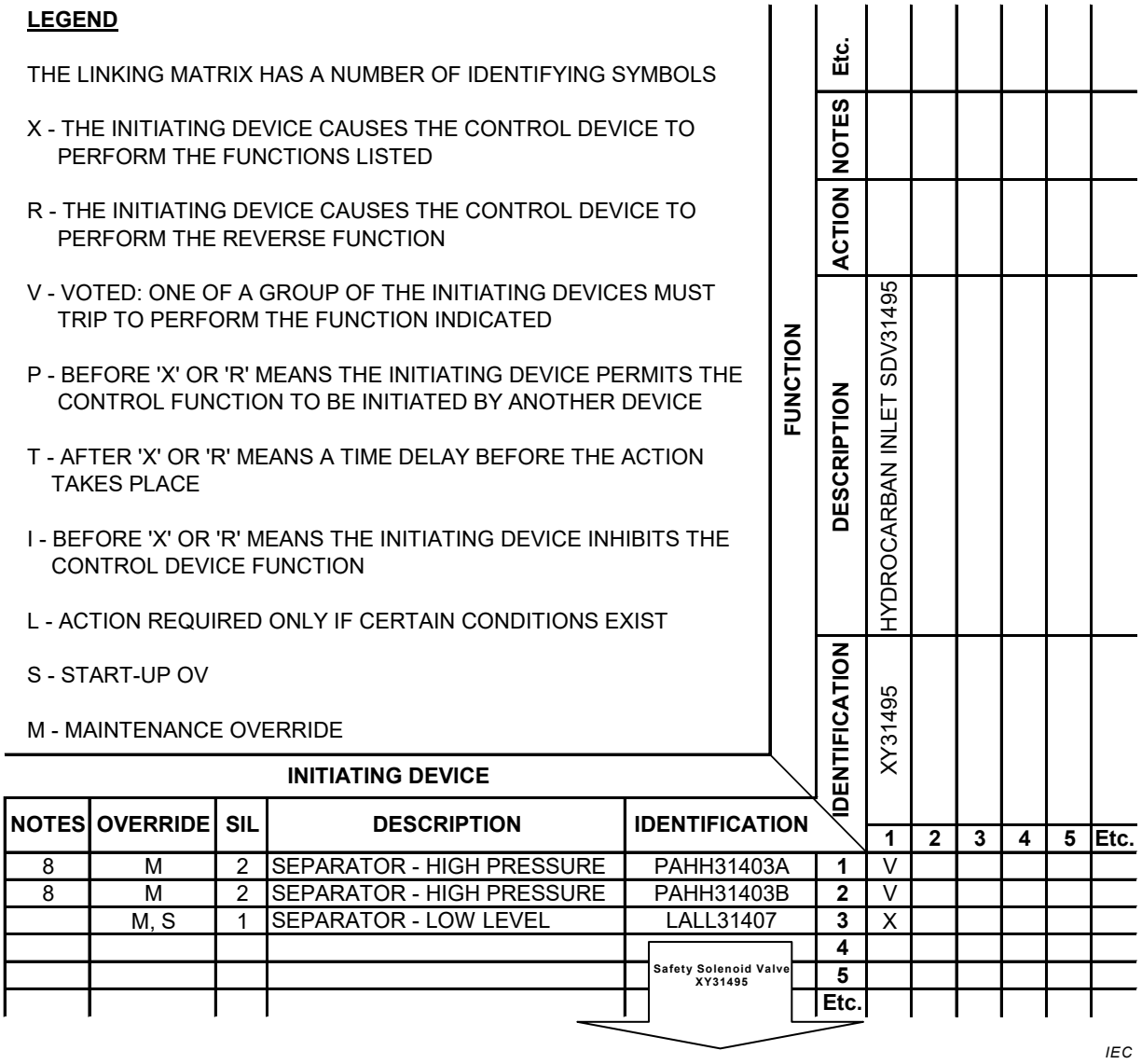


Figure D.2 – Example of (part of) an ESD cause & effect diagram (C&E)

Below is an example of an AP for a SIF with two 1oo2 voted analogue signals from pressure sensors and a digital output to a single final element. The safety concept is DTS (de-energize to safe state). The program language is Function Blocks.

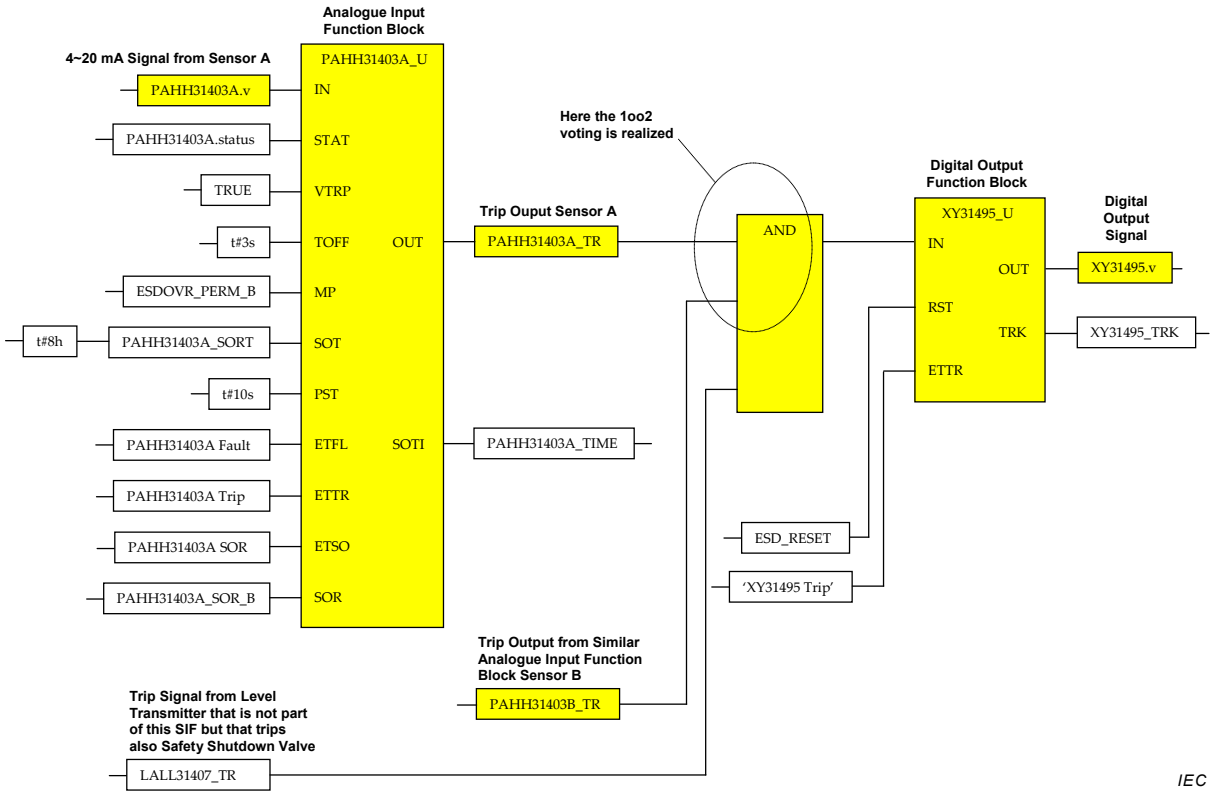


Figure D.3 – Example of (part of) an application program in a safety PLC function block programming

Annex E
(informative)

Methods and tools for application programming

E.1 Typical toolset for application programming

Typically, the toolset supporting the PE programming will include the following capabilities:

a) Configuration editor. This editor is used to configure the I/O SIS subsystem, the I/O memory variables, and communication functions.

b) Language editors. These editors are used by the application programmer to develop the programs that perform all the functions needed by the system (safety and non-safety).

c) Libraries of previously assessed functions and function blocks. These functions and function blocks can be used in the APs.

d) Custom function and function block development capability. Some suppliers provide a development environment that allows the user to develop custom functions and function blocks that can be used by the supported application languages. These custom functions and function blocks should be thoroughly tested prior to use in the AP.

e) AP scheduling facility. These scheduling facilities support the setting of the order of desired execution sequence and their scan rates.

f) Downloading capability. This allows the developer to download the AP, function block libraries, variable data and other configuration information into the logic solver hardware for execution.

g) Emulation capability. Some suppliers provide a development environment with the capability to emulate all of the APs on the computer that supports the development environment. This allows thorough off-line testing of the APs before they are downloaded into the logic solver.

h) Program monitoring capability. The monitoring capability allows the user to view data from the executing program on user-defined screens or on the actual function block or ladder diagram program screens. The development environment may also provide the capability to monitor the execution of the emulator. In addition, the programs executing in the logic solver can be monitored.

i) Diagnostic displays of the logic solver. These displays show the status of the main processor modules, communication modules, and the I/O modules in the system. Typically, the pass, fail, active status of each module is shown; and in many cases, more detailed information about faults in the system is available.

The PE system will be supported by a programming environment that supports the coding of the AP, the configuration of application parameters and interfaces and the testing/ monitoring of the AP execution. Many PE systems intended for use in safety applications will be supported by a dedicated set of tools, together with a manual which will describe how to use the tools to ensure that the AP achieves the intended integrity. The design environment and application language should possess features that facilitate:

- abstraction, modularity and other features which control complexity; wherever possible, the AP should be based on well-proven modules that may include user library functions and well-defined rules for linking the modules;
- expression of:
  - functionality, ideally as a logical description or as algorithmic functions;
  - information flow between modular devices of the application functions;
  - sequencing requirements;
  - assurance that SIF always operate within the defined time constraints;

  - freedom from indeterminate behavior;
  - assurance that internal data items are not erroneously duplicated, all used data types are defined and appropriate action occurs when data is out of range or bad;
  - design assumptions and their dependencies.
- comprehension by developers and others who should understand the design, both from an application functional understanding and from a knowledge of the constraints of the technology;
- verification and validation, including coverage of the AP, functional coverage of the integrated application, the interface with the SIS and its application specific hardware configuration;
- AP modification. Such features include modularity, traceability and documentation.

E.2 Rules and constraints for application program design

Following is a list of items to consider when developing APs for SISs:

a) break the AP into discrete SIF with a SIL for each SIF;

b) understand the hardware architecture of each SIF and duplicate this hardware architecture in each SIF AP;

c) do not optimize the AP if this leads to excessive complexity (this often requires an advanced programmer to interpret the AP);

d) use AP development techniques from the vendor instructions (e.g., safety manual);

e) do not combine AP from one SIF with any other SIF;

f) use AP language (e.g., type, function) in which the facility is trained, capable of understanding and troubleshooting;

g) provide a written description of the AP consistent with the functional description, located with the AP documentation;

h) modularize the AP consistent with the process flow (e.g., the first module is common AP which is not SIF related but which is required in the SIS, the second module is the first SIF located at the process inlet, the last module is the last SIF located at the process outlet);

i) thoroughly test (e.g., simulate, inspect, review) each AP module and obtain second independent analysis (include the operating and maintenance department here and in all subsequent steps);

j) thoroughly test the combination of modules that make up a process SIS subsystem and obtain second independent analysis;

k) thoroughly test the SIS AP and obtain second independent analysis;

l) utilize AP when checking out the hardware (e.g., confirming I/O connected to correct sensor/final element);

m) include testing of the AP in the run-in (e.g., process operation without hazardous material) of the process;

EXAMPLE End-to-end checks in communications links, bounds checking on sensor inputs, bounds checking on data parameters and diverse execution of application functions.

n) AP support team members are to be available during process turnover to facility (e.g., commissioning);

o) No interlocks between SIF.

E.3 Rules and constraints for application programming

Following are some PE logic solver application programming rules that should be considered and the validity will depend on the application:

a) Do not use SKIP and JUMP functions;

b) Do not use NOT functions;

c) Do not use indirect addressing;

d) Do not use compression algorithms;

e) Do not use of logic based on arithmetic calculations results;

f) Do not use logic with internal state memory (e.g., flip-flop memories);

g) Do not use text variables in SIF;

h) Do not use functions or subroutines that include variable or parameter transmission;

i) Do not customize library functions;

j) Do not use interruptions;

k) Do not use latching;

l) Do not use compression of Boolean variables inside integer variables;

m) Do not inverse the sensors or actuator physical state in the logic;

n) Do not partition a SIF interlocks over several logic solvers;

o) Do not use network communication functions other than passive functions

p) Do use plant approved, safety assessed programming methods;

q) Do use standardized modules (e.g. ‘’typicals’’);

r) Do provide device alpha-numeric descriptors that provide task description and cross-referencing for each sensor, final element (e.g., solenoid valves, valves, motors, alarms), SIF, etc. consistent with and related to design drawings (e.g., P&I diagrams, arrangement drawings, logic diagrams);

s) Do use plant approved and previously assessed logic solver pre-programmed safety functions (e.g., emergency stop, light curtains, safety gates);

t) Do separate PE logic solver programming into three separate areas, input circuit, logic circuit, output circuit:

   – Input circuits should be drawn vertically in a ladder diagram format which each rung having a sensors on the left and input modules on the right; each sensor should be wired discretely;

   – Logic diagrams should be drawn vertically in a ladder diagram (or appropriate LVL) format with each rung having inputs on the left and an output on the right;

   – Output diagrams should be drawn vertically in a ladder diagram format which each rung having a logic solver output on the left and a final element on the right; each final element should be wired discretely;

u) The design approach should normally be de-energized to trip to a safe state; for systems requiring energize to trip special precautions will be required;

v) The logic solver I/O addressing and the logic solver programming should be arranged to mirror the process application (e.g., the initial programming and I/O assignments should be related to the application start cycle and continue in its development in the same format as the process flow dictates, ending with the stop function).

w) Support functions, such as proof testing, manual control, bypass, alarms, and diagnostics, should be identified as such and separated from the SIF;

x) Provide the necessary spare I/O, memory and processing capacity so that the clarity of, and the capability to, provide necessary application programming is maintained during future modification/expansion requirements;

y) Diagrams should have cross referencing to the location of multiple uses of any component by the AP (e.g., input, output, internal register);

z) Ensure that the order of processing within the AP meets the real time response.

Annex F
(informative)

Example SIS project illustrating each phase of the safety life cycle with application program development using relay ladder language

NOTE This example is used with permission from ISA and AIChE CCPS, *Guidelines for Safe Automation of Chemical Processes*, New York, 1993, available from: AIChE, 345 East 47th Street, New York, NY 10017, Tel: (212) 705-7657.. The example is modified to meet IEC 61511 requirements.

F.1 Overview

The example in Annex F is provided to illustrate how to apply each phase of the safety life-cycle implementation using ladder logic in compliance with IEC 61511 series.

This is the 3rd edition of this example. The 1st edition was issued by CCPS prior to IEC 61508 and IEC 61511 issue. The 2nd edition was issued by ISA (TR84.00.04, part 2) which adhered to the 1st editions of IEC 61508 (2000) and IEC 61511 (2003). This 3rd edition adheres to IEC 61508 (2010) and IEC 61511 series. In addition, this example has been partitioned consistent with the steps in the IEC 61511-1:–, Figure 7 safety life-cycle.

It is intended to demonstrate one method to meet the requirements of IEC 61511. The reader should be aware that IEC 61511 series is performance based, and that many approaches can be used to achieve compliance. Some of the methods applied in this example include: what-if and HAZOP techniques for H&RA, LOPA for allocation of safety functions to protection layers, fault tree analysis for SIL verification, and ladder logic to document the AP requirements. Other techniques and tools could be utilized at each of these steps in the SIS safety life-cycle to meet the requirements of the standards.

The example utilizes the similar chemical process presented in CCPS AIChE, *Guidelines for Safe Automation of Process Applications*, 1993.

This example selects a SIS subsystem of a process and applies to it the design philosophy, procedures, techniques, and verification methodology discussed in IEC 61511.

This example shows cradle (concept)-to-grave (decommissioning) documentation for each SIF. This documentation pedigree gives auditors and plant personnel the means to track the SIF through the SIS safety life-cycle phases back to the process hazards analysis (PHA) that created it. Each SIF is clearly identified in each document to facilitate tracking between life-cycle phases. A vital part of safety is the ability to demonstrate to others (e.g., auditors, regulators, insurance companies) that the risk reduction provided by each SIF is adequate.

This example does not represent a complete design for a polymerization process because of the extensive detail that is required to achieve a high-integrity, safely automated design. As a result, this example includes a number of simplifications.

All references shown refer to information within this example unless otherwise noted.

F.2 Project definition

F.2.1 General

The process is the polymerization of vinyl chloride monomer (VCM),

$$CH_2{=}CHCl$$

to make polyvinyl chloride (PVC),

$$[{-}CH_2{-}CHCl{-}]_n$$

The example involves an hazardous reactant, VCM, which is flammable and has toxic combustion products, as well as being a known carcinogen. The process also illustrates a larger-scale batch operation that operates in a semi-continuous manner during an approximately 10-hour period while the polymerization progresses. A simplified description of the process steps is also provided.

F.2.2 Conceptual planning

Once a business decision is made to consider producing a certain product – in this example, polyvinyl chloride – the initial project team is assembled. This team will start by evaluating potential process routes to identify a technology that will satisfy production needs while meeting responsibilities for health, safety, security, and protection of the environment.

F.2.3 Process hazards analysis

In the very early stages of process evaluation and project definition, a process hazards analysis team starts to interact closely with the designers. For projects handling hazardous materials, the team will include not only process design engineers but also health and safety specialists. The team should often have access to other specialists – such as chemists, operating personnel, consultants or engineering contractors having experience with the same or similar processes, and process licensors. In this example, a well-proven process is available as a starting point. Therefore, we will concentrate on the aspects of the design process that influence or directly involve the design of the process control systems and safety interlock systems. More detailed information on related aspects of the design process can be found in the following list of texts from the Center for Chemical Process Safety, American Institute of Chemical Engineers:

- *Guidelines for Hazard Evaluation Procedures;*
- *Guidelines for Chemical Process Quantitative Risk Analysis;*
- *Guidelines for Safe Storage and Handling of High Toxic Hazard Material;*
- *Guidelines for Vapor Release Mitigation;*
- *Guidelines for the Technical Management of Chemical Process Safety.*

F.3 Simplified process description

The manufacture of PVC from the monomer is relatively straightforward. The heart of the process is the reactor vessel in which the polymerization takes place over a period of about ten hours, while the reactor contents are agitated mechanically and the heat of reaction is removed by the circulation of cooling water through the reactor jacket. Because the process involves the charging of a batch to the reactor, process systems are designed with multiple reactor units in parallel, so that the process can operate on a semi-continuous basis. For simplicity, this example will focus on one of the units, recognizing that a real production facility will typically have several parallel units operating in sequence.

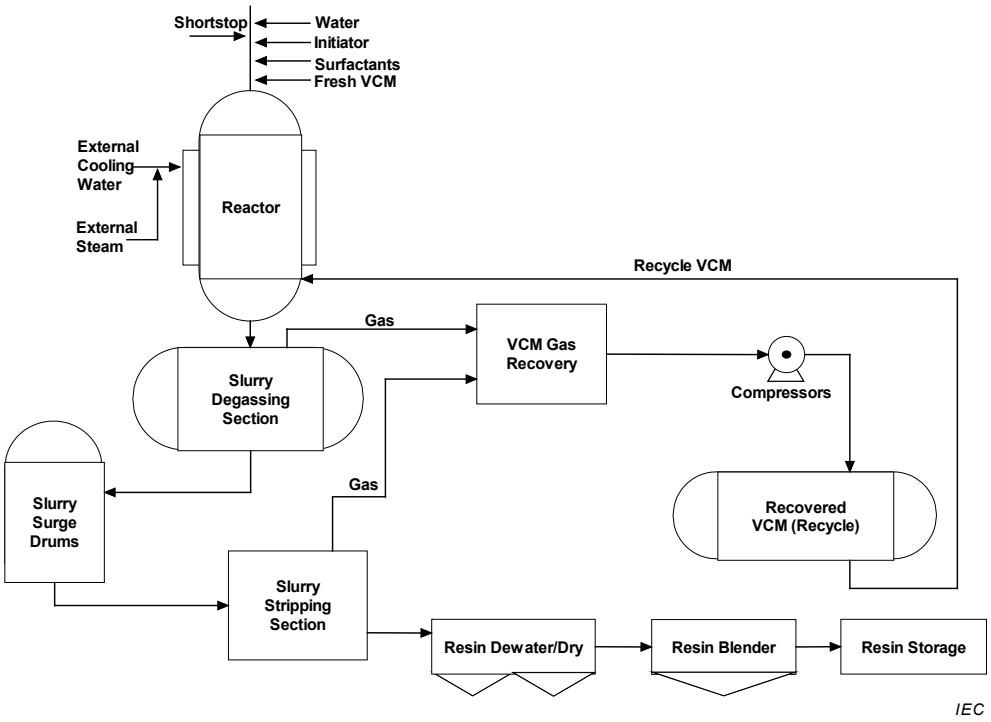


Figure F.1 – Simplified flow diagram: the PVC process

Figure F.1 is a simplified process flow diagram for a typical PVC manufacturing facility. If the reactor vessel has been opened for maintenance after the last batch was processed and dumped, it should first be evacuated to remove any residual air (oxygen) in the vapour space, to minimize the oxidation reaction of monomer which produces HCl and may lead to stress corrosion damage to the reactor vessel as well as to poor product quality. Otherwise, the first step is to treat the reactor vessel with anti-foulant solution to prevent polymerization on the reactor walls. This is followed by charging the vessel with de-mineralized water and surfactants.

Then, the liquid vinyl chloride monomer (VCM) charge is added at its vapour pressure (about 3,86 Barg at 21 °C – 56 psig at 70°F).

The reaction initiator is a peroxide that is dissolved in a solvent. Since it is fairly active, it is stored at cold temperatures in a special bunker. Small quantities are removed for daily use in the process and are kept in a freezer. It is first introduced into a small charge pot associated with the reactor to assure that only the correct quantity is added.

After the reaction initiator is introduced, steam-heated water is applied to the reactor jacket to raise the temperature to about 54,5 °C to 60 °C – 130 °F to 140 °F (depending on the batch recipe for the particular grade of product), where the reaction will proceed at a satisfactory rate. Agitation is necessary to suspend the VCM in the water (control particle size), improve heat transfer throughout the batch, and produce a uniform product. Since the reaction is exothermic, cooling water is then circulated through the vessel jacket to control the reactor temperature. Reactor conditions are controlled carefully during the approximately eight hours required for completion of the polymerization.

The reaction is completed when the reactor pressure decreases, signalling that most of the monomer has reacted. Reacted polymer is dumped from the reactor and sent to downstream process units for residual VCM recovery, stripping, dewatering, and drying.

F.4 Preliminary design

All special local requirements are reviewed, applicable regulations are identified, and general risk guidelines are established. Utility requirements (e.g., air, cooling water, electrical power) are reviewed and confirmed to be adequate for the application.

F.5 IEC 61511 application

F.5.1 General

When the preliminary planning is complete (see Clauses F.2 through F.4 inclusive), the implementation of IEC 61511 is begun.

For this example the design strategy is to initialize the life-cycle design (Figure F.2) and break down the life-cycle phases into ten steps consistent with Figure F.2 and Table F.1 (safety life-cycle overview). At this point in the project, it may be beneficial to use the life-cycle table to assign responsibility for each life-cycle phase as shown in Table F.1.

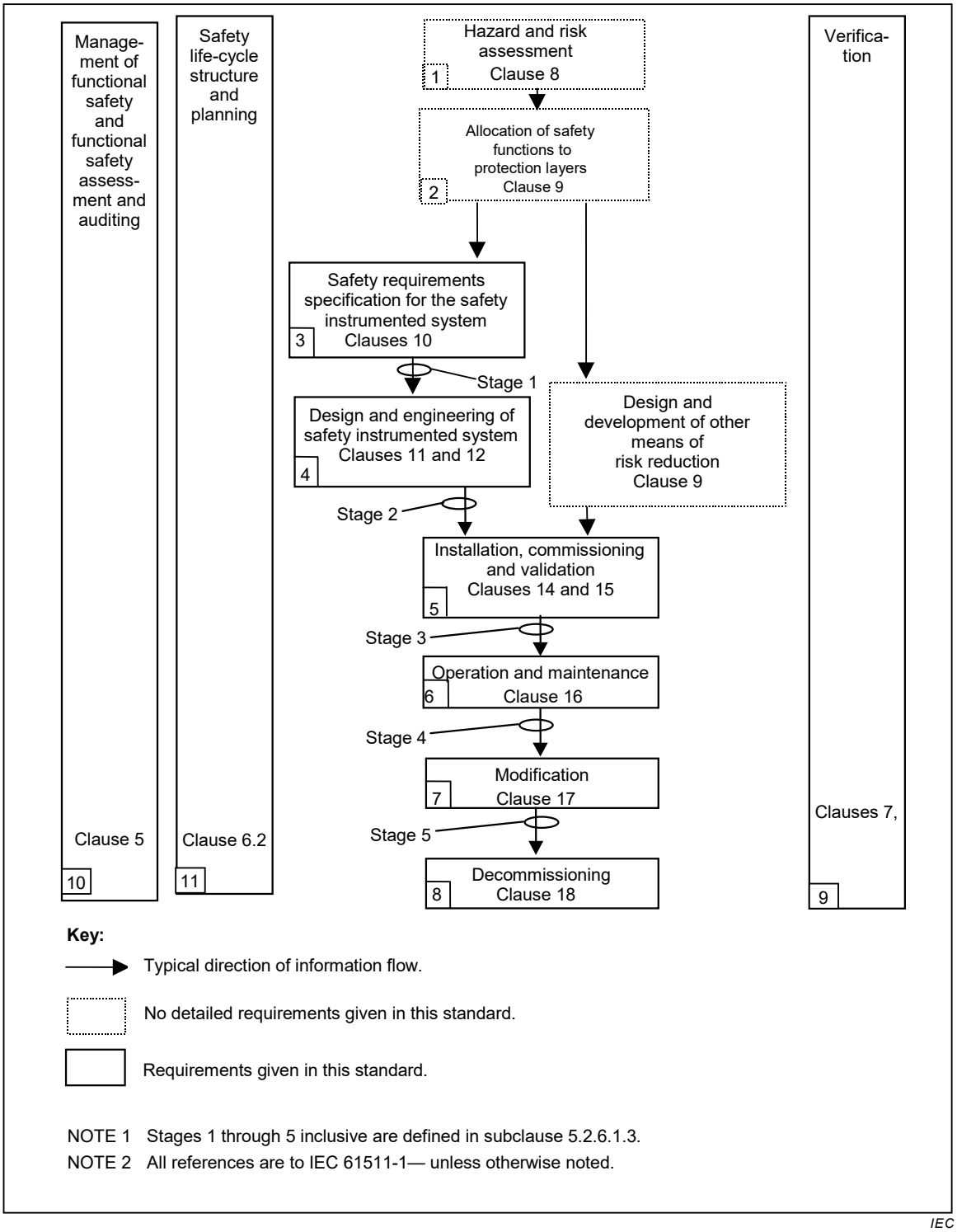


Figure F.2 – SIS safety life-cycle phases and FSA stages

Table F.1 – SIS safety life-cycle overview

Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs	Responsibility
Figure F.2 box #	Title					
1	H&RA	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction	PHA team See F.2.2
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL		A description of the required SIF and associated safety integrity requirements	Description of allocation of safety requirements (see Clause 9 of IEC 61511:—)	PHA team See F.2.2
3	SIS SRS	To specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety	10	Description of allocation of safety requirements (see Clause 9 of IEC 61511:—)	SIS safety requirements; AP safety requirements	E & I team
4	SIS design and engineering	To design the SIS to meet the requirements for SIF and safety integrity	11 and 12.4	SIS safety requirements; AP safety requirements	Design of the SIS in conformance with the SIS safety require-ments; planning for the SIS integration test	E & I team

Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs	Responsibility
Figure F.2 box #	Title					
5	SIS installation, commission-ing and validation	To integrate and test the SIS; To validate that the SIS meets in all respects the requirements for safety in terms of the required SIF and the required safety integrity	12.3, 14, 15	SIS design; SIS integration test plan; SIS safety requirements; Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS design results of SIS integration tests; Results of the installation, commissioning and validation activities	Construction
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	SIS requirements; SIS design; Plan for SIS operation and maintenance	Results of the operation and maintenance activities	Operations
	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modification	Operations
8	Decommission-ing	To ensure proper review, sector organization, and ensure SIF remain appropriate	18	As-built safety requirements and process information	SIF placed out of service	Operations
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.5	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase	Operations
10	SIS FSA	To investigate and arrive at a judgment on the functional safety achieved by the SIS	5	Planning for SIS FSA; SIS safety requirement	Results of SIS FSA	Operations

F.5.2 Step F.1: Hazard & risk assessment

See Life-cycle phase in Table F.2 below.

Table F.2 – SIS safety life-cycle – Box 1

Overview					
Safety life-cycle phase or activity		**Objectives**	**Requirements clause or subclause of IEC 61511:—**	**Inputs**	**Outputs**
Fig. 2, box 1	H&RA	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction

F.5.3 Hazard identification

The hazard identification process started during the business decision analysis (Clause F.2). It is one of the most important functions of the PHA team, and is ongoing until the process is turned over to plant operations and becomes subject to operational safety review and audit programs.

F.5.4 Preliminary hazard evaluation

The first step in any process development planning is to identify the broad parameters of the production process, to define safety and environmental hazards (or hazardous events), and to seek opportunities for making the process inherently safer. To do this, information is required about the physical and hazardous properties of all the feedstock, intermediates, products and wastes involved in possible alternative processes. For this example, where a specific polymer is being made from its monomer, there is little choice about the basic reactant. The available alternative processes vary the polymerization medium-solution, suspension or emulsion. The significant properties of VCM are summarized in Table F.3 (latest VCM material safety data sheet should be used in a ‘’real’’ example).

However, the reaction conditions and the initiator (plus any additives) should be carefully chosen to assure that the reaction rate can be safely controlled to prevent runaway reactions, while producing adequate quality and yield. The selected technology involves polymerization in water, but does require small quantities of a relatively dangerous liquid initiator. The hazards associated with the initiator also need careful attention, but are not included in this simplified example.

F.5.5 Accident history

Next, the hazards are identified. In this example, the primary hazards are associated with the flammability and toxicity of combustion products from VCM. In actual plant design, personnel exposure and environmental ambient VCM limits would also be major considerations; for

simplicity, these are not covered in this example. As a first step, it is useful to review the past history of accidents associated with similar operations.

In the case of VCM, we find reference to an accident in a PVC plant, in which four lives were lost and ten people were injured. This accident was due to discharging a batch from the wrong reactor vessel, so that monomer was released into a room containing the parallel reactors. VCM vapour was presumably ignited by a spark from electric machines or by static electricity and the building housing the reactors exploded.

In another accident, a worker mistakenly opened a manhole cover on a reactor that was in service, releasing a large quantity of vinyl chloride that ignited and caused a flash fire resulting in the death of the maintenance person and two labourers.

Another accident involved charging a reactor with 946 litre – 250 gallons of VCM with the bottom valve of the reactor open. Although a serious hazard was created by this release, ignition did not occur and no one was injured. Other incidents are noted, such as one in which an explosion occurred during maintenance work on a vinyl chloride pump (due to a poly-peroxide contaminant that was present as a result of three simultaneous, abnormal situations). VCM was also released from a scrubber in a VCM production plant due to maintenance problems with a plugged valve during periodic recharging. Ignition of VCM resulted in one death and several injuries.

There also have been VCM releases and fires associated with transportation. A derailment of 16 cars near Houston, TX, USA, led to the escape of VCM from a 182 kilolitre – 48,000-gallon rail tanker with immediate ignition. After 45 minutes of exposure to the fire, a second rail car of VCM ruptured violently, producing a large fireball, killing a fireman and injuring 37 other people. Large sections of a tank car were found about 120 metre – 400 feet from the derailment site after the explosion.

In addition, there are likely to be numerous minor incidents for every major accident reported. Attention should be paid to the potential for small releases since these may be partial pathways to major accidents. Particularly with highly flammable pressurized material, ignited small releases may cause larger failures if they heat other system devices. Thus, integrity of a VCM system should be at a high level.

Table F.3 – Some physical properties of vinyl chloride

Formula: CH_2=CHCl
Synonyms: vinyl chloride monomer (VCM)
Monochloroethylene
Chlorethene
vinyl chloride (VCl)
Shipped as compressed liquefied gas; Reid Vap. press.=5,17 bar.a /75 psia
Gas, colorless, sweet odor; Mol wt. = 62,5; Sp. Grav. (vap) = 2,16
Normal boiling point = -13,4 °C / 7,1 °F; Sp. Gr. (liqNBP) = 0,97; Floats and boils on water
Critical T = 431 K / 317°F; Critical P = 55,4 bar.a / 775 psia; Melting point = -154 °C / -245 °F
Heat of vaporization = 372,16 kJ/kg / 160 Btu / lb; Heat of combustion = 18 924 kJ/kg / 8 136 Btu/lb
Heat of polymerization = 1 695,6 kJ/kg / -729 Btu / lb; normally stable at ambient conditions; polymerizes in presence of air, sunlight, moisture, heat, or free radical initiators unless stabilized by inhibitors.
FIRE HAZARDS:
Flammable limits in Air: 3,6–33 %
Flash point: -61 °C /–108 °F (open cup); Autoignition *T* =472 °C / 882 °F
Spills flash, boil and produce heavier-than-air gas cloud that may be ignited with flashback.
Poisonous gases (HCl, CO, etc.) produced in fire
May explode if ignited in confined space
External fire exposure to container may result in BLEVE
HEALTH HAZARDS:
Irritating vapor to eyes, nose and throat.
If inhaled, causes dizziness, difficult breathing, and may cause serious adverse effects, even death.
Excessive exposure may cause lung, liver and kidney effects. Human carcinogen, listed by OSHA, The International Agency for Research on Cancer (IARC), and the US National Institute of Health National Toxicology Program (NTP).
Threshold limit value: 5 ppm
OSHA PEL: 1 ppm TWA, 5 ppm excursion limit average over any period not exceeding 15 minutes.
Odor threshold: 260 ppm
Liquid contact may cause frostbite.
WATER POLLUTION:
Limit in process water: 10 ppm
Limit in water discharged offsite: 1 ppm
AIR EMISIONS:
Limit in process discharge to atmosphere: 10 ppm (local standard)
Limit for annual concentration at plant boundary: 0,2 $\mu g/m^3$ VCM in air
RESPONSE TO DISCHARGE:
Issue warning — High flammability, remove ignition sources, ventilate
Stop flow
Evacuate area, allow entry only with proper protective gear
Let large fires burn; extinguish small fires with dry chemical or CO_2
Cool exposed container with water
Prevent entry into sewer systems to avoid potential explosions

F.6 Preliminary process design safety considerations

For this example, the desired production rate of PVC is 90 million kilogram/200 million pounds per year, or about 10 400 kg/h / 23 000 lb /hr. Based on known reaction kinetics, at a reaction temperature of about 60 °C /140 °F, the corresponding cycle time is about 8 hours. In setting the reactor inventory, judgment is usually used with some awareness of the fact that hazard magnitude for catastrophic vessel failure is related to the amount of hazardous material. At one extreme, a single reactor might be used, with a production batch of 81,6 tonne/180 000 lb of PVC in a 40 % slurry mixture, requiring a reactor sized for about 189 000 litre/50 000 gallons capacity. This would be unwise, since no redundancy is present and there is a very large, flammable, high-pressure inventory. Also since capacity is not distributed, production batches would be large and infrequent, and would require downstream equipment sized for large inventories. Furthermore, this reactor would require addition of a large quantity of the dangerous initiator solution–a large enough inventory to raise serious safety concerns.

At the other extreme, a large number, say ten, of small reactors, each designed for a 8,16 tonne/18,000-lb production batch (about 18 900 litre/5 000 gallons), might be used. In the first extreme, inventories are large; in the second, batches are small, switching operations are much more frequent, and there are many more interconnecting lines, valves, and complexities. Tradeoffs would be considered, based on operational needs, availability of equipment, and cost, as well as safety.

Refinement of such analyses leads to selection of the number of reactors in parallel and the size of the reactor unit. At this point, it is well to provide for any potential for future expansion in capacity. In this example, it is decided to install three parallel reactors, each with a 64 400 litre/17 000-gallon capacity. The 20 litre/5 gallons of initiator solution required per batch is a manageable quantity for safe handling. The maximum inventory of VCM in a reactor is estimated to be 27,2 tonne/60 000 lb.

Reaction temperature is selected to achieve a desired molecular weight, which is end-use driven. Proper reactor cooling water temperature control for stable reactor operation is required to prevent runaway reaction. Stable control of the polymerization reaction temperature requires a low temperature difference between the cooling water and the reaction temperature. For this example, the tempered cooling water supply temperature is high enough to provide a low temperature difference, versus the 60 °C / 140 °F reaction temperature, for safe operation. The tempered cooling water comes from an established, highly reliable source with sufficient quantity and pressure available.

For this example, it was assumed that relief valves and vent valves go to a scrubber so that discharges are not environmental incidents.

F.7 Recognized process hazards

The primary acute hazards associated with VCM release are fire and explosion, with generation of toxic combustion products. These types of hazard include the following:

a) Jetfires: A leak from a pressurized system ignites and forms a burning jet that might impinge on other equipment and cause damage. (In rough terms, jet length is about 150 times the jet orifice diameter–a jet from a 50 mm/2-in. hole could produce a burning jet about 9 metre/30 feet long.).

b) Flash fires: A pressurized liquid release flashes, producing flammable vapour that travels to an ignition source. Upon ignition, the flame travels back through the flammable vapour cloud. (The flammable plume in this case can be substantially larger than the flame jet.).

c) Poolfires: Residual liquid from a flashing release forms a pool which may ignite and burn with a flame height that is two or three times the width of the pool.

d) BLEVEs (boiling liquid expanding vapour explosions): A pressurized tank of VCM or associated piping exposed to an external fire may fail due to metallurgical weakening. Such failure may result in a catastrophic tank failure, a fireball and the potential for rocketing fragments. Relief valve overpressure protection will not prevent a BLEVE.

e) Explosions: Leakage of flammable gas into a confined space with subsequent ignition may lead to explosions or detonations with substantial overpressures.

f) Hydraulic failure: Overfilling of a tank with subsequent liquid expansion through heating may lead to collapse of any vapour space and rapid pressurization. Sudden tank failure may ensue.

g) Stress corrosion failure: Air (oxygen) in the system may increase the presence of chloride ions and may lead to loss of metallurgical integrity.

h) Toxic combustion products: The combustion products of VCM include phosgene, hydrogen chloride and carbon monoxide along with other toxics. (These will be present in the aftermath of a fire, particularly if the fire is within a confined space).

i) Runaway polymerization reaction: VCM polymerization has the potential to rupture the reactor, releasing the VCM with major damage possible.

In addition, VCM presents chronic exposure hazards, being a known human carcinogen, and is a regulated substance with regard to personnel exposures to its vapours, having an OSHA PEL (personnel exposure limit – time weighted average) of 1 ppm in air over 8 hours (5 ppm limit over 15 minutes). Further, federal and local regulations limit its discharge levels from process vents and plant water treatment systems. There are also stringent limits set on the amount of residual VCM that may be present in the PVC product.

There are some lesser short-term hazards involved with inhalation of VCM vapour and the potential for auto-refrigeration of flashing fluid. Personnel require protection from both inhalation and possible freeze burns.

At this point, scoping hazard zone estimates are made to indicate the magnitude of major potential accidents. A 27,2 tonne/60 000-lb release of VCM could produce a flammable vapour cloud equivalent to a cubic volume that is about 120 metre/400 feet on a side. Because VCM is a heavy gas and may contain aerosols from flashing, a major vapour cloud is much more likely to be pancake-shaped, but still might have a flammable footprint of 300 – 450 metre/1,000-1,500 feet in diameter. This indicates that the maximum accident involving a single reactor might have offsite impacts, and could fill a substantial confined volume with flammable gas. In terms of the assessment criteria discussed in Table F.8 below, this impact should be considered to be at least "severe," and probably "extensive," depending on specific data considerations. To be conservative, the PHA team considers it to be in the "extensive" impact category. *(Note:* The bulk storage of VCM on site is not considered in this limited example.)

F.8 Process design definitions strategy

The details of the design require definition of the basic operating procedures and maintenance strategies for the facility. Figure F.3, a preliminary P&I diagram, is provided to assist in this effort. The operational steps for the process are outlined below:

a) Pre-evacuation of air: If the reactors have been opened for maintenance, oxygen should be removed from the system for quality and metallurgical integrity reasons.

b) Reactor preparation: The empty reactor is rinsed with high-pressure water, leak tested if the hatch has been opened, and treated with antifoulant.

c) Demineralised water charging: A controlled charge of water is added. An overcharge might lead to a hydraulic overfill; an undercharge may cause quality problems and potential runaway reaction. Any surfactants or other additives are also introduced during this step.

d) VCM charging: An accurate charge of VCM is added to the reactor.

e) Reactor heat-up: The initiator is added from the charge pot to the batch, and steam is added to the cooling water circulated through the reactor jacket until the batch is at a temperature where the reaction will proceed (about 5,5°C / 10°F below the steady-state reaction temperature).

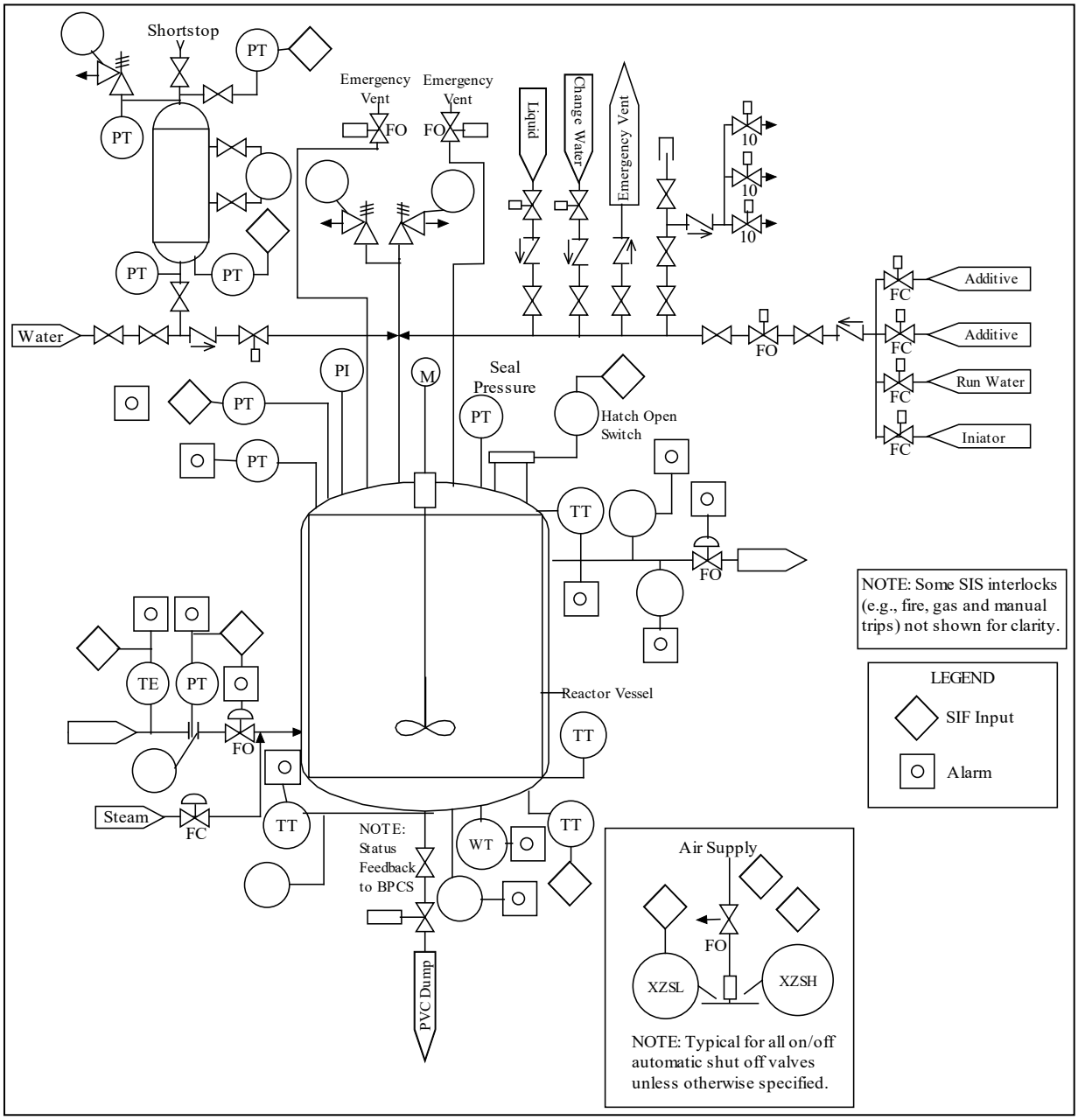
f) Reaction: The steam system is isolated and cooling water is circulated through the reactor jacket to control temperature by removing the heat of polymerization while the reaction progresses.

g) Termination: When the reactor pressure starts to decrease because most of the VCM present has been consumed by the polymerization, the batch will be discharged.

h) Reactor discharge: The reactor contents are dumped under pressure to a downstream holding facility where the system is degassed for subsequent stripping and drying. To prevent resin settling in the reactor, the agitator operates during the dumping procedure. Unreacted VCM is recovered for reuse.

There are two additional process systems that are provided for an emergency situation. In the event of an uncontrolled reaction or the potential for such an event, the polymerization can be stopped rapidly by addition of a shortstop chemical (chain stopping agent) to the batch. However, agitation of the batch is necessary for good distribution of the shortstop to rapidly terminate the polymerization. If the agitator has failed, the shortstop should be added within a minute or two, to allow mixing before the liquid swirl in the reactor dissipates. As a back-up, the reactor contents can be mixed by “burping” the reactor—dropping pressure to generate rising bubbles within the bulk liquid mass. These are both operator-activated events.

The second emergency system is an automatic depressurization system. In the event of an uncontrolled reaction, the reaction can be safely limited by depressurizing the reactor to the vent system. The heat of vaporization of the boiling reaction mass safely removes heat from the reactor. The emergency vent system will be sized to handle the peak venting needs of the reactor system.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk
Checked: V. May
R. Brown
Approved: W. Burk
DWG# XXXXX1

IEC

Figure F.3 – Example of the preliminary P&ID for PVC reactor unit

Piping headers are shown consolidated for clarity. See Figure F.11 for header clarity.

F.9 Preliminary hazard assessment

F.9.1 General

Once the design was developed in some detail, the PHA team subjected the design to a preliminary hazard assessment. This assessment is considered preliminary because the design is not yet complete. The PHA team used a what-if/checklist review (Table F.4) for the simpler portions of the process, and a HAZOP (Table F.5) on the more complex portions of the process.

From the hazard identification process and from the past accident history, it seems that the example process reactor has the potential for “minor” through “extensive” events as defined in Table F.8.

In addition, design integrity should consider the need to meet the strict containment requirements to prevent emissions of VCM that might endanger worker safety and health. The results of this hazard review should be carefully documented, with particular regard to event sequences that might lead to uncontrolled releases.

Table F.4 and Table F.5 show only partial lists of hazards pertinent to this example. A typical project would have a much more extensive list of What-If and HAZOP items.

Table F.4 – What-If/Checklist

Prepared and approved by the process hazards analysis team, see Clause F.2.

What if...	Hazard	Consequences	Safeguards	Ref#	Recommendations	By
What if area wide electrical power fails. (UPS instrumentation power remains)	Runaway reaction through loss of agitation. Indicated by agitator motor off, low coolant flow, high reactor pressure, and high reactor temperature.	Runaway reaction causes reactor overpressure and loss of containment.	Add shortstop and burp reactor to stop runaway. Depressurize reactor – SIS (Pressure safety valve sized for this event).		Use LOPA to determine required SIL	
Batch recipe error – two charges of initiator are used	High initiator concentration causes runaway reaction. Indicated by high reactor temperature and pressure.	Runaway reaction leads to reactor overpressure and loss of containment.	Add shortstop. Depressurize reactor – SIS (Pressure safety valve sized for this event).		Use LOPA to determine required SIL	
What if reactor agitator seal fails	VCM fume release. Indicated by high pressure in the reactor seal and fume detector in the area.	VCM fumes are flammable.	Additional ventilation around reactor seal. Depressurize reactor on high seal pressure – SIS.		Use LOPA to determine required SIL	
NOTE This is only a partial list of hazards.						

Table F.5 – HAZOP

Prepared and approved by the process hazards analysis team, see Clause F.2

Guideword (GW)	Deviation	Causes	Consequences	Safeguards	Ref#	Recommendations	By
No	No flow	Cooling water control system failure	Eventual runaway reaction through reactor high temperature and/or high pressure	Add shortstop. Depressurize reactor SIS (Pressure safety relief valve sized for this event)		Use LOPA to determine required SIL	
		Pump stops due to pump power failure	Eventual runaway reaction through reactor high temperature and/or high pressure	There is a steam drive on the pump in addition to electric power. Add shortstop. Depressurize reactor SIS (Pressure safety relief valve sized for this event)		Use LOPA to determine required SIL	
No	No agitation	Agitator motor drive fails	Reduced cooling temperature, non-uniformity, leads to runaway reaction. As indicated by high reactor temperature, pressure, and low agitator motor amperage.	Add shortstop and burp reactor to stop runaway. Depressurize reactor SIS (Pressure safety relief valve, sized for this event)		Use LOPA to determine required SIL	
More	Higher temperature	Temperature control failure causes overheating during steam heating	High temperature leads to runaway reaction. Indicated by high reactor pressure and temperature.	Add shortstop. Depressurize reactor SIS (Pressure safety relief valve sized for this event)		Use LOPA to determine required SIL	
More	Higher level	Level control failure allows the reactor to overfill	Reactor becomes liquid full as the temperature increases, possible hydraulic reactor damage and VCM release. Indicated by high charge level, high charge weight, or high reactor pressure.	Compare high level and weight with recipe. Depressurize reactor SIS (Pressure safety relief valve sized for this event)		Use LOPA to determine required SIL	
NOTE This is only a partial list of hazards.							

Based on these results, a team of appropriate PHA process and instrumentation experts summarized a list of accident events where SIF were proposed as mitigation of the hazard.

Table F.6 is a partial list of accident events and the associated prevention strategy used to propose interlock strategy and actions to help further identify or create additional independent layers of protection. Table F.6 is prepared and approved by the Process Hazards Analysis Team, see Clause F.2

Table F.6 – Partial summary of hazard assessment for SIF strategy development

#	Initiating event	Process upset	Process variables affected	Preventive strategy
1	Cooling water control fails	Loss of cooling leading to runaway reaction	– Low C.W.* Flow – High reactor temp. – High reactor pressure	– Add shortstop – Depressurize reactor (SIS) – Pressure safety valves (IPL)
2	Agitator motor drive fails	Reduced cooling, temperature non-uniformity leads to runaway reaction	– Low agitator motor amperage – High reactor temp. – High reactor pressure	– Add shortstop and burp reactor to stop runaway. – Depressurize reactor (SIS) – Pressure safety valves (IPL)
3	Area-wide loss of normal electrical power (UPS instrumentation power remains)	Loss of agitation leading to runaway reaction	– Agitation motor off – Low coolant flow – High reactor pressure – High reactor temp.	– Add shortstop and burp reactor to stop runaway. – Depressurize reactor (SIS) – Pressure safety valves (IPL)
4	Cooling water pumps stop, pump power failure	Loss of cooling leading to runaway reaction	– Low C.W. flow – High reactor temp. – High reactor pressure	– Steam drives on pumps – Add shortstop – Depressurize reactor (SIS) – Pressure safety valves (IPL)
5	Batch recipe error; two charges of initiator are used	High initiator concentration causes runaway reaction	– High reactor pressure – High reactor temp.	– Add shortstop – Depressurize reactor (SIS) – Pressure Safety valves (IPL)
6	Control system failure overfills reactor	Reactor becomes liquid full as the temperature increases, possible hydraulic reactor damage and VCM release.	– High charge level – High charge weight – High reactor pressure	– Compare level & weight with recipe – Depressurize reactor (SIS) – Pressure safety valves (IPL)
7	Temperature control failure causes overheating during steam heat-up step	High temperature leads to runaway reaction.	– High reactor pressure – High reactor temp.	– Add shortstop – Depressurize reactor (SIS) – Pressure safety valves (IPL)

#	Initiating event	Process upset	Process variables affected	Preventive strategy
8	Reactor agitator seal fails	Seal failure can lead to dangerous VCM fume release	– High Pressure in Reactor Seal – Fume Detection in Reaction Area	– Additional ventilation around seal – Depressure reactor on high seal pressure (SIS)
* C.W. stands for cooling water .				

As a result of the above hazards being identified, the PHA team made the following recommendations:

a) Implement the following SIS preventive strategy dealing with runaway reaction scenarios:
   – If a high-temperature or pressure condition occurs, there is sufficient time for the operator to remotely add shortstop.

   NOTE For items 2 and 3 of Table F,6, "burping" of the reactor is required after adding the Shortstop to mix the shortstop into the reaction mass, since the agitator is not working.

   – If this does not stop the runaway, a "high-high" temperature or pressure SIF will open the emergency de-pressure vent valves to safely control the runaway.

b) For runaways that occur because the agitator is not working (items 2 and 3 of Table F.6) protection is needed in addition to the recommendation given in “a)” above:
   – Loss of agitation (low amps) will be indicated to the operator by an alarm, and after adding the shortstop, "burping" is required to mix the shortstop into the reaction mass.
   – As in recommendation “a)” above, the emergency de-pressure SIF(s) is a backup to control the runaway.

c) Low or no cooling water flow upsets are controlled by the protection in recommendation a) above. If low cooling water flow was caused by power loss to the water pumps, the operator is alerted by the low-flow alarm to turn on the steam turbine water pump drive;

d) Overcharging the reactor with water or VCM can cause overfilling and possible reactor hydraulic overpressure damage. This upset is avoided by preventing the batch heat up if the weigh cells or the reactor level exceed the "high" limit for that batch addition step in the BPCS. Backup is provided by the "high-high" reactor pressure SIF that activates the emergency de-pressure vent valves;

e) Failure of the reactor agitator seal causes dangerous releases of VCM. To protect against this it is recommended to activate the emergency de-pressure SIF(s) for high pressure in the agitator seal;

f) Because the shortstop system is very important in controlling runaway reactions, interlocks in the BPCS to assure shortstop availability are also recommended by the team. The BPCS interlocks do not allow VCM charging to reactor if the shortstop tank level is low, or if the nitrogen pad pressure on this tank is low.

F.9.2 Step F.2: Allocation of safety functions

Table F.7 provides a view of the key elements in the allocation of safety functions.

Table F.7 – SIS safety life-cycle – Box 2

Overview					
Safety life-cycle phase or activity		**Objectives**	**Requirements** **Clause or subclause of IEC 61511-1:2016**	**Inputs**	**Outputs**
IEC 61511-1:2016Figure 7, box 2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL	9	A description of the required SIF and associated safety integrity requirements	Description of allocation of safety requirements (see Clause 9 of IEC 61511-1:2016)

F.10 SIF safety integrity level determination

Using the proposed list of SIF, a PHA team meeting is held to determine the required SIL for each SIF. The layer of protection analysis (LOPA) method will be used. For a description of the LOPA method, refer to IEC 61511-3:—, Annex F. Additional guidance is provided in AIChE, CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment,* 2001.

F.11 Layer of protection analysis (LOPA) applied to example

Clause F.11 explains the transition from data shown in the partial summary of hazard assessment information (Table F.6) to LOPA (Table F.9).

The list below shows LOPA scenario descriptions:

– Event 1: Cooling water control fails

This upset initiates a runaway reaction that can catastrophically rupture the reactor. The impact of this event was judged to be “extensive,” which, as discussed in Table F.8 Note 1, leads to a tolerable frequency of 10^{-5}/year for a single scenario. Several failures in the control system could cause this upset, with operating experience indicating that this type of upset occurs about once every 10 years. Protection per Table F.6 was the shortstop addition, but the runaway reaction may be too fast for the operator to respond to an alarm. This protection layer is not included for risk reduction. The area is normally occupied, so it was assumed that personnel could be impacted by the event. The pressure safety valves (PSVs) are only estimated to be 90 % effective, since plugging is a common problem in this service. Since the PSVs share a common relief line, they are conservatively considered to be a single Independent Protection Layer. This led to an intermediate event likelihood of a 10^{-2} per year. Per the conservative assumptions used in this example, only the PSVs qualified as an IPL. The PHA team reviewed all the process safety risk issues and decided that a SIF was appropriate. As shown in Table F.9, this requires a SIL 3 SIF.

NOTE The PSVs are provided to comply with the pressure vessel codes, but as shown by the LOPA (utilizing the corporate risk criteria of Table F.8), these are not sufficient protection to meet the risk target for this scenario. This note is typical for all LOPA scenarios in this example.

– Event 2: Agitator motor drive fails

This upset initiates a similar runaway reaction as Event #1, except that, since agitation has stopped, the additional step of reactor “Burping” (F.8) is required for stopping the runaway reaction by adding shortstop. Again, this runaway may occur so fast that the operator may not be able to respond, so no risk reduction is taken for operator response to alarms. Several failures in the control system or the agitator itself could cause this upset, with operating experience indicating that this type of upset occurs about once every 10 years. SIF S-1 is the only effective SIF for this event, and it requires SIL 3.

– Event 3: Area-wide loss of normal electrical power

While the upset has obvious differences from Event F.2, the SIF SIL selection comes to a similar result as Event F.2.

– Event 4: Cooling water pump power failure

The upset in Event 4 is similar to the upset in Event 1. Operator intervention can stop this runaway by starting the steam turbine driven water pumps, or adding shortstop. While this operator action was judged to be very effective, no risk reduction credit was taken because of operator availability. The analysis shown in Table F.9 led to SIL 3 for SIF S-1.

– Event 5: Double charge of initiator

This upset leads to a very energetic runaway reaction with a high rate of heat generation and rapid pressure rise even though the cooling water is operating. The pressure rise would be too fast for temperature to be an effective measurement to trigger the SIF. Both the PSVs, and the de-pressure SIF are designed to safely control this runaway. Because of design and procedure safety features, this upset requires a very unlikely combination of failures. Therefore, a moderate initiating event likelihood of 10^{-1} was selected. The moderate likelihood, one non-SIS IPL, and “extensive” severity, led to a SIL 3 for SIF S-2.

– Event 6: Overfill reactor caused by control system failure

The impact of this upset would be to hydraulically overpressure the reactor, causing a blown flange gasket or similar release. With the large numbers of batches per year and their varying recipes, the likelihood is judged to be moderate (1 per 10 years). The team judged the effectiveness of the BPCS level and weigh cell alarms with operator intervention to be 90 % effective (10^{-1}) since the alarms are located in a separate BPCS controller. The pressure safety valves and the de-pressure SIS will be effective in dealing with this upset. The severity level of “severe,” with a moderate initiating event likelihood, and two non-SIS IPLs, indicated that a SIL 1 was appropriate for the de-pressure SIF. Even though a SIL 1 SIF is indicated, SIF S-2 should be designed to SIL 3 as required by Event 5 above.

– Event 7: Temperature control failure during heat-up step – Overheats batch

This event leads to a runaway reaction similar to Event 1. The event impact and protection aspects are similar to Event 1, except that the temperature transmitter is not considered as suitable as risk reduction for this event. During heat-up the operator has time to add the shortstop to prevent the runaway. However, since the temperature transmitter is used for control, it may be part of the initiating cause of this hazard. Therefore, operator response to a high temperature alarm would not be an IPL for this event. SIF S-1 should be designed to SIL 3, which was already required for Event 1.

– Event 8: Agitator seal fails

The special seal design used for this reactor restricts VCM releases to small flow rates if the seal fails. The spot ventilation provided will be sufficient to minimize this fire and explosion hazard. The PHA team judged the severity as “severe” and decided that spot ventilation was 90 % effective (10^{-1}). There are no IPLs, the severity is “severe,” and the likelihood is high, so per Table F.9, a SIL of 2 is appropriate.

F.12 Tolerable risk criteria

The tolerable risk criteria used for this example are shown in Table F.8 below.

These criteria are company-specific. Each company will have to apply its own risk criteria when defining the necessary safety functions and if appropriate agree with local regulator authority.

Table F.8 – Tolerable risk ranking

Severity	Definition	Tolerable frequency (events/year) (see Note 1)
Extensive	One or more fatalities or irreversible health effect	10^{-4}
Severe	Multiple medical treatment case injuries; 1 or 2 restricted workday cases or lost workday case or moderate health effect cases	10^{-3}
Minor	Minor injury or reversible health effects	10^{-2}

NOTE 1 The tolerable frequencies shown are for total risk from all hazards. The tolerable frequency for each LOPA scenario is set one order of magnitude lower to account for multiple hazards (i.e., each scenario with "extensive" severity is assigned a tolerable frequency of 10^{-5}). This approach is acceptable for this example because the operating area is not normally occupied, with routine operator patrols (single person per patrol) being the primary reason for personnel being exposed to the hazards associated with this operation.

NOTE 2 Table F.8 data is Company Standard.

NOTE 3 The company in this example is a corporation with operations in Great Britain as well as the USA. For projects implemented in Great Britain, additional risk criteria would be applied. In Great Britain, the view of HSE is that the risk of a harmful event has to be reduced to the point where the cost of any further risk reduction is grossly disproportionate compared with the benefit gained. References*: Reducing Risk Protecting People*, HSE, ISBN No. 07176-2151-0, published 2001; www.hsebooks.co.uk; IEC 61511-3.

Table F.9 – VCM reactor example: LOPA based integrity level

Prepared and approved by the process hazards analysis team, see Clause F.2.

#	1	2	3	4	5			6	7	8	9	10	11	12
	Impact event	Severity level/ Tolerable frequency	Initiating cause	Initiation frequency (events/yr)	PROTECTION LAYERS			Additional mitigation	Intermediate event frequency (events/yr)	Number of IPLs	SIF needed?	SIF integrity level	Mitigated event frequency (per year)	Notes (SIF ID)
					Process design	BPCS	Alarms etc.							
1	Reactor rupture	E 10^{-5}	Coolant H2O control fails	10^{-1}	No	No	No	PSVs 10^{-1}	10^{-2}	1 (PSVs)	Yes	3 (Depress.) 10^{-3}	10^{-5}	S-1
2	Reactor rupture	E 10^{-5}	Agitator motor drive fails	10^{-1}	No	No	No	PSVs 10^{-1}	10^{-2}	1 (PSVs)	Yes	3 (Depress.) 10^{-3}	10^{-5}	S-1
3	Reactor rupture	E 10^{-5}	Area wide loss of normal electrical power	10^{-1}	No	No	No	PSVs 10^{-1}	10^{-2}	1 (PSVs)	Yes	3 (Depress.) 10^{-3}	10^{-5}	S-1
4	Reactor rupture	E 10^{-5}	Cooling water pump power failure	10^{-1}	No	No	No	PSVs 10^{-1}	10^{-2}	1 (PSVs)	Yes	3 (Depress.) 10^{-3}	10^{-5}	S-1
5	Reactor rupture	E 10^{-5}	Double charge of initiator	10^{-1}	No	No	No	PSVs 10^{-1}	10^{-2}	1 (PSVs)	Yes	3 (Depress.) 10^{-3}	10^{-5}	S-2
6	Reactor damage hydraulic over-pressure	S 10^{-4}	Overfill reactor, control system failure	10^{-1}	No	No	Level (400 LSH) and weigh cell (300 WTH) alarms 10^{-1}	PSVs 10^{-1}	10^{-2}	1 (PSVs)	Yes	3 (Depress.) 10^{-3} (SIL 1 req'd)	10^{-6} (10^{-4} req'd)	S-2
7	Reactor rupture	E 10^{-5}	Temp. control fails add excess steam	10^{-1}	No	No	No	PSVs 10^{-1}	10^{-2}	1 (PSVs)	Yes	3 (Depress.) 10^{-3}	10^{-5}	S-1
8	Release of VCM	S 10^{-4}	Agitator seal fails	10^{-1}	Spot ventilation at reactor seal 10^{-1}	No	No	No	10^{-2}	0	Yes	2 (Depress.) 10^{-2}	10^{-4}	S-3
Severity level E—extensive; S—severe; M—minor (see Table F.8); Likelihood values are events per year; other numerical values are probabilities.														

For simplicity, this example does not take credit for the reactor not being in operation 100 % of the time. Nor does it account for the fact that the hazards exist for each of the three reactors.

After the LOPA was completed, the mitigated event likelihood for scenarios 1 to 5 and 7 were summed. The total frequency of 6E-5 meets the corporate tolerable frequency criteria for "Extensive" events of 10^{-4} as shown in Table F.8. The total mitigated event frequency for scenarios 6 and 8 was 1.01E-4, which meets the corporate tolerable frequency criteria of 10^{-3} for "Severe" events.

F.13 Step F.3: SIS safety requirements specifications

F.13.1 Overview

Table F.10 – SIS safety life-cycle – Box 3

Overview					
Safety life-cycle phase or activity		**Objectives**	**Requirements clause or subclause of IEC 61511-1—**	**Inputs**	**Outputs**
IEC 61511-1:2016 Figure 7, box 3	SIS SRS	To specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety	10	Description of allocation of safety requirements (see Clause 9 of IEC 61511-1:2016)	SIS safety requirements; AP safety requirements

The information in this example SRS may be contained in a single document format. It may alternatively be contained in a combination of documents. The following requirements are for this example only.

F.13.2 Input requirements

The information in Table F.11, SIF and associated SILs, were the outputs of step 2 and were used in the development of the SRS.

Table F.11 – Safety instrumented functions and SILs

Identifier	Monitored process variables	SIL
S-1	Reactor high pressure and high temperature	3
S-2	Reactor high pressure	3
S-3	Agitator seal high pressure	2

The BPCS performs operational functions for an orderly start-up and normal shutdown. These are not included in this example.

The PHA team has identified plugging as a potential problem in this application. The design team should take this concern into account when it designs the SIS.

No regulatory requirements that would impact the SIS design were identified.

F.13.3 Safety functional requirements

Table F.12 lists the safe state for each SIF and shows the functional relationship between process inputs and outputs, including the logic required.

Table F.12 – Functional relationship of I/O for the SIF(s)

SIF #	SIL	Sensor	Description	Final element safe state
S-1	3	100PT 100PT1 100TT	If reactor pressure exceeds 125 psig or reactor temperature exceeds 200 °F	Open 100PV Open 100PV1
S-2	3	100PT 100PT1	If reactor pressure exceeds 125 psig	Open 100PV Open 100PV1
S-3	2	200PT	If seal pressure greater than 10 psig	Open 100PV Open 100PV1

Table F.13 shows the process instrument inputs to the SIS, their trip points, normal operating ranges, and operating limits.

Table F.13 – SIS sensors, normal operating range & trip points

Tag	Calibration range	Normal operating range	Pre-trip alarm		Trip point	
100PT	0-200 psig	60-100 psig	115 psig	incr	125 psig	incr
100PT1	0-200 psig	60-100 psig	115 psig	incr	125 psig	incr
100TT	0-250 °F	125-175 °F	180 °F	incr	200 °F	incr
200PT	0-50 psig	0-20 psig	5 psig	incr	10 psig	incr

All SIF are to be designed for de-energized to trip operation.

Final elements go to their safe state on loss of energy as defined in Table F.9. Final elements are voted (1oo2) to meet architectural and PFD_{avg} requirements.

A response time of one minute or less is considered adequate for each SIF, unless otherwise noted.

IEC 61508 assessed transmitters and logic solver are used for the SIS. The assessed transmitters also meet the requirements for prior use.

A review by the PHA team indicated that there are no combinations of safe process states that, when occurring concurrently, create a separate hazard.

The transmitters have a systematic capability of SC 2 and the logic solver has a SC of 3.

The transmitters for S-1 are voted 1oo3 and for S-2 are voted 1oo2 to meet architectural and PFD_{avg} requirements.

The BPCS HMI will serve as the primary human-machine interface for the SIS. All alarm display functions will be implemented in the BPCS HMI; no hardwired annunciation is required. An engineering/maintenance interface will be located in a secure location.

Upon loss of the HMI, the operator has a shutdown button mounted on the console that will be used to initiate a sequence of actions, which is necessary to bring the process to a safe state

in an orderly fashion. The shutdown pushbutton provides discrete inputs to the SIS and BPCS logic solvers and causes shortstop chemical addition through BPCS action.

The PHA team reviewed the safety manual of the selected SIS logic solver and determined that manual actuation of the safety valves, independent of the logic solver, is not required. Based on that review and the undesirable consequences of immediate process depressurization, direct manual activation will not be included in the SRS. See the logic diagram (Figure F.11).

Since this is a batch operation, the process will be shut down in the event of faults being detected in the SIS. That is, the process will not be operated with the SIS running in degraded mode.

Pre-trip alarms that the operator may respond to in order to keep the SIS from shutting down the systems should be assigned the highest priority.

All resets to SIS trips will be reset manually. The manual reset switches are to be located on the operator console in the control room.

Since this is a batch operation and good control system engineering practices are used, spurious trip rate is not a concern.

Shadowing (functional duplication of the SIS application logic in the BPCS) has been provided to address systematic AP faults. It was recognized that shadowing increases the spurious trip rate, but for the batch process in this example, spurious trips were not a concern.

Field device and HMI fault detection by diagnostics will prevent start-up, but alarm only when batch is operational.

When the SIS shuts the process down, all BPCS control loops will be placed in manual and outputs set at the safe state.

Each SIS circuit (e.g., I/O, communication, diagnostics) should be monitored to ensure they are in the energized state prior to SIS start up.

Each transmitter should be automatically checked to ensure bad value (e.g., below 4 mA) does not exist prior to SIS startup.

The operating modes include charging, reacting, and dumping. All functions of the SIS should be operational in each mode.

No overrides, inhibits or bypasses should be provided.

There are no special requirements for the SIS to survive a major accident event.

F.13.4 Safety integrity requirements

The required SIL for each SIF is defined in Table F.9.

Hardware features to achieve the required SIL are:

- the logic solver to have a SC of 3 (i.e., device PFD_{avg} between 0,001 and 0,000 1) supported by IEC 61508 assessments;
- sensors and final elements to be selected based on compliance with IEC 61508 and user approval (see ISA TR84.00.04-Part 1);

- all final elements to be provided with position sensors and checked to ensure valve position is consistent with logic gate command.

Diagnostic features to achieve the required SIL are:

- diagnostics provided with the logic solver;
- high and low limit checking on all input sensors in both the SIS and the BPCS;
- compare diagnostic on 100PT and 100PT1 in both the SIS and the BPCS;
- shadowing in the BPCS.

The reactor will be shut down twice a year for off-line maintenance and safety interlock testing. All protection layers identified in the LOPA that provide risk reduction should be tested at this same frequency. Note: Since this is a batch operation, some SIS devices could be tested more frequently (e.g., the vent valves could be tested before each batch is started) if necessary to meet the target PFD_{avg}. Presently, the SIL verification calculations described in Clause F.16 (“SIF device parameters”) indicate that the higher test frequency is not required. However, if operating experience shows that SIF device failure rates are actually higher than assumed in the PFD_{avg} calculations, higher frequency testing of some devices could be implemented.

All SIF are powered from a UPS to reduce spurious trips. Since this is a batch process, there are no additional provisions for avoidance of spurious trips.

Common cause failures to be minimized by:

- providing separate taps for the redundant pressure transmitters;
- providing separate lines for the redundant vent valves;
- ensuring alarms claimed as an IPL in Event 6 of Table 7 are completely independent of the SIF (i.e., separate DCS controllers are utilized for the control functions, alarm functions, and the shadowing functions of the BPCS);
- applying good engineering practices (e.g., grounding, surge protection, power sources, diversity) as outlined in Clauses F.18 and F.19;
- addressing human factors (e.g., configuration, calibration, testing) by the use of different personnel for checking and approval.

F.14 Functional description and conceptual design

Clause F.14 describes how safety functional requirements and safety integrity requirements were integrated to allow development of SIF architectures, verification of the SIL for each SIF, and development of SIS AP.

F.14.1 Narrative for example reactor system logic

Three automatic SIF, S-1 through S-3, are implemented in the SIS:

- SIFs S-1 and S-2 protect against high temperature/pressure reactor runaways, since the reaction is exothermic, and high pressure results from high temperature;
- if pressure transmitters 100PT or 100PT1 exceed 125 psig or temperature transmitter 100TT exceeds 200 °F, safety function S-1 opens the reactor vent valves.

Since the pressure rise is extremely rapid when a double charge of initiator is added or the reactor is overfilled, SIF S-2 is provided to prevent these events. The slower response of the temperature transmitter may not detect this extremely fast event so the temperature transmitter 100TT is not included in the PFD_{avg} calculation. The vent valves will open if either 100PT or 100PT1 exceeds 125 psig.

Since identical smart pressure transmitters are being used for this application, the probability that a systematic error could cause both transmitters to fail at the same time should be taken into account. Diagnostics are provided in both the SIS and BPCS logic solvers to detect transmitter values that are out of range high, out of range low, or that deviate from each other. The diagnostic coverage is accounted for in the PFD_{avg} calculations as described in Clause F.16.

SIF S-3 is provided to open the vent valves 100PV and 100PV1 when seal pressure exceeds 10 psig as measured by 200PT.

Since initiating causes for scenarios 1 through 8 put demands on devices of the same SIF, the demands should be summed to determine the mode of operation for each SIF. In this example, they sum to 0,8 demands/year, which is less than one demand a year for the SIF. Therefore, each SIF will operate in low demand mode. See ISA TR84.00.04:2015 and A.9.2.3 for guidance on demand versus continuous mode of operation.

Table F.14 – Cause and effect diagram

Reactor cause and effect diagram (table format)						
Cause				**Effect**		
Safety function No.	Sensor/ Input	Description	Trip Setting	Final Device	Action	Comments
S-1	100PT 100PT1	Reactor pressure **OR**	> 125 psig	100PV	OPEN	Depressurize reactor
	100TT	Reactor temperature	> 200 °F	100PV1	OPEN	Depressurize reactor
S-2	100PT 100PT1	Reactor high pressure	> 125 psig	100PV 100PV1	OPEN OPEN	Depressurize reactor
S-3	200PT	Reactor seal pressure	>10 psig	100PV 100PV1	OPEN OPEN	Depressurize reactor

F.15 SIL verification calculations

Given the above functional and integrity requirements, a sketch (i.e., a bubble diagram as shown in Figures F.4, F.6 and F.8) was developed for each SIF to:

- describe how the functional and integrity requirements were met;
- illustrate how the SIF architecture meets the SIL requirements;
- show the PFDavg for each SIF subsystem (sensor subsystem, logic solver subsystem, final element subsystem);
- provide a basis for the development of the SIS architecture;
- provide a basis for the SIF PFDavg calculation.

The bubble diagrams were then utilized to develop a fault tree for each SIF, using commercially available software. The output of the fault tree analysis software documents the SIF PFD_{avg} (see Figures F.5, F.7, and F.9). At this point, the calculated PFD_{avg} was compared to the required PFD_{avg} (see Table F.9, column 10); where the calculated PFD_{avg} failed to meet Table 7 requirements, the conceptual design was altered accordingly.

Each type of SIF device is listed below in Table F.15, along with its reliability parameters. The parameters were developed from prior use, vendor data, and industry databases, with the emphasis on field data.

Mean time to fail dangerous *(MTTFd)*:

Table F.15 – MTTFd figures of SIS F.1 devices

Emergency vent valve	60 years
Pressure transmitter	60 years
Temperature transmitter with RTD	60 years
Solenoid valve	35 years
SIS logic solver	2 500 years

Common cause:

Common cause issues were addressed by the techniques described in Clause F.18. The residual common cause failures were addressed by adding factors to the fault tree for each SIF. These factors were based on plant experience. For both the valves and solenoid valves, the common cause failures were estimated at 1 % of the total dangerous undetected failures; for the transmitters, the common cause failures were estimated at 2 % of the total dangerous undetected failures (i.e., the dangerous undetected failure rate for transmitters due to common cause failures equals 0,02 × (1/60); for valves due to common cause failures equals 0,01 × (1/60); and for solenoid valves due to common cause failures equals 0,01 × (1/35)).

Systematic faults:

The SIS logic solver has a systematic capability of SC 3, which addresses failures of hardware, architectural requirements (fault tolerance) and the embedded software. Note that systematic failures of AP were not addressed in the assessment of the logic solver. Systematic logic solver AP failure issues were addressed by shadowing the logic in the BPCS (see bubble diagrams Figures F.4, F.6, and F.8). The BPCS was used to reduce the systematic failures of SIS AP; however, the contribution of the BPCS hardware to the PFD_{avg} has not been included in the fault tree analysis for each SIF.

NOTE 1 The above technique was used in addition to implementation of the techniques defined in IEC 61511-1:2016, Clause 12.

The pressure and temperature transmitters are smart devices, contain programmable (fixed programming language) devices and have a systematic capability of SC 2 based on compliance with IEC 61508. The transmitters were used in SIL 3 applications (i.e., SIF S-1 & SIF S-2). To address systematic failures, each SIL 3 SIF had several techniques implemented:

- For SIF S-1, prior use performance in equipment selection, while diversity (temperature and pressure) and diagnostics (see F.14.1, “Narrative for Example Reactor System Logic”) were used in design to ensure that systematic software errors are at a level commensurate with a SIL 3 application.
- For SIF S-2, prior use analysis (see note below), fault tree analysis (see Figure F.7) and diagnostics were used to ensure that systematic software failures in the transmitters are at a level commensurate with a SIL 3 application.

NOTE 2 Based on prior use data, the team estimated that 2 % of the total common cause failures of the transmitters were due to software faults. The fault tree shown in Figure F.7 illustrates how the software faults were accounted for in the PFD_{avg} calculation for SIF S-2. If insufficient prior use data was available, an alternative would be for the user to contact the transmitter manufacturer to seek assurance that the techniques used to develop the embedded software were in accordance with the guidelines provided in IEC 61508 for SIL 3 software.

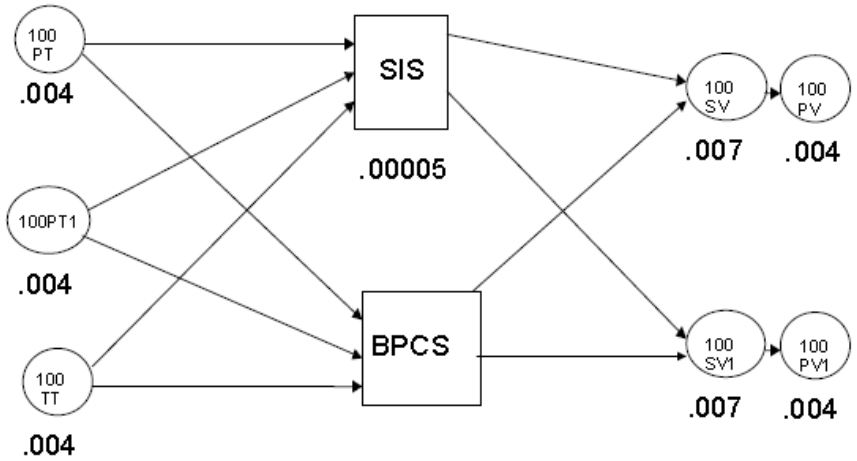
Hardware fault tolerance(HFT)

For SIF S-1 and SIF S-2, the fault tolerance used for sensors and valves was based on IEC 61511-1:2016, Table 6 (SIL 3).

For SIF S-3, the fault tolerance used for sensors and valves was based on IEC 61511-1:2016 Table 6 (SIL 2).

The logic solver was designed and third-party assessed to meet the requirements of IEC 61508 (including fault tolerance) for SIL 3 applications. Therefore, the fault tolerance requirements of IEC 61511 are met for SIF S-1, S-2 and S-3.

SIF S-1



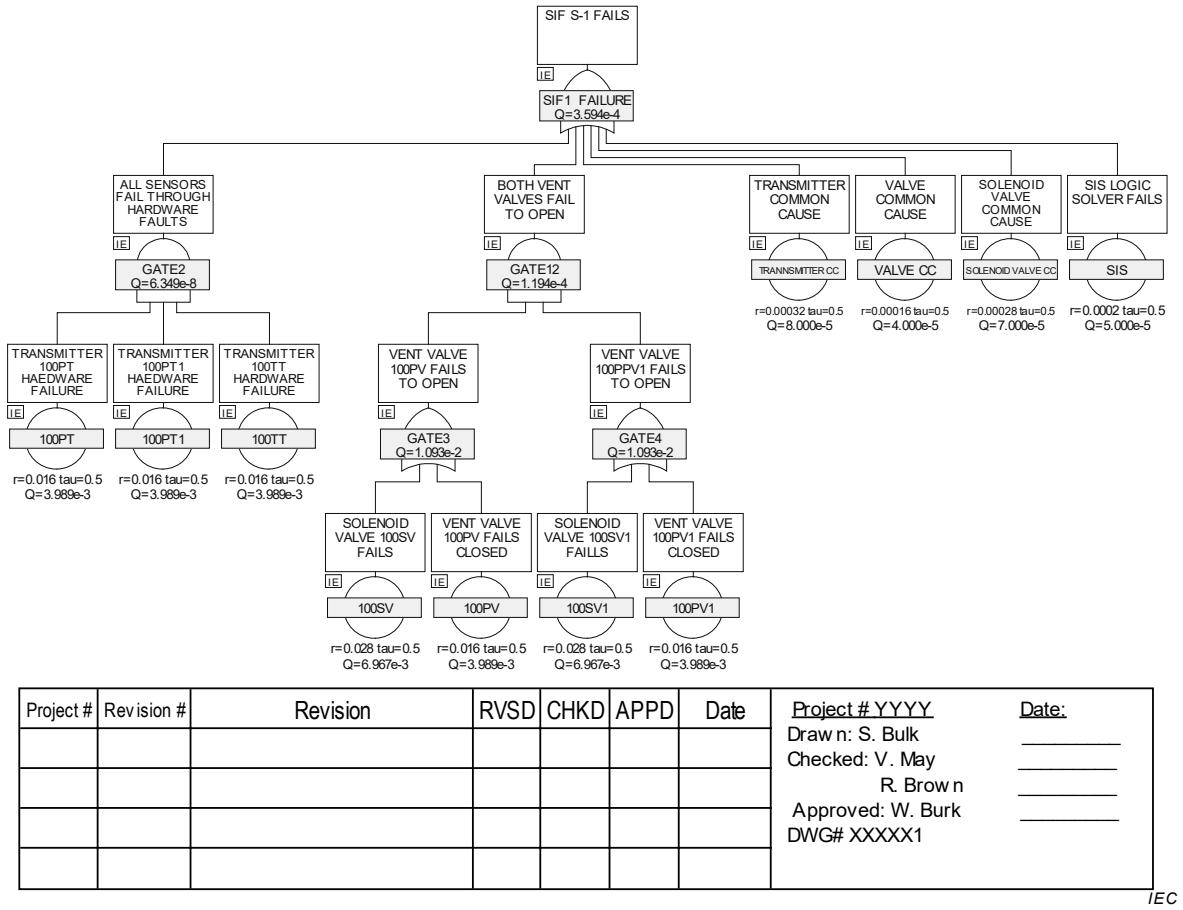
Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Figure F.4 – SIF S-1 Bubble diagram showing the PFD_{avg} of each SIS device

See Figure F.5 for fault tree calculations.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Key

E Enabling event

Q Unavailability (PFD_{avg})

r Failure rate (failures/year)

tau Test interval (years)

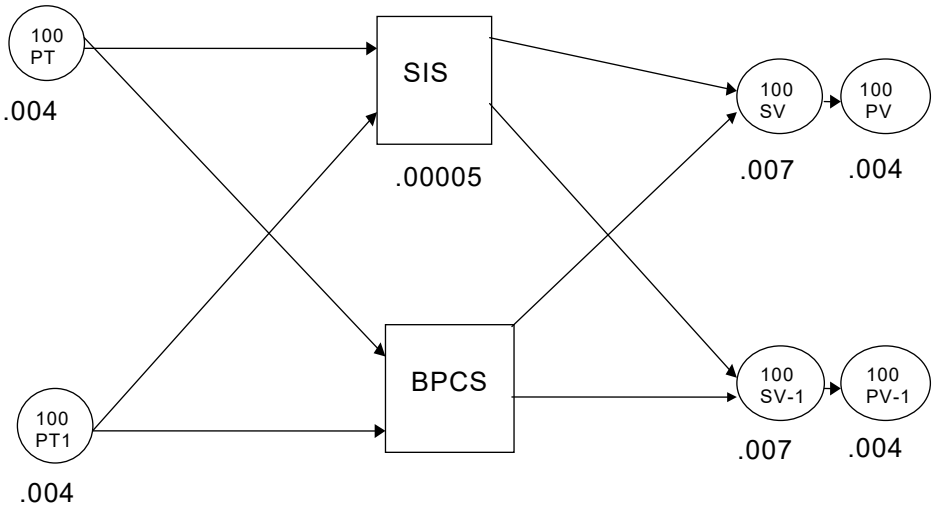
SIF S-1 has a PFD_{avg} rounded to 3,6e-4, therefore meets SIL 3.

Figure F.5 – S-1 Fault tree

SIF S-2

If reactor pressure is above 125 psig, open vent valves 100PV and 100PV1. The required SIL = 3 (which implies $PFD_{avg} = 10^{-3}$ to 10^{-4})

S-2



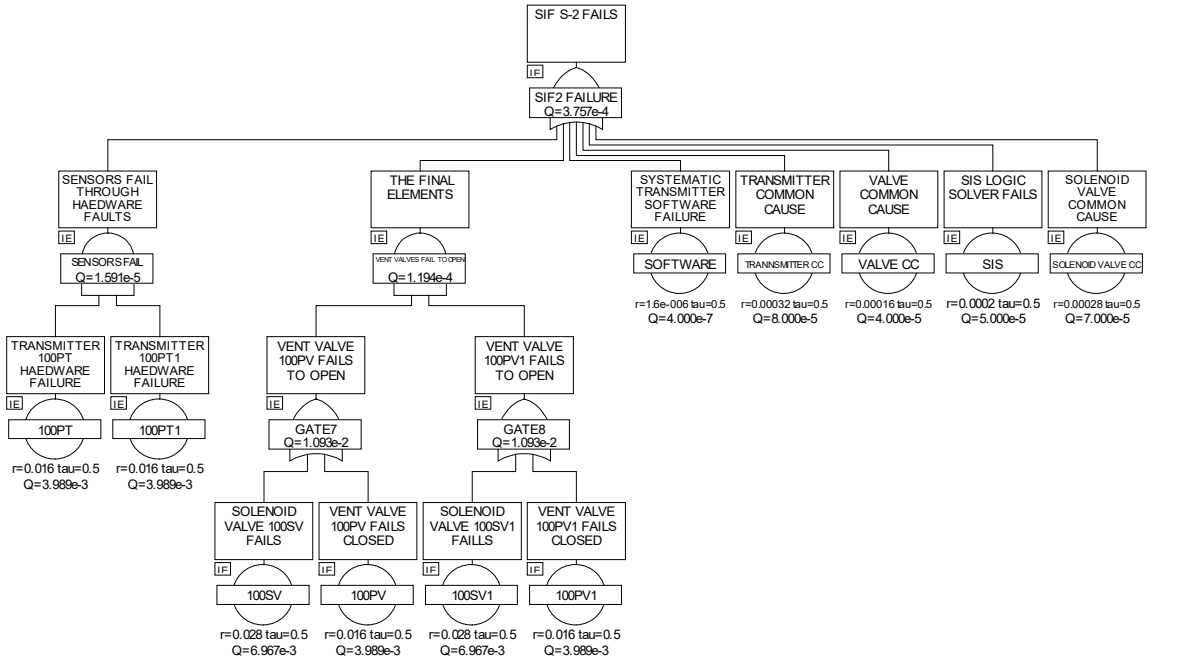
Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Figure F.6 – SIF S-2 Bubble diagram showing the PFD_{avg} of each SIS device

See Figure F.7 for the fault tree calculations.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Key

E Enabling event

Q Unavailability (PFD_{avg})

r Failure rate (failures/year)

tau Test interval (years)

Safety function S-2 has a PFD_{avg} rounded to 3,8e-4, therefore meets SIL 3.

Figure F.7 – SIF S-2 fault tree

SIF S-3

If the agitator seal pressure is greater than 10 psig open 100PV and 100PV-1. The required SIL = 2 (PFD_{avg} = 10^{-2} to 10^{-3}).

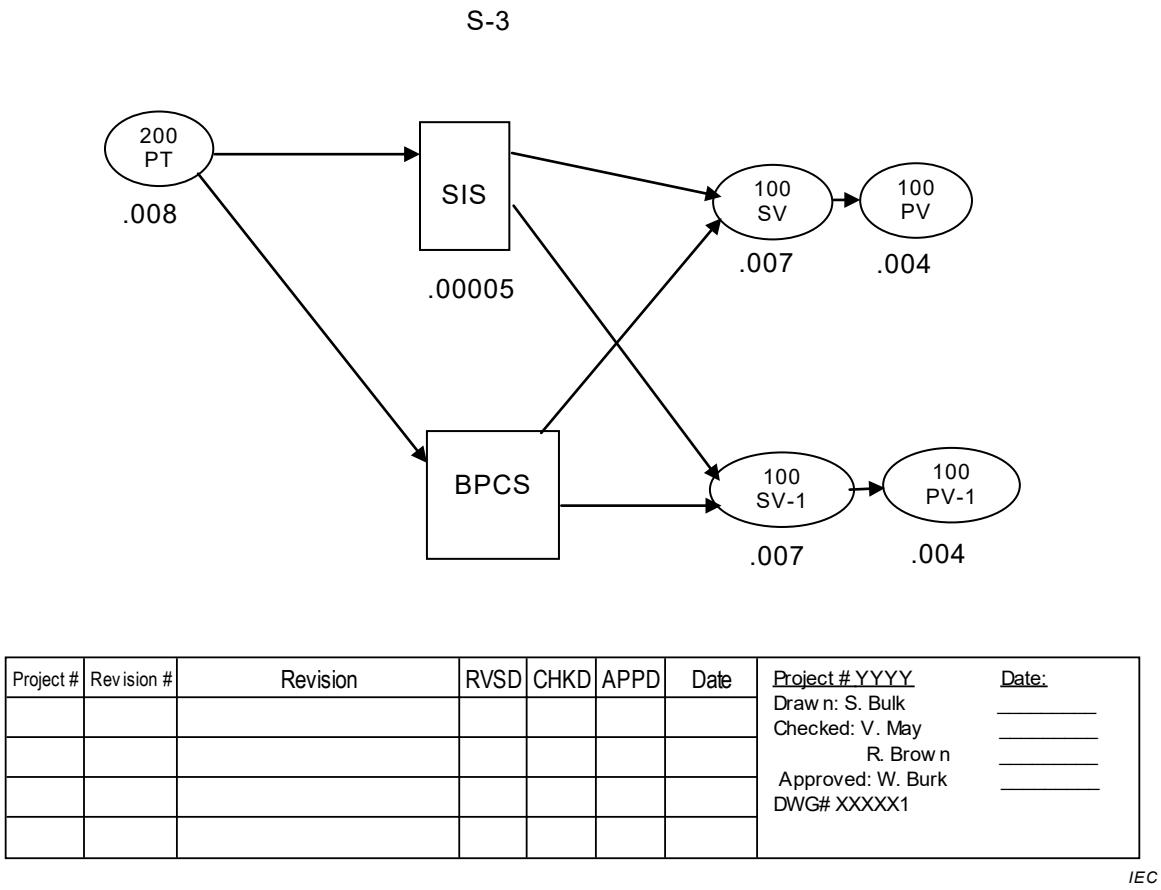
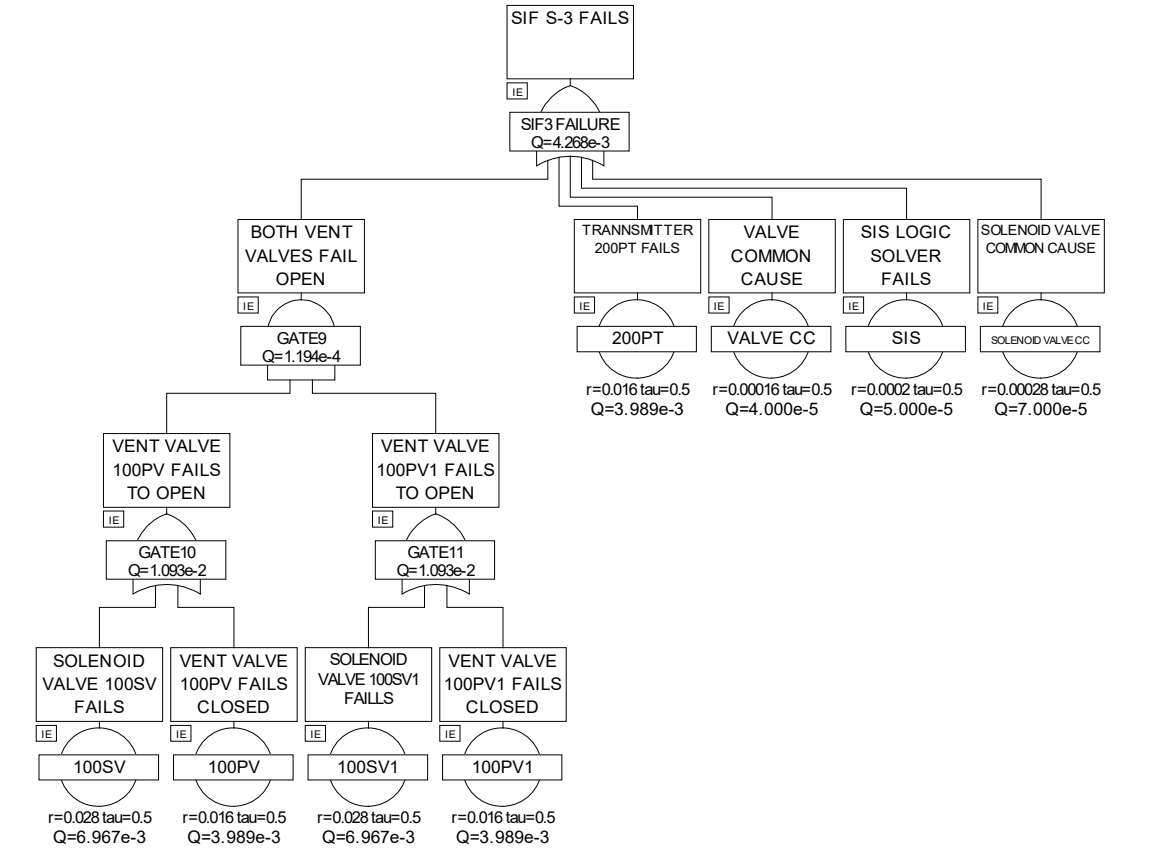


Figure F.8 – SIF S-3 Bubble diagram showing the PFD_{avg} of each SIS device

See Figure F.9 for fault tree calculations.



Key

E Enabling event

Q Unavailability (PFD_{avg})

r Failure rate (failures/year)

tau Test interval (years)

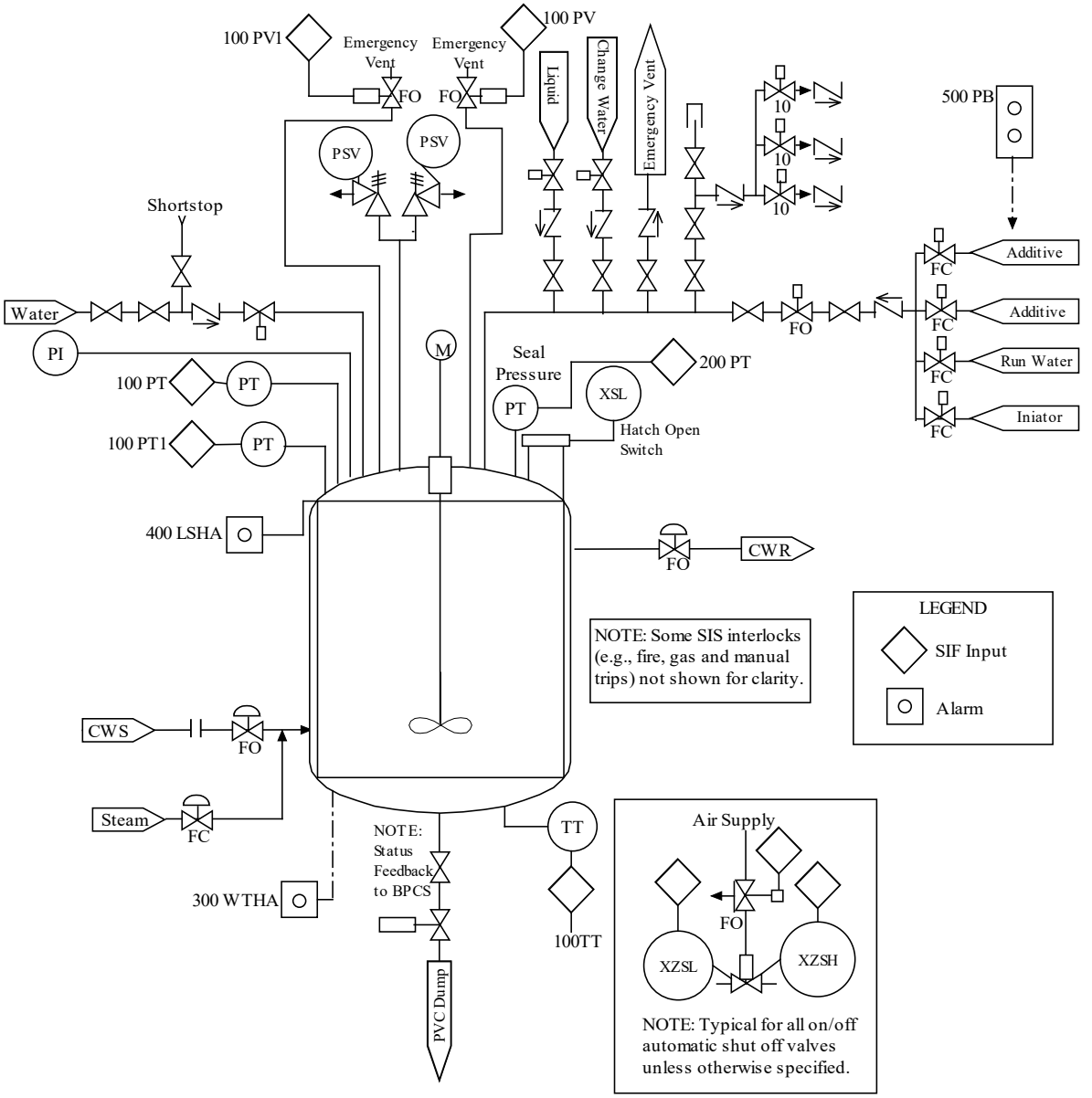
Safety function S-3 has a PFD_{avg} rounded to 4,3e-3, and therefore meets SIL 2.

Figure F.9 – SIF S-3 fault tree

F.16 Application program requirements

The SRS (particularly, the logic narrative (Subclause F.14.1), the cause and effect diagram (Table F.14), and the P&I diagram (Figure F.10)) were utilized to develop the AP requirements, as illustrated in the ladder diagrams (Figure F.11).

Ladder diagrams reflecting the functional requirements for each SIF are illustrated in Figure F.11, Sheets 1 through 5 inclusive. The ladder diagram also illustrates the electrical line voltage characteristics, grounding characteristics, circuiting requirements, and diagnostics to assist the designer/programmer in developing the AP.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Figure F.10 – P&ID for PVC reactor unit SIF

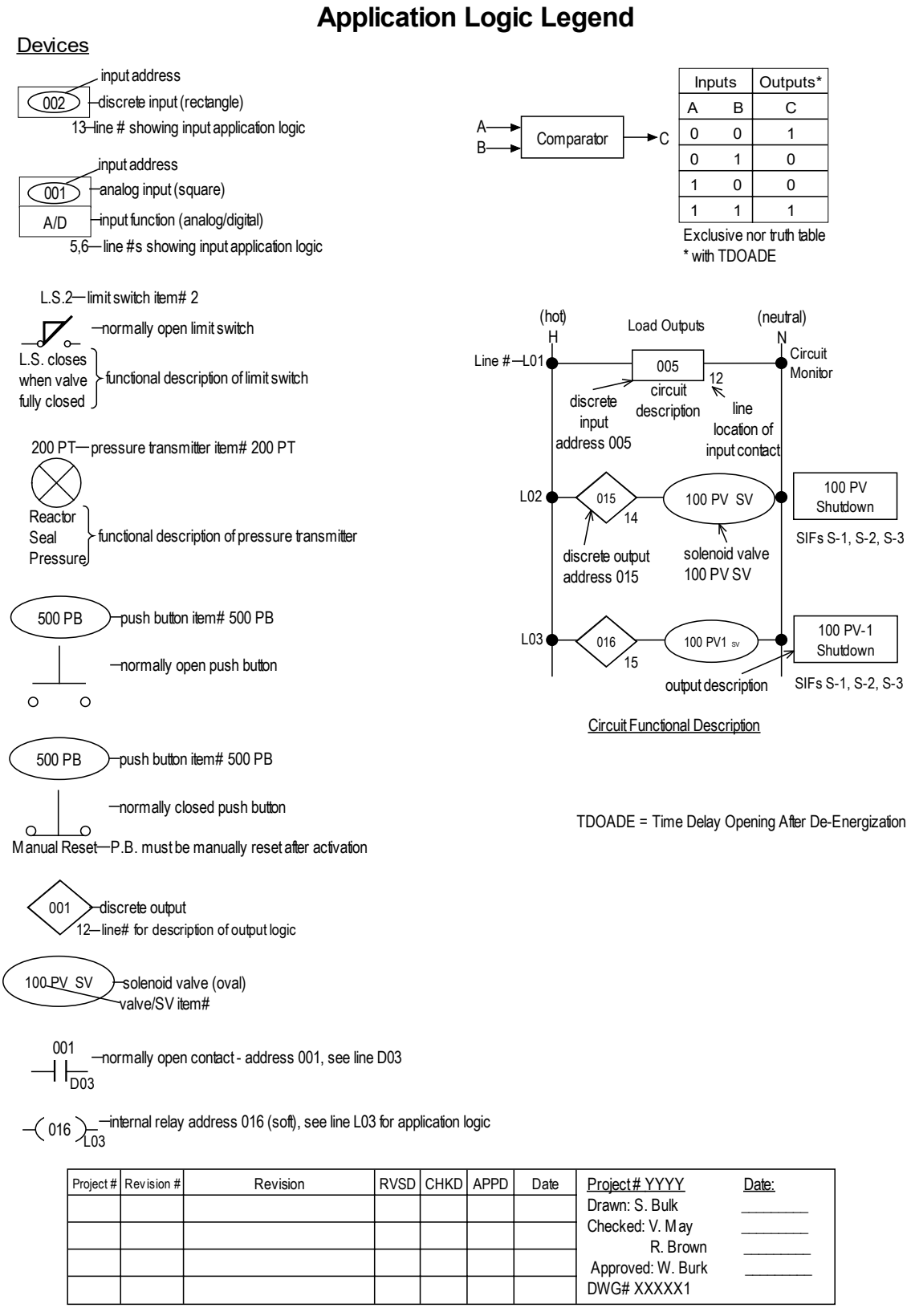
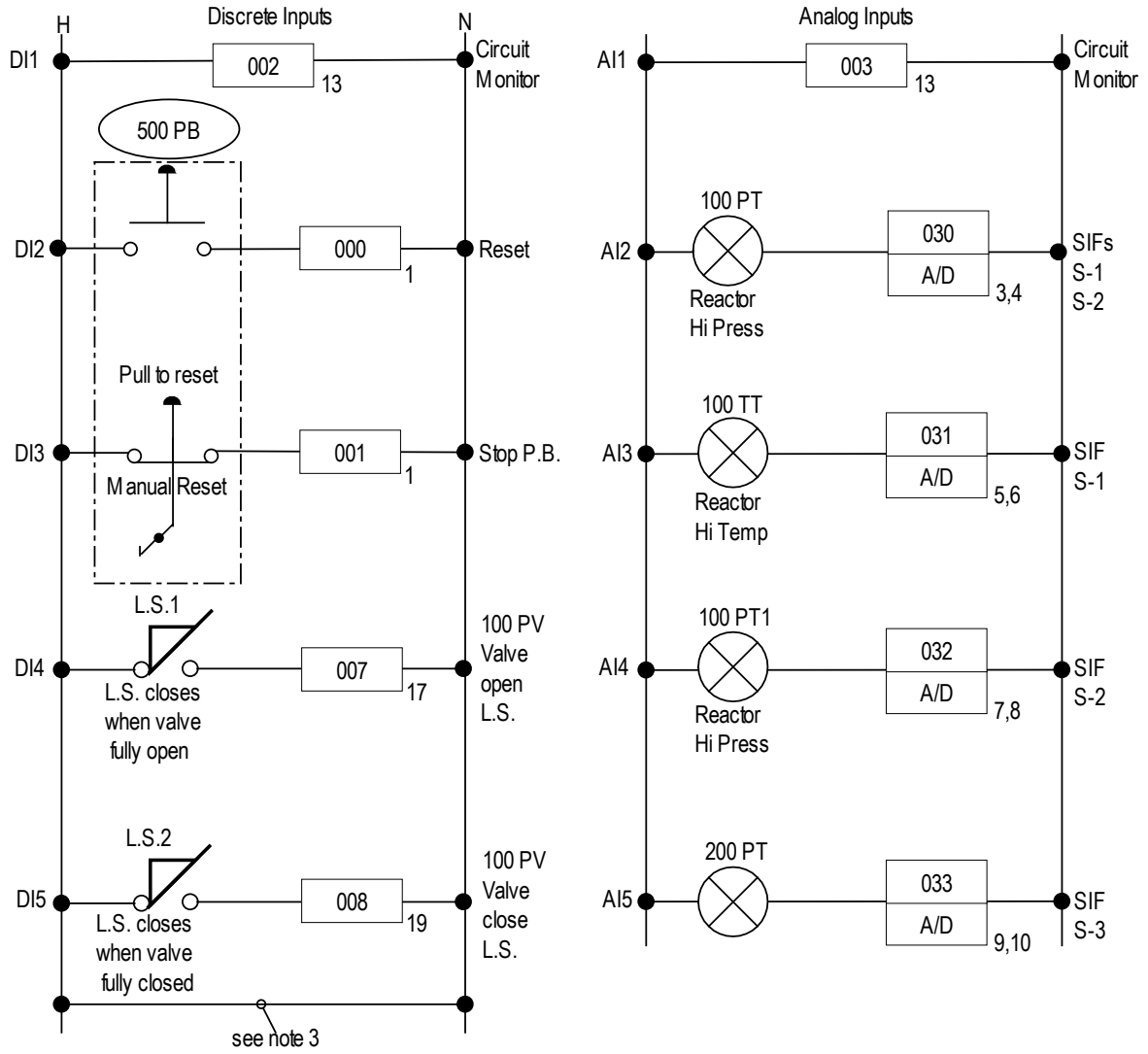


Figure F.11 – Legend *(1 of 5)*



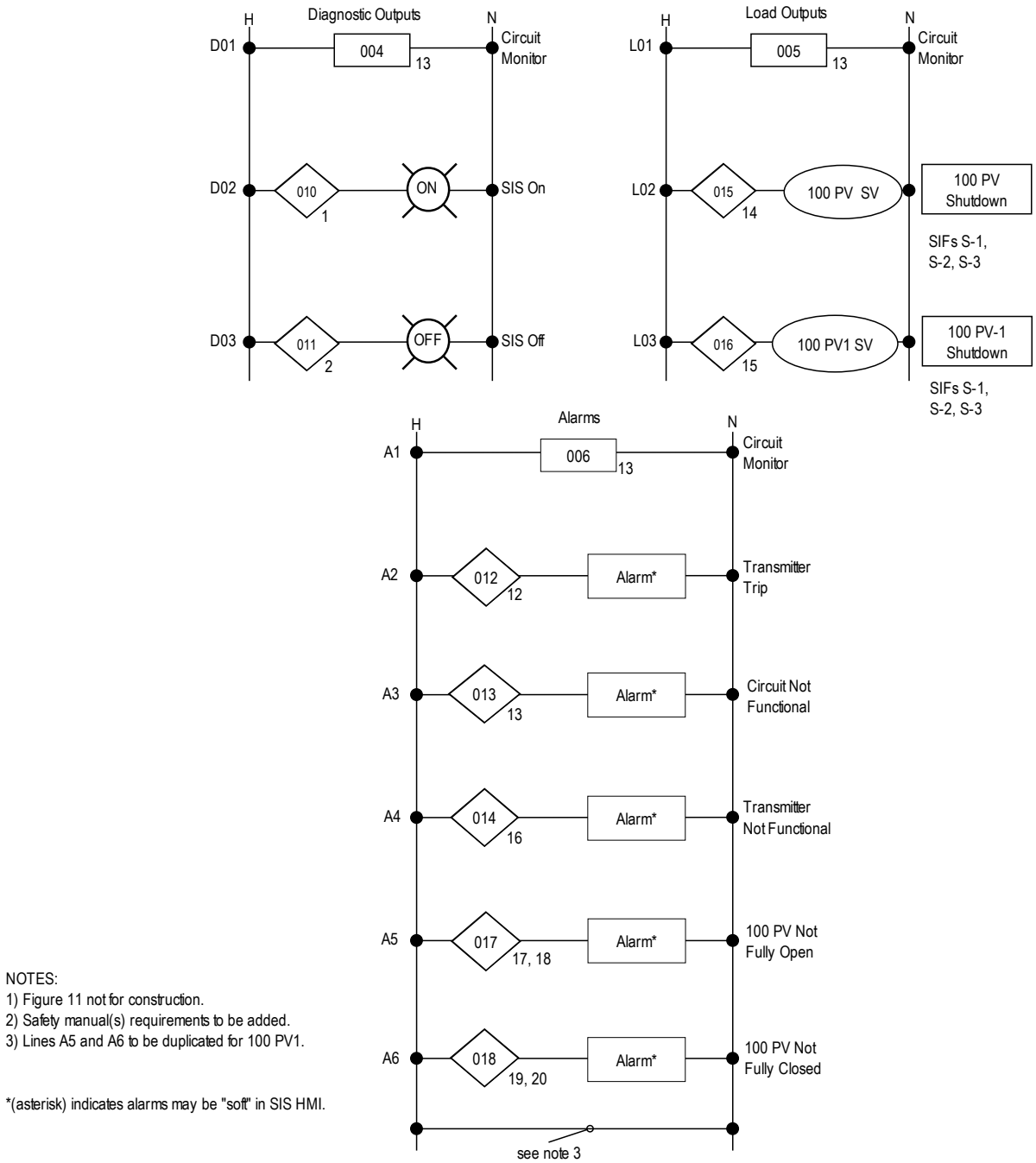
NOTES:
1) Figure 11 not for construction.
2) Safety manual(s) requirements to be added.
3) Lines D14 and D15 to be duplicated for 100PV1.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk
Checked: V. May
R. Brown
Approved: W. Burk
DWG# XXXXX1

IEC

Figure F.11 *(2 of 5)*



NOTES:
1) Figure 11 not for construction.
2) Safety manual(s) requirements to be added.
3) Lines A5 and A6 to be duplicated for 100 PV1.

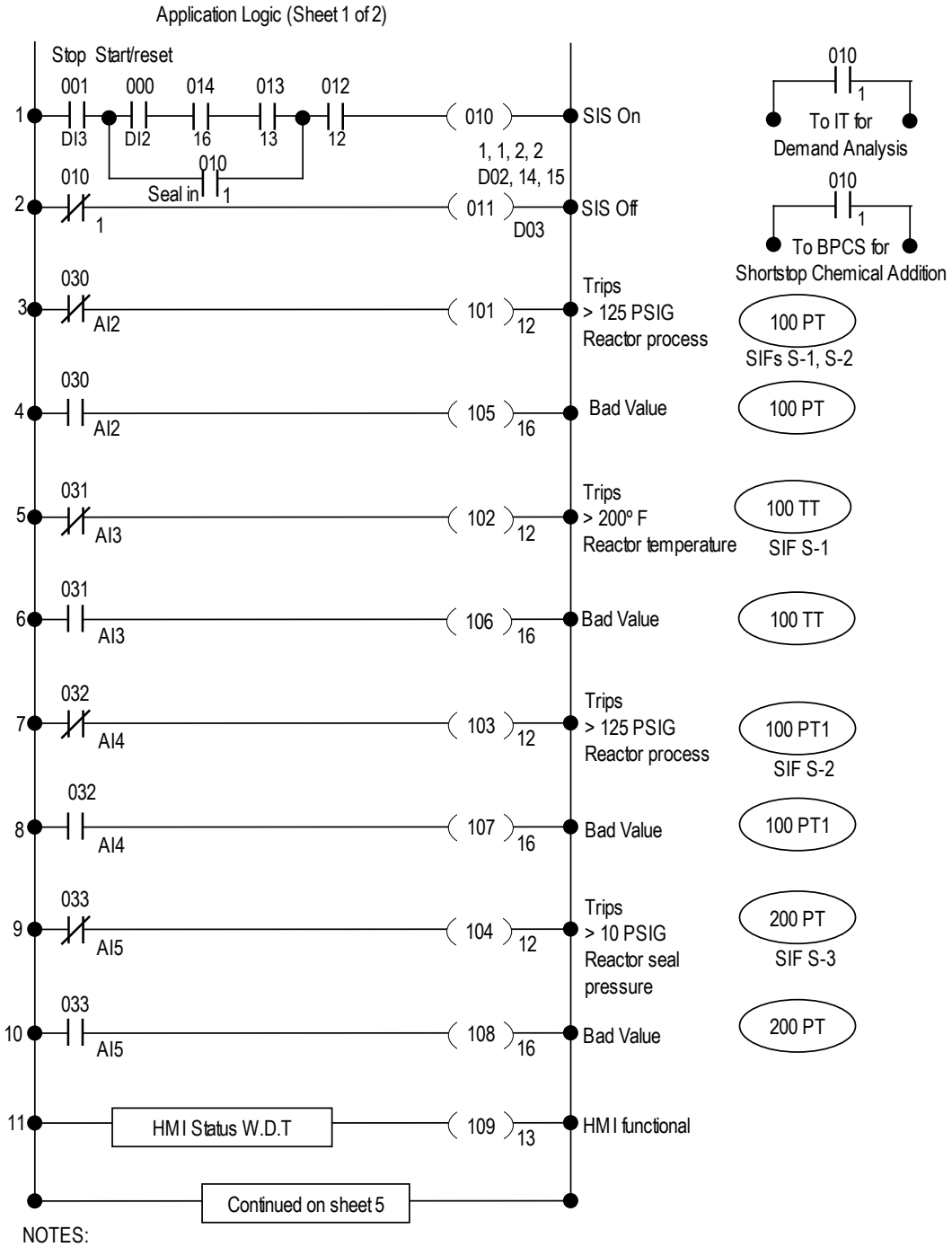
*(asterisk) indicates alarms may be "soft" in SIS HMI.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Figure F.11 *(3 of 5)*



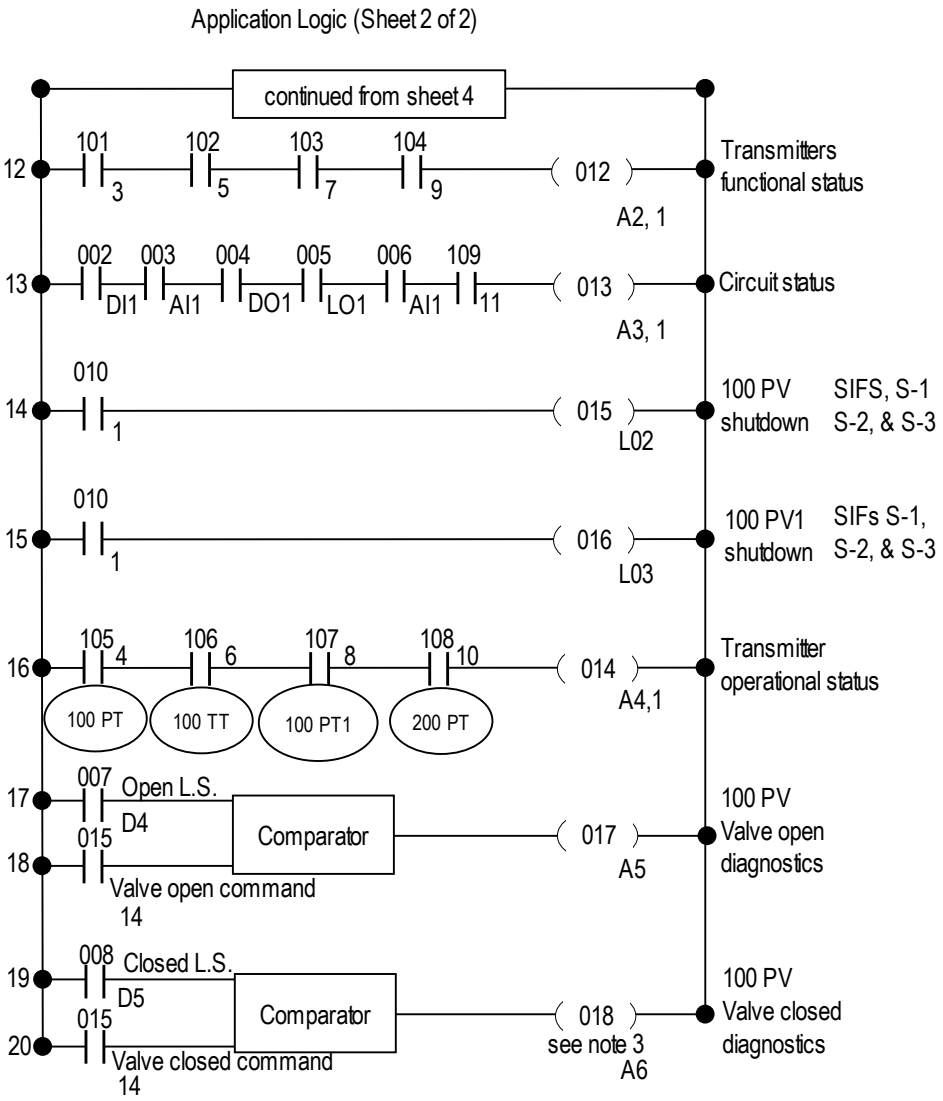
NOTES:
1) Figure 11 not for construction.
2) Safety manual(s) requirements to be added.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Figure F.11 *(4 of 5)*



NOTES:
1) Figure 11 not for construction.
2) Safety manual requirements to be added.
3) Lines 17, 18, 19, and 20 to be duplicated for 100 PV1.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Figure F.11 *(5 of 5)*

F.17 Step F.4: SIS safety life-cycle

Table F.16 – SIS safety life-cycle – Box 4

Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs
IEC 61511-1:2016 Figure 7, box 4	SIS design and engineering	To design the SIS to meet the requirements for SIF and safety integrity	11 and 12.4	SIS safety requirements AP safety requirements	Design of the SIS in conformance with the SIS safety requirements; planning for the SIS integration test

Table F.16 provides the objectives, inputs, outputs, and reference to the related clauses and subclauses for SIS design and engineering.

F.18 Technology and device selection

F.18.1 General

Clause F.18 lists some of the key parameters employed when selecting the technologies and devices in this example.

a) plant PHA team approves all devices used in SIS service;

b) low complexity devices with plant familiarity;

c) systematic capability with documented source;

d) maintenance and testing philosophy consistent with plant personnel capability/experience;

e) operator/maintenance interface based on existing plant criteria;

f) cost and schedule per project estimates and timing respectively;

g) use of BPCS for AP diversity (shadowing);

h) all technology selected has been previously used on plant (i.e., prior use) and is well understood by plant maintenance personnel;

i) failure modes and failure rates of each equipment piece (including data source) provided with documentation;

j) immunity to electromagnetic interference found in an industrial site;

k) vibration protection (e.g., circuit boards vibrating out of sockets, device and wiring failures) provided with each equipment piece.

F.18.2 Logic solver

The logic solver parameters included:

a) applied each item under “General” in F.18.1;

b) the SIS logic solver is IEC 61508 assessed with a systematic capability of SC 3. It uses a limited variability language (i.e., ladder logic) for application programming;

c) location of all logic solver devices in manufacturing building control room;

d) the process safety time for all SIF is long enough that typical PLC response times are adequate;

e) plant operating and maintenance experience (i.e., prior use) was considered in selecting the safety logic solver;

f) Appropriate integration with BPCS.

F.18.3 Sensors

Transmitters were used in lieu of discrete switches except for valve position switches, where proximity switches were used (to take advantage of non-contacting characteristic).

Transmitters were supplemented with out of range and improper output value diagnostics in the SIS and BPCS logic solvers.

Transmitter failure rate data was based on the systematic capability supplied with either the IEC 61508 assessment or IEC 61508 compliance data, and assumed that good installation practices were followed.

Individual taps were provided for each sensor.

Transmitters utilized are programmable (smart) devices with the following features:

a) Diagnostics, remote access to calibration information and on-board device description features providing an increased level of assurance that the corresponding device is in place and in working order.

b) Security feature(s) (e.g., write protect, password, keyed) to restrict access to calibration adjustments which could result in inadvertent changes that render the device incapable of performing its safety function.

c) Appropriate transmitter update time (i.e., time delay between a change in the process and the output response of the sensor is acceptable).

d) Where appropriate, transmitters are provided with drains, vents and test connection capability.

e) The 4-20 mA sensor outputs of the transmitters are direct connected to the SIS and parallel wired to the BPCS.

F.18.4 Final elements

The final control devices utilized are solenoid valves and emergency vent valves. Final control devices are de-energized-to-trip, and go to their safe states on loss of either air or electric utilities (i.e., emergency vent valves fail open).

Final control devices were selected based on prior use.

F.18.5 Solenoid valves

Solenoids are specified with the following:

a) high-temperature moulded coils, Class H or F to provide longer life in the continuously energized state (typical for de-energize to trip applications);

b) high and low operating temperature ratings of the solenoid meet or exceed the ambient conditions in which it will be installed;

c) capacity of the flow exit path from the valve operator to vent sized in order to satisfy the timing specifications of the application (valve response times under 10 seconds are sufficient);

d) turn-off rating of logic solver output(s) is sufficiently low to guarantee solenoid valve will drop out when outputs are in the “off” mode.

The mean time to dangerous failure (MTTFd) for solenoid valves was determined as follows:

1) prior use information was obtained from actual operating experience (internal and external) as well as through manufacturer-supplied data;
2) prior use information indicated that during 140 unit years of use in similar applications, two dangerous solenoid valve failures occurred (valve would not vent). Based on this, the lower 70 % confidence limit (see IEC 61511-1:2016, notes in 11.9.3 and 11.9.4) and TR84.00.04 -1, TR84.00.09) on the MTTFd was calculated at 38,7 years. A MTTFd of 35 years was selected for the PFD_{avg} calculations.

F.18.6 Emergency vent valves

Emergency vent valves are specified to ensure action of vent valves on loss of utilities and operating signals meets the functional safety requirements. Based on this and PHA evaluation of any different failure action requirements the emergency vent valves open on:

a) loss of power;
b) loss of air supply;
c) open signal from the SIS logic solver or BPCS logic solver to the solenoid valve.

In addition, the emergency vent valves have the following features:

1) visual indication of the valve's actual position is provided, including:
   – Local indication via valve stem position indicator
   – Remote indication of valve position via limit switches
2) spring return actuators are utilized. Actuator sizing and fail-safe spring design considerations include the proper analysis of the maximum required shutoff pressure.

NOTE For this application, globe valves were utilized, with flow under the plug.

Monitoring of each valve includes comparison of valve signal to valve position, supplemented by alarming.

F.18.7 Modulating valves

Modulating valves were not required for the SIF considered in this example.

F.18.8 Bypass valves

The PHA team analysis determined that bypass valves were not necessary since this is a batch process offering a number of off-line opportunities for maintenance. Operations and maintenance were consulted on this matter and they approved this approach.

F.18.9 Human-machine interfaces (HMIs)

F.18.9.1 General

The logic solver interface capability was designed to allow for a functionally safe interface to the BPCS for shadowing, operator interface, alarming, diagnostics and interchange of specific values.

The following was implemented in the SIS interfaces to the BPCS:

- use of redundant HMI console;
- use of redundant communication links;
- use of an internal communication watch-dog timer for interfaces handling critical data e.g., all data to the BPCS operator console);
- the shutdown pushbutton (500PB) was mounted on one of the HMI consoles, and equipped with a plastic safety cover to avoid inadvertent shutdowns.

Factors considered in the design of the operator interface include:

- alarm management requirements;
- operator response needs;
- good ergonomics.

Changes to the AP (including trip settings) of the SIS can only be made through the SIS engineering consoles with appropriate security measures (Clause F.22).

F.18.9.2 Alarm management

Alarm management ensures that problems and hazards are presented to the operator in a manner that is timely and easily identified and understood by using alarm prioritization. Alarm prioritization reflects the site's alarm management philosophy. Features implemented include:

- alarms for which risk reduction credit is taken in the LOPA have the highest priority. These alarms (300WTHA and 400LSHA) should be checked at the same twice-per-year frequency as the SIS;
- pre-trip alarms that initiate operator action prior to SIS action have the highest priority;
- use of BPCS operator interface features to distinguish the different priority level alarms;
- use of pre-trip and trip alarms to help define operator response requirements;
- SIS diagnostic alarms are displayed on a separate graphic in the HMF.

F.18.9.3 Operator response

The ability of the operator to respond to HMI-initiated alarms requires the following implementations:

- Use of sequence-of-events (SOE) recording: The normal scanning time of the BPCS provides true first-out alarm functionality;
- Use of pre-trip alarms: The operator may take corrective action before a trip occurs (e.g., adding shortstop to prevent runaway reaction). In these cases pre-trip alarms are provided. Pre-trip alarm and trip settings take into account process dynamics and sensor response.

F.18.9.4 Human factors

"Human factors" refers to the interface design parameters that can affect the ability of the operator to effectively identify and respond to alarm and status information. Design factors implemented include:

- consistent use of colors, lights, types, shapes, and sizes of switches, location of switches, etc.;
- use of a switch guard over the operator shutdown switch (500PB) to reduce the possibility of accidental operation;
- mechanical operation of the operator shutdown switches (pull to reset).

F.18.10 Separation

F.18.10.1 General

Subclause F.18.10 describes the separation inherent in the design of each SIF.

Separation is provided to reduce common cause faults and facilitate addressing security issues that may arise because of inadvertent changes. These types of problems could make the SIS and BPCS unavailable at the same time. To address these concerns, design approaches consistent with the plant's training and successful prior use experience are implemented.

F.18.10.2 Power sources

Separation of the SIS I/O power from non-SIS power circuits should be implemented by using a separate distribution transformer for the SIS instrument power panel branch circuits. This provides a defence against common cause faults related to grounding problems. SIS power source distribution is further separated to ensure redundant power sources (i.e., normal and uninterruptible power supply (UPS)) are routed physically separate and branch circuits partitioned to address inputs, logic solver, I/O power supply(s), load outputs, and diagnostic outputs.

Separate raceway systems (e.g., conduits, cable trays, ducts, and wire-ways) are not required because electro-magnetic compatibility (EMC) issues are addressed consistent with good engineering practices for:

- maximum application energy levels (480 V and below);
- cable/raceway/equipment specification and spacing;
- separation of power and instrument signals conductors (i.e., 4-20 mA) into different cables;
- unique identification (i.e., colour coding) of SIS equipment;
- covering of SIS terminal connection points;
- computerized cabling installation program identifying each conductor, cable, raceway, and connection point.

F.19 Common cause and systematic failures

F.19.1 General

The following F.19.2 to F.19.19 define the design provided to address common cause and systematic failure issues.

Design techniques implemented to avoid common cause failures include separation, redundancy, diversity, and peer review.

Techniques used to avoid systematic errors include peer review, use of design approaches with a good prior use track record, diversity, and comparison diagnostics.

F.19.2 Diversity

Diversity was achieved by the use of different equipment (SIS & BPCS logic solvers), different designs to perform a common function (SIS AP & BPCS shadowing), and different embedded and AP and programmers.

F.19.3 Specification errors

Specification errors (e.g., wrong ambient temperature range, incorrect parameter [e.g., 0 °C when 0 °F is intended], improper metallurgy for a group of instruments) were identified and corrected through the use of peer review by personnel familiar with the subject matter under review.

F.19.4 Hardware design errors

Hardware design errors were addressed through the use of SIS equipment that meets prior use criteria with either IEC 61508 assessment or IEC 61508 compliance data or plant approval analysis. The design adheres to corporate best practices, the safety manual for each certified device, and the application manual for non-certified devices, and included peer review.

F.19.5 Software design errors

PE equipment was selected for use based on prior use and either IEC 61508 assessment or IEC 61508 compliance. AP in the BPCS was utilized to “shadow” the SIS AP, thus gaining the advantage of diverse embedded software.

To reduce systematic failures due to embedded software faults, a compare of the two pressure sensors and a high and low limit check were configured in both the SIS and the BPCS.

Control of AP systematic errors were addressed by implementing several of the techniques and measures listed, including:

- limited variability language for all application programming, unless fixed variability programming was available (e.g., PE based transmitters, PE based operator consoles);
- a logic documentation scheme (see Figure 11) that could be interpreted by all involved personnel, providing self-explanatory process-related documentation embedded in the AP documentation;
- peer review and simulation tools were used to reduce the AP design errors;
- “shadowing” to continuously monitor the AP performance and provide diversity of programming;
- manufacturers’ safety manual requirements.

F.19.6 Environmental overstress

The facility design does not consider earthquakes or airplane crashes, but is specified to withstand a level 5 hurricane. The environmental conditions to which the SIS will be exposed that were addressed include:

- temperature;
- humidity;
- contaminants;
- vibration;
- grounding;
- power line conditioning;
- electro-magnetic compatibility (EMC).

F.19.7 Temperature

SIS devices, such as logic solvers, I/O modules, sensors, and final elements, are adversely affected by temperature extremes. Temperature related design decisions that were implemented in the design include:

- operating temperatures specified by manufacturers;
- location of equipment in areas where temperature excursions are kept within manufacturers’ specifications;
- weather protection and temperature control for outdoor equipment;
- use of drip legs or drains, or drying the instrument air to reduce the potential of failures due to ice formation should be implemented as appropriate;
- heat tracing where required.

F.19.8 Humidity

Relative humidity should be maintained per manufacturers’ requirements (typically below 90 % for electronic systems). To reduce harmful effects of high humidity (e.g., steam,

outdoors), electronic assemblies should be protected by applying conformal coating and by using an anti-wetting “contact lubricant” to ensure a gas-tight connection between connectors.

F.19.9 Contaminants

To protect against potential contamination, the following should be provided:

- adequate ventilation and dust protection of the immediate environment;
- where corrosive atmospheres are a concern, either installation of filters or adsorbent materials are provided for the HVAC system, and (air) purge is implemented for all other equipment;
- for field-mounted electronics, the use of purged cabinets and/or conformal coating and some form of contact protection at connectors.

F.19.10 Vibration

The building does have some vibration. To counter this problem all SIS plug-in devices (e.g., “ice cube” relays, I/O boards) are provided with positive latching mechanisms. The SIS logic solver cabinet utilizes vibration isolation mounts to minimize the transmission of vibration from the cabinet to the logic solver.

F.19.11 Grounding

The grounding was designed to facilitate use of programmable electronic technology by implementing:

- ground system resistance below 5 ohms;
- use of Ufer system (footing) grounds;
- electrically continuous building steel;
- upgrade of building steel “cone of protection” with copper conductors where required.

F.19.12 Power line conditioning

Power line conditioning was designed to provide protection to the SIS from power line abnormalities such as outages, lightning, dips, sags, brown-outs, surges, and spikes.

Lightning protection is provided by the implementation of protection devices that are:

- coordinated to the withstand capability (e.g., short circuit, overload) of the devices being protected;
- located to protect each SIS device as well as cone of protection.

The existing power distribution system does have harmonic content. The SIS power distribution system was designed to provide protection against harmonics.

SIS overload and short circuit protection were provided with the following features:

- individual fusing of each I/O circuit to limit the effect of a fault in that circuit;
- coordinating the branch fuse with the circuits feeding the branch to minimize the possibility of a larger part of the I/O structure being disabled by a low level fault.

F.19.13 Electro-magnetic compatibility (EMC)

Electronic and programmable electronic systems use low level signals, digital circuits, microprocessors, memory chips, etc., that are susceptible to electrical noise e.g., electro magnetic interference (EMI). The EMI generated by personnel communication systems, such as handheld two-way radios, base station radios, cellular phones, personal computers,

wireless modems, and variable frequency drives was evaluated during design. The SIS was designed to address this issue by implementing the following features:

a) electronic enclosures provided the SIS protection from external (outside the cabinet) noise sources;

b) raceway and cable design provided the SIS with protection from internal (inside the cabinet) noise sources;

c) noise filters were provided where required.

Additional EMI reduction techniques included:

1) metallic enclosures;

2) metal barriers;

3) cable and wire shielding;

4) twisted pair wiring;

5) proper grounding;

6) proper device location;

7) wiring routing away from EMI source;

8) separation.

SIS equipment selection criteria required that the equipment be capable of withstanding EMI levels typically existing in an industrial environment. This was accomplished by:

- specifying equipment that was designed, built, and tested in accordance with applicable standards (e.g., IEC 61131, TUV);
- installing the equipment consistent with manufacturers' installation guidelines.

F.19.14 Utility sources

Electricity and instrument air are key utilities servicing the SIS. The content and quality of their design is directly related to their availability to service the SIS. Regardless of the design, it was assumed during the PHA that parts or all of these utilities would not be available.

The electrical utility and plant personnel (e.g., power house, other operating processes) were consulted to determine the availability of existing utility sources. Based on these findings the utility sources were designed with features to improve availability, including:

- Instrument air
  - used clean, dry instrument quality air;
  - provided sufficient pneumatic power capacity to final control devices to ensure adequate operating time for the final control devices;
  - pneumatic vents provided with protection against plugging, dirt, insects, and freezing;
  - length and diameter of pneumatic power and signal tubing sized to provide satisfactory performance.
- Electricity
  - used redundant power source for SIS logic solver, inputs, HMI, and diagnostic outputs;
  - provided time delay under voltage protection (30 cycles) for motor loads;
  - alternate power source has the same power quality as the primary source;
  - located alternate power sources (e.g., UPS) so that each can be maintained without impacting the performance of the other;
  - SIS was designed with start-up permissive that requires availability of all SIS electrical circuits.

F.19.15 Sensors

Separate taps are used for each sensor to minimize common cause failures.

F.19.16 Process corrosion or fouling

This process has limited potential for reaching abnormal process conditions leading to corrosion. It is also a batch process, which facilitates clean outs between process runs. No special design requirements were implemented.

F.19.17 Maintenance

Maintenance organization participated in the planning, verification and approval of the design. Special attention was placed on design as it related to calibration, training requirements, bypassing, and testing.

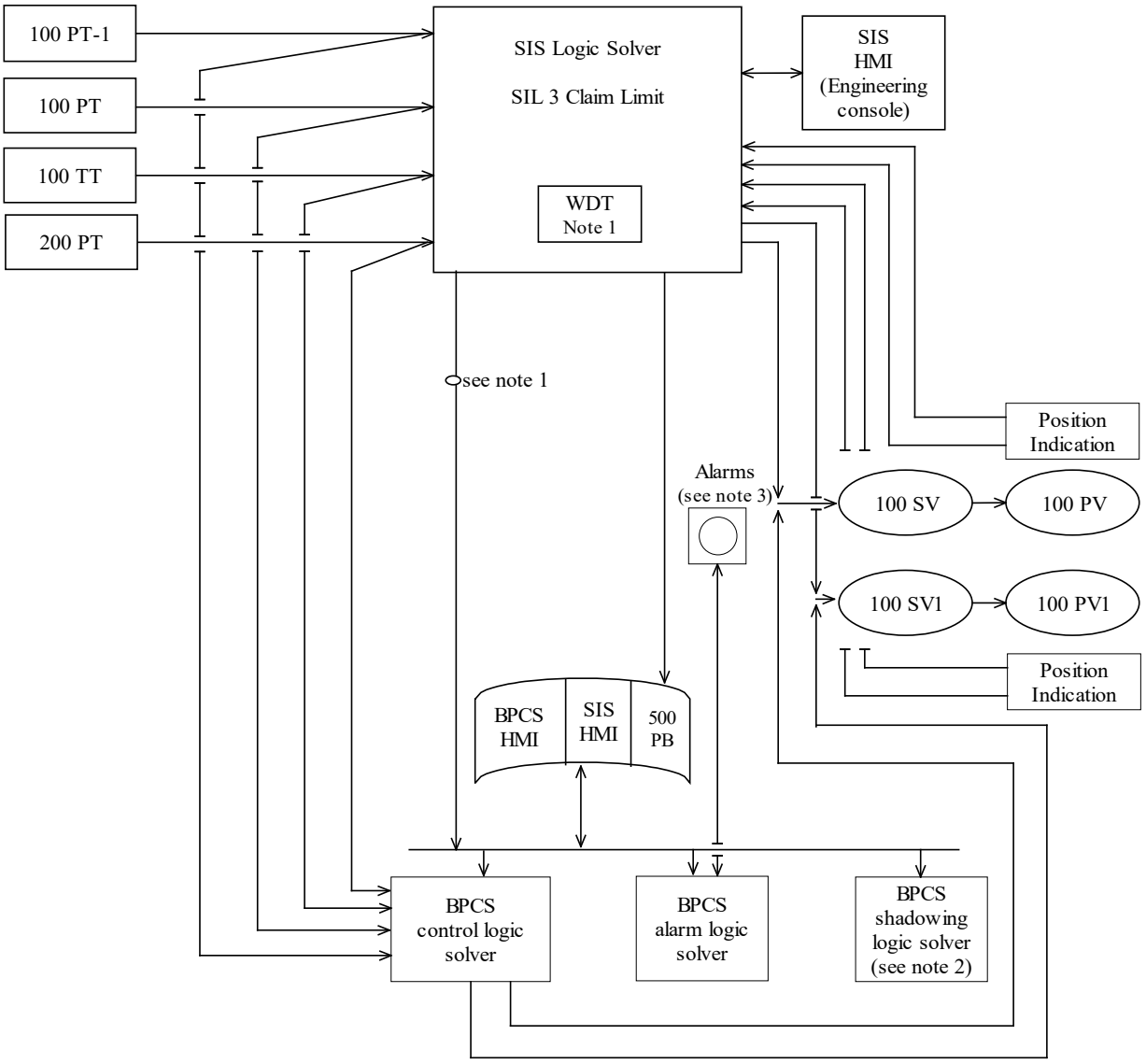
F.19.18 Susceptibility to mis-operation

Operations organization participated in the planning, verification and approval of the design. Special attention was placed on design as it related to contributing to simplified operating procedures, minimizing operator intervention requirements in the production run, having appropriate modes of operation to ensure ability to terminate a batch at key intervals, testing of AP to ensure it meets process needs, and confirming that alarm management /HMI issues were addressed to their satisfaction.

F.19.19 SIS architecture

The following discusses the SIS architecture. Figure F.12 provides the SIS architecture. The purpose of F.19.19 is to illustrate the SIS architecture with its relationship to outside influences (e.g., BPCS, HMI, process sensors and final elements).

The BPCS communicates with the SIS over a data highway. However, security requirements mandate that SIS setpoint changes and SIS configuration changes can only be made through the dedicated SIS engineering console. The SIS engineering console should be connected directly to the SIS from the control room whenever changes are made to SIS setpoints or configuration



Note #1 - Communication link to the SIS HMI is supplemented with a communication WDT ensuring SIS HMI is functional during the operational cycle.
Note #2 - Shadowing of SIS application software.
Note #3 - Weigh cell & level alarms (300 WTA & 400 LSA [see figure 11]).

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Figure F.12 – SIS for the VCM reactor

F.20 SIS application program design features

AP documentation incorporates comments that are detailed enough to explain the function of each symbol, the function of each SIF, and the relationship of each symbol to its SIF. The comments are sufficiently complete to assist engineering and maintenance personnel in understanding the AP functions, as well as navigating within the AP.

F.21 Wiring practices

Good wiring practices are essential to ensuring desired SIS availability is achieved. Following is a list of wiring practices that were implemented in this SIS:

- Circuits do not share neutral conductors or DC common returns in order to minimize the:
  - possibility of inadvertent interruption of a circuit(s) if a neutral or common is lifted or opened;
  - potential for ground loops and wiring errors;
  - additional (10 % spare, 20 % space) branch circuits are provided.
- I/O fusing features include:
  - the use of individually fused I/O circuits to better isolate faults and minimize potential common cause effects;
  - the use of isolated type I/O;
  - the use of external fusing (i.e., external to the PLC I/O fusing) where required and where card removal can be minimized;
  - the use of fuse holder terminal blocks (with integral fuse holder/disconnecting lever) as a means of providing a disconnect for maintenance purposes.
- The use of EMC resistant transparent glass to allow visual access to diagnostic information (e.g., I/O lights).
- Internal (i.e., inside SIS logic solver cabinet) lighting and twist-lock receptacle for SIS to eliminate plugging in inductive devices.
- SIS terminations are identified when located near non-SIS terminals.
- Twisted pair wiring was used to minimize magnetic and common cause noise where required.

F.22 Security

The security measures taken with respect to the SIS design maintain safety integrity by preventing unauthorized or inadvertent modification of any of the SIS functions or devices including the logic solver, the application logic, the user interfaces, sensors and final elements. For those devices (e.g., interface devices) where it is more difficult to control physical access, the use of administrative procedures should be implemented.

Some basic security approaches implemented were:

- written approval with reasons for access;
- written approval with persons requiring access identified;
- definition of required training and/or familiarity with the system before access is permitted;
- definition of who is to have access to the system, under what circumstances, and to perform what work. This included the procedures needed to control the use of maintenance bypasses.

SIS features that facilitate access control. Examples of such design features include:

- clear identification of SIS devices via distinctively colored labels;
- physical separation of SIS and BPCS equipment (making it easier to secure the associated enclosures with key-locks);
- use of a diverse technology (which would typically require a different maintenance interface).

The use of PES based SIS introduced additional security concerns because of the relative ease of making changes in the application logic. For these systems, additional features were implemented including:

- restricting access to the maintenance/engineering interface;
- establishing administrative policies/procedures that define the conditions under which the maintenance interface may be connected to the system during normal operation;
- use of virus checking software and appropriate program and file handling procedures in the engineering console to help avoid corruption of the embedded and/or application logic;
- the use of SIS utility software that tracks revisions in the application logic and allows the determination (after the fact) of when a change was made, who made the change, and what the change consisted of;
- no external connections of the SIS or BPCS to the internet or phone lines.

F.23 Step F.5: SIS installation, commissioning, validation

Table F.17 – SIS safety life-cycle – Box 5

Safety life-cycle phase or activity		**Objectives**	**Requirements clause or subclause of IEC 61511-1:2016**	**Inputs**	**Outputs**
IEC 61511-1:— Figure F.7, box 5	SIS installation commissioning and validation	To integrate and test the SIS To validate that the SIS meets in all respects the requirements for safety in terms of the required SIF and the required safety integrity	12.3, 14, 15	SIS design SIS integration test plan SIS safety requirements Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS design results of SIS integration tests Results of the installation, commissioning and validation activities

Table F.17 provides the objectives, inputs, outputs, and reference to the related clauses and subclauses for SIS installation, commissioning, and validation.

F.24 Installation

The SIS installation began with the availability of design, building facility, process equipment, utilities (e.g., electrical) and instrumentation equipment. The installation ended with the transition (i.e., turnover) of the SIS from construction to operations. This transition reflected acceptance by operations; at this time commissioning was begun (see Clause F.24).

The corporate purchasing and receiving inspection functions were considered adequate to ensure that the specified SIS devices were received in good working order, with appropriate documentation to support their use per 11.5 of IEC 61511-1:2016. Interim storage adheres to the manufacturer's safety manual for each device and includes any necessary preventative maintenance for the equipment.

Note that a procedure was available to transition back to Installation mode so that corrections to problems found by operations could be implemented; this transitioning resulted in adjacent equipment being in different states of completion/acceptance (i.e., Installation versus operations state). For this project a white tag was used for operations state and a green tag for construction state.

Each instrument was identified with its instrument tag number. The SIS was provided with the following additional identifying characteristics:

- all SIS instrumentation provided with a visual identification (i.e., painted red) of its status as a SIS device;
- SIS cabinet provided with nameplate referencing SIS drawing numbers;
- SIS HMI(s) identified (software faceplate identification) as SIS related devices;
- each SIF device was identified with a label showing its loop drawing #, and SIF #.

Construction was not involved with the installation of AP. The AP was developed, tested, and verified during design and was introduced into the SIS during commissioning.

Construction verification activities prior to turnover to operations included:

- “ring out” installed wiring to ensure proper grounding and SIS interconnection;
- energize the controls (thus ensuring no shorts or overloads) including I/Os;
- “bump” (e.g., short “jog” activation) each motor and each valve to ensure operation in the correct direction;
- ensure all utilities (e.g., pneumatics) are functional;
- do a “walk-through” to verify installation was complete, safe, and correct;
- provide complete and “as built” documentation of the SIS.

Operations participated in the above verification activities so that operations:

- understands the battery limits and location of the SIS devices;
- understands the location of utilities and their critical devices (e.g., disconnect, overload and short circuit protection (e.g., fuses, circuit breakers));
- could provide the necessary detail to their commissioning plan (see clause F.25);
- maintenance became familiar with the SIS installation by working under construction supervision to perform selected SIS verification activities discussed herein (e.g., “ring out” SIS).

The completed installation was verified and approved by an inspection team composed of construction, operations and design personnel. When complete, the equipment was tagged to reflect operations acceptance and ownership (i.e., responsible for equipment).

F.25 Commissioning

The term commissioning identifies the period of time beginning after completion of turnover (i.e., from construction to operations) and ending with the verification that the SIS commissioning is complete and can proceed to validation (see Clause F.27). For this example, commissioning of the SIS began immediately after the BPCS was commissioned.

SIS commissioning involves the identification, scheduling, planning, organizing, supervision, and documentation of SIS hardware system checkout, and operating system(s) (i.e., embedded software) checkout.

Commissioning of this example SIS is also referred to as “checkout” since this term better reflects the major activity implemented in commissioning. Checkout is a step-by-step procedure that ensures:

- all SIS connectivity is correct (including grounding);
- all utilities (e.g., electrical, pneumatic) are functioning properly;
- all SIS devices (e.g., sensors, logic solver(s), final elements, HMI(s), engineering stations, communication systems) are energized and functioning properly;
- sensor settings are correct.

Devices with fixed programming languages (FPL) (e.g., smart transmitters) were checked at this time. The PE logic solver engineering station and its “force” function were utilized during checkout. Plant maintenance were key participants in this activity, with support from construction and design as needed. Operations approved commissioning as complete and satisfactory before proceeding to validation.

F.26 Documentation

Necessary documentation should be available to personnel. As a result, a check was performed to ensure that all documentation was available and correct, before proceeding to validation.

The final list of approved documents included:

- H&RA documentation (What Ifs (Table F.4), HAZOP (Table F.5));
- tolerable risk ranking (Table F.8);
- documentation of risk allocation to protection layers – determination of SIL for each SIF (LOPA);
- test procedure for each SIF (see Clause F.27);
- safety requirement specification including:
  - P&I diagrams;
  - logic diagrams;
  - AP printout;
  - safety manuals;
  - assessing body safety justification;
  - equipment selection justification method documentation;
  - manufacturer installation instructions;
  - SIS hardware/AP/installation/maintenance documentation;
  - systematic capability justification;
  - SIL verification calculations (i.e., PFD_{avg}) for SIF including bubble diagrams.

F.27 Validation

The term validation identifies the period of time beginning after completion of commissioning and ending with the conclusion that the SIS meets the functional requirements defined in the SRS.

Validation of the SIS began after the SIS was commissioned and the BPCS was validated.

SIS validation involved the identification, scheduling, planning, organizing, supervision and documentation of a number of activities. These activities included SIS:

- hardware system run-in;
- operating system(s) (i.e., embedded software) run-in;
- AP run-in;
- start-up (acceptance test approval and turnover to production, i.e. a division of operations).

Validation of this example SIS was subdivided into “run-in” and “start-up” to better reflect the major activities implemented in validation.

Run-in is a step-by-step procedure that ensures the SIS is functionally correct by using non-hazardous process materials (e.g., water in lieu of hazardous liquid) while operating the process as though it were making finished product. To allow this to occur, the SIS logic solver AP was installed (see Clause F.23) and tested (see Clause F.27) thoroughly through all its modes of operation (e.g., start, run, stop). Production personnel were key participants at this time with support from maintenance and design. Upon successful completion and Operations' approval of run-in, the SIS was turned over for start-up.

Start-up is an activity that requires operations to safely produce a quality product at a pre-approved rate of production. During this procedure the SIS devices were checked to ensure they were functioning properly and were capable of performing their safety function as established during run-in. Once this was satisfactorily completed, results were documented, and operations approval was finalized. Validation of this SIS project was complete.

F.28 Testing

Much of the required testing discussed in Clause F.28 was done during initial validation of the SIS. The test procedures described below are also used for the periodic testing and inspection described in Clause F.29, Step 6.

The test procedure was written by the designer of the SIS. The procedure included recognition of the potential for safety incidents as the result of SIF testing. As a result the test procedure was explicit in how to safely proceed with the test and the quantity/quality of required equipment and personnel.

Included in the tests were the following activities:

- device tests;
- shop-testing and calibration;
- simulation;
- logic tested separately;
- automatic testing;
- manual testing;
- documentation of "as-found" and "as-left" conditions;
- detailed step procedure.

There were some key features that were tested beyond just the trip setting and the final control devices. Diagnostics, such as loss of signal, were tested, whether the diagnostics generate alarms or take the process to a safe state. SIF latching and reset logic were tested, including the position of final control device on reset. The reset position was documented and tested.

The SIS interaction with the BPCS was tested. SIF indications sent to the BPCS were tested as well as any actions taken on the indications. BPCS shadowing the SIS logic was tested independently to prove both systems work as designed.

A general procedure for SIF testing follows:

- Bypass other SIF that should be cleared to test the target SIF.
- Simulate normal operating conditions:
  - simulate instrument signals at normal operating conditions;
  - put the target final control devices in the normal operating position;
  - put controllers and other devices in the normal operating mode.

- Test the SIF:
  - record the actual trip point of the SIF;
  - verify the SIF alarm and actions on the final control devices;
  - verify the BPCS SIF related actions.
- Clear the SIF condition:
  - verify the SIF actions remain in the safe state.
- Reset the SIF:
  - verify the SIF actions reset to the designed state.

The example procedure assumes the instruments are shop tested and calibrated. The example procedure is written for all of the SIS functions to be tested at one time, rather than an individual procedure for each SIF. The procedure first checks the main SIS function and the final control devices. Each of the following listed testing actions tests a SIF without retesting the final control devices. Each testing action provides a test procedure in case a transmitter is replaced or a trip setting is changed.

An important key to the successful validation testing phase was the involvement of plant operations and maintenance personnel to assure a clear understanding of all aspects of the process, the BPCS, and the SIS. Personnel included:

- qualified control room operator;
- qualified electrical and instrument technicians.

In Table F.18 below, a list of instrument types and some of the testing procedures used is given.

Table F.18 – List of instrument types and testing procedures used

PRESSURE	
Normal connections	Provide drain/vents and test pressure connection downstream of primary block valve.
Remote diaphragm seals	Isolation valves and calibration rings should be provided for on-line testing. Consider elevation relative to tap(s) and specific gravity of fill fluid of capillary in validating the calibration.
TEMPERATURE	
Thermocouple	A continuity check on the device can be performed to determine operability only. Verify the milli-volt output at a known temperature against a standard curve.
Resistance temperature detectors (RTD)	Resistance can be measured to verify device operability. Verify the resistance at a known temperature against its standard calibration table.
Filled systems	Remove sensing device and place in temperature bath.
Bimetallic switch	Remove sensing device and place in temperature bath.

The following procedure is an example for validation of the SIS functions, including diagnostics alarms. This example does not include testing of the BPCS functions. Each SIS device (e.g., sensor, logic solver, final element) has testing (or replacement) recommended by the manufacturer which may not be addressed in this example procedure, but is assumed to be implemented separately. Refer to ISA-TR84.00.03:2012, *Mechanical Integrity of Safety Instrumented Systems (SIS).* For examples of test procedures, refer to the manufacturers' safety manual proof test section. A complete test procedure might also include testing of:

- the BPCS actions on activation of the safety function, such as controllers switching to manual mode;
- the BPCS shadow interlock functions;
- the BPCS alarms on the safety system diagnostics;

- the BPCS alarms allocated as safety layers in the LOPA.

An example of a reactor R1 interlock check procedure is given below:

NOMEX® is cited in the procedure below.[1]

[1] NOMEX® is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of this product.

Title:	Reactor R1	Prepared by:	DATE:
	Interlock check procedure	Revised by:	DATE:
Area:		Technical approval:	DATE:
PSM Critical:	Yes	Approved by:	DATE:

☐ FILE COPY ☐ FIELD COPY

Test summary

A. Sensors/switches tested:

Tag	Zero	Span	Units	Normal	Normal mA	Alarm	Alarm mA	Trip	Trip mA	Tolerance
100PT	0	200	PSIG	100	12	115	13.2	125	14	± 2 PSIG
100PT1	0	200	PSIG	100	12	115	13.2	125	14	± 2 PSIG
100TT	0	250	Deg F	125	12	180	15,52	200	16,8	± 2 Deg F
200PT	0	20	PSIG	2,5	6	5	8	10	12	± 1 PSIG

B. Final control devices tested:

Tag	Position
100PV	Open
100PV1	Open

C. Test results:
Check one:

_____ All devices passed the test.

_____ Corrective actions were required to pass the test.

Date check procedure completed: _____.

D. Safety & health

- Personal protective equipment as required per area procedure (e.g., safety glasses, hard hat, safety shoes)

E. Special protective equipment

- NOMEX® as required for flash protection.

F. Pre-test conditions and lockout

- Reactor should be de-inventoried down, and locked out, using lock, tag & try procedure.
- The emergency shutdown systems should be inactive.
- Barriers should be in place as required.

- Communication (e.g., signs, memos, scheduling, planning) should be complete.

G. Permits

- Line break permits for each transmitter.

H. Special equipment

- One current simulator.
- One transmitter hand held communicator.

I. Reference prints

- P&ID #:
- Logic Sheet #:
- E&I Drawing #:

J. Manpower

- Qualified control room operator
- Qualified electrical and instrument technicians

Each interlock test procedure has its own unique safety considerations. The following text should be modified to meet specific application requirements.

Calibration and inspection

A. Instrument calibrated or calibration verified:

Instruments calibrated per maintenance procedures.

Tag	Description	Trip	As found	Initials	Date
100PT	Reactor pressure north				
100PT1	Reactor pressure south				
100TT	Reactor temperature				
200PT	Reactor seal pressure				

B. Instruments and final control devices inspected:

Field installations inspected for issues with wiring, tubing, filters, gages, solenoids, insulation, and process connections.

Tag	Description	As found	As left	Initials	Date
100PT	Reactor pressure north				
100PT1	Reactor pressure south				
100TT	Reactor temperature				
200PT	Reactor seal pressure				
100PV	Reactor vent valve north				
100PV1	Reactor vent valve south				

Interlock test procedure

Time check procedure started: _____Date: _____

Procedure to be performed by:

Title	Signature	Date
Control room operator		
E&I technician		
E&I technician		
Operations team manager		

Interlock check procedure general set-up

E&I technician:

A. Simulate normal operating conditions.

_____ Clear all BPCS interlocks on 100PV and 100PV1.
_____ Update bypass check sheet for bypass #1.

Interlock check procedure for reactor SIS shutdown PB

Test frequency:	6 months
Test objective:	Manual reactor safety system shutdown opens reactor pressure control valves 100PV and 100PV1. Also test final control device diagnostics.

A. Clear the interlock. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.
_____ Verify the reactor safety system active light EA010 is lit.
_____ Verify the reactor safety system deactivated light EA011 is not lit.

B. Simulate normal conditions. (Control room operator)

_____ Verify the reactor vent valve closed diagnostic alarm EA18 is not lit.
_____ From the BPCS, close reactor vent valve 100PV.
_____ From the BPCS, close reactor vent valve 100PV1.
_____ Set all BPCS controllers to normal operating position.
_____ Set all BPCS controllers to normal operating mode.
_____ Set all BPCS valves and motors to normal mode.

C. Field verify normal conditions. (Field operator)

_____ Field verify the reactor vent valve 100PV is closed.
_____ Field verify the reactor vent valve 100PV1 is closed.

D. Test the diagnostic alarm. (E&I technician)

_____ Disconnect the signal from the reactor vent valve closed position switch 100LSC.
_____ Verify the reactor vent valve closed diagnostic alarm EA18 is lit.
_____ Reconnect the signal from the reactor vent valve closed position switch 100LSC.
_____ Verify the reactor vent valve closed diagnostic alarm EA18 is not lit.

_____ Disconnect the signal from the reactor vent valve closed position switch 100LSC1.

_____ Verify the reactor vent valve closed diagnostic alarm EA18 is lit.

_____ Reconnect the signal from the reactor vent valve closed position switch 100LSC1.

_____ Verify the reactor vent valve closed diagnostic alarm EA18 is not lit.

E. Test the interlock. (Control room operator)

_____ Shutdown the reactor safety system by pressing the shutdown stop pushbutton 500PB.

F. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system active light EA010 is not lit.

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor vent valve open diagnostic alarm EA17 is not lit.

_____ From the BPCS, verify reactor vent valve 100PV is open.

_____ From the BPCS, verify reactor vent valve 100PV1 is open.

_____ Verify all BPCS controllers are set to safe position.

_____ Verify all BPCS controllers are set to safe mode.

_____ Verify all BPCS valves and motors are in safe mode.

G. Field verify normal conditions. (Field operator)

_____ Field verify the reactor vent valve 100PV is open.

_____ Field verify the reactor vent valve 100PV1 is open.

H. Test the diagnostic alarm. (E&I technician)

_____ Disconnect the signal from the reactor vent valve open position switch 100LSO.

_____ Verify the reactor vent valve open diagnostic alarm EA17 is lit.

_____ Reconnect the signal from the reactor vent valve open position switch 100LSO.

_____ Verify the reactor vent valve open diagnostic alarm EA17 is not lit.

_____ Disconnect the signal from the reactor vent valve open position switch 100LSO1.

_____ Verify the reactor vent valve open diagnostic alarm EA17 is lit.

_____ Reconnect the signal from the reactor vent valve open position switch 100LSO1.

_____ Verify the reactor vent valve open diagnostic alarm EA17 is not lit.

I. Clear the interlock. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

_____ Verify the reactor safety system deactivated light EA011 is not lit.

_____ Verify the reactor vent valve open diagnostic alarm EA17 is not lit.

J. Field verify reset conditions. (Field operator)

_____ Field verify the reactor vent valve 100PV is open.

_____ Field verify the reactor vent valve 100PV1 is open.

K. Verify reset conditions. (Control room operator)

_____ From the BPCS, verify reactor vent valve 100PV is open.

_____ From the BPCS, verify reactor vent valve 100PV1 is open.

_____ Verify all BPCS controllers are set to safe position.

_____ Verify all BPCS controllers are set to safe mode.

_____ Verify all BPCS valves and motors are in safe mode.

Interlock check procedure for reactor pressure, 100PT

SIF	S1, S2
Name of event:	Overpressure of reactor
Event classification:	SIL 2
Test frequency:	6 months
Test objective:	High reactor pressure opens reactor pressure control valves 100PV and 100PV1.

A. Run the diagnostics (E&I technician)

_____ Connect to the reactor pressure transmitter 100PT using a handheld communicator and run the transmitter diagnostics.

_____ Verify there are no diagnostic errors.

B. Simulate normal conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

C. Test the interlock. (E&I technician)

_____ Disconnect the reactor pressure transmitter 100PT from the safety system.

D. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

E. Simulate normal conditions. (E&I technician)

_____ Connect a simulator to the reactor pressure transmitter 100PT.

_____ Simulate 100 PSI (12 mA) at the reactor pressure transmitter 100PT.

_____ Update bypass check sheet for bypass #2.

F. Simulate normal conditions. (Control room operator)

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is not lit.

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

G. Test the interlock. (E&I Technician)

_____ Slowly increase the simulated signal at the reactor pressure transmitter 100PT to 125 PSI (14 mA).

_____ Record the setting at which the interlock tripped: _____

H. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

I. Clear the interlock. (E&I technician)

_____ Slowly decrease the simulated signal at the reactor pressure transmitter 100PT to 100 PSI (12 mA).

J. Verify the reset conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is not lit.

K. Return to current conditions. (E&I technician)

_____ Remove the simulator from the reactor pressure transmitter 100PT.

_____ Reconnect the reactor pressure transmitter 100PT to the safety system.

_____ Update bypass check sheet for bypass #2.

L. Verify current conditions. (Control room operator)

_____ Verify the reactor pressure transmitter 100PT is reading actual reactor pressure.

Interlock check procedure for reactor pressure, 100PT1

SIF	S2
Name of event:	Overpressure of reactor
Event classification:	SIL 2
Test frequency:	6 months
Test objective:	High reactor pressure opens reactor pressure control valves 100PV and 100PV1.

A. Run the diagnostics (E&I technician)

_____ Connect to the reactor pressure transmitter 100PT1 using a hand-held communicator and run the transmitter diagnostics.

_____ Verify there are no diagnostic errors.

B. Simulate normal conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

C. Test the interlock. (E&I technician)

_____ Disconnect the reactor pressure transmitter 100PT1 from the safety system.

D. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

E. Simulate normal conditions. (E&I technician)

_____ Connect a simulator to the reactor pressure transmitter 100PT1.

_____ Simulate 100 PSI (12 mA) at the reactor pressure transmitter 100PT1.

_____ Update bypass check sheet for bypass #3.

F. Simulate normal conditions. (Control room operator)

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is not lit.

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

G. Test the interlock. (E&I technician)

_____ Slowly increase the simulated signal at the reactor pressure transmitter 100PT1 to 125 PSI (14 mA).

_____ Record the setting at which the interlock tripped: _____

H. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

F. Clear the interlock. (E&I technician)

_____ Slowly decrease the simulated signal at the reactor pressure transmitter 100PT1 to 100 PSI (12 mA).

J. Verify the reset conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is not lit.

K. Return to current conditions. (E&I technician)

_____ Remove the simulator from the reactor pressure transmitter 100PT1.

_____ Reconnect the reactor pressure transmitter 100PT1 to the safety system.

_____ Update bypass check sheet for bypass #3.

L. Verify current conditions. (Control room operator)

_____ Verify the reactor pressure transmitter 100PT1 is reading actual reactor pressure.

Interlock check procedure for reactor temperature, 100TT

SIF	S1
Name of event:	Overpressure of reactor
Event classification:	SIL 2
Test frequency:	12 months
Test objective:	High reactor temperature opens reactor pressure control valves 100PV and 100PV1.

A. Run the diagnostics (E&I technician)

_____ Connect to the reactor pressure transmitter 100TT using a handheld communicator and run the transmitter diagnostics.

_____ Verify there are no diagnostic errors.

B. Simulate normal conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

C. Test the interlock. (E&I technician)

_____ Disconnect the reactor temperature transmitter 100TT from the safety system.

D. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

E. Simulate normal conditions. (E&I technician)

_____ Connect a simulator to the reactor temperature transmitter 100TT.

_____ Simulate 125 Deg F (12 mA) at the reactor temperature transmitter 100TT.

_____ Update bypass check sheet for bypass #4.

F. Simulate normal conditions. (Control room operator)

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is not lit.

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

G. Test the interlock. (E&I technician)

_____ Slowly increase the simulated signal at the reactor temperature transmitter 100TT to 200 Deg F (16,8 mA).

_____ Record the setting at which the interlock tripped: _____

H. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

F. Clear the interlock. (E&I technician)

_____ Slowly decrease the simulated signal at the reactor temperature transmitter 100TT to 125 Deg F (12 mA).

J. Verify the reset conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is not lit.

K. Return to current conditions. (E&I technician)

_____ Remove the simulator from the reactor temperature transmitter 100TT.

_____ Reconnect the reactor temperature transmitter 100TT to the safety system.

_____ Update bypass check sheet for bypass #4.

L. Verify current conditions. (Control room operator)

_____ Verify the reactor temperature transmitter 100TT is reading actual reactor temperature.

Interlock check procedure for reactor seal pressure, 200PT

SIF	S3
Name of event:	Overpressure of reactor seal
Event classification:	SIL 2
Test frequency:	6 months
Test objective:	High reactor seal pressure opens reactor pressure control valves 100PV and 100PV1.

A. Run the diagnostics (E&I technician)

_____ Connect to the reactor pressure transmitter 200PT using a handheld communicator and run the transmitter diagnostics.

_____ Verify there are no diagnostic errors.

B. Simulate normal conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

C. Test the interlock. (E&I technician)

_____ Disconnect the reactor pressure transmitter 200PT from the safety system.

D. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

E. Simulate normal conditions. (E&I technician)

_____ Connect a simulator to the reactor seal pressure transmitter 200PT.

_____ Simulate 2,5 PSI (6 mA) at the reactor seal pressure transmitter 200PT.

_____ Update bypass check sheet for bypass #5.

F. Simulate normal conditions. (Control room operator)

_____ Verify the reactor safety system transmitter diagnostic alarm EA014 is not lit.

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

G. Test the interlock. (E&I technician)

_____ Slowly increase the simulated signal at the reactor seal pressure transmitter 200PT to 10 PSI (12 mA).

_____ Record the setting at which the interlock tripped: _____

H. Verify the interlock actions. (Control room operator)

_____ Verify the reactor safety system deactivated light EA011 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is lit.

_____ Verify the reactor safety system will not reset when reset button PB000 is pressed.

F. Clear the interlock. (E&I technician)

_____ Slowly decrease the simulated signal at the reactor seal pressure transmitter 200PT to 2,5 PSI (6 mA).

J. Verify the reset conditions. (Control room operator)

_____ Reset the reactor safety system by pressing the reset button PB000.

_____ Verify the reactor safety system active light EA010 is lit.

_____ Verify the reactor safety system transmitter trip alarm EA012 is not lit.

K. Return to current conditions. (E&I technician)

_____ Remove the simulator from the reactor pressure seal transmitter 200PT.

_____ Reconnect the reactor pressure transmitter 200PT to the safety system.

_____ Update bypass check sheet for bypass #5.

L. Verify current conditions. (Control room operator)

_____ Verify the reactor seal pressure transmitter 200PT is reading actual reactor seal pressure.

Interlock Check Procedure General Completion

E&I technician:

A. Return all other interlocks to operation.

_____ Return all BPCS interlocks on 100PV and 100PV1 to service.
_____ Update bypass check sheet for bypass #1

Test and inspection completed by:

Title	Signature	Date
Control room operator		
Control room operator		
E&I technician		
E&I technician		
Operations team manager		

Time check procedure completed: _____Date: _____

Post test inspection and documentation

A. Verify that any changes to the procedure have been reviewed with management and approved.
B. If any device failed, what corrective action was required:

_____
_____
_____
_____
_____
_____

Complete signatures on the file copy and file with safety system test records. Table F.19 provides an illustration of how a check sheet addressing interlock check procedure bypass/simulation can be documented.

Table F.19 – Interlock check procedure bypass/simulation check sheet

Bypass #	Loop	Location	Method	Step installed	Initials	Step removed	Initials
1	DCS	DCS	Flag	1.1		7.1	
2	100PT	Transmitter	Simulator	3.4		3.10	
3	100PT 1	Transmitter	Simulator	4.4		4.10	
4	100TT	Transmitter	Simulator	5.4		5.10	
5	200PT	Transmitter	Simulator	6.4		6.10	
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
18							
20							

F.29 Step F.6: SIS operation and maintenance

Table F.20 – SIS safety life-cycle – Box 6

Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs
IEC 61511-1:— Figure F.7, box 6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	SIS requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities

Training of operations, maintenance, and other support personnel on the function of both the BPCS and SIS was performed prior to placing the systems in operation and is updated at any time any changes are made to either system.

New items to consider regarding SIS operation and maintenance training include:

- terminology (e.g., SIS, SIF, PFD_{avg}, SIL, layers of protection);
- hazards and risk analysis;

- architecture (e.g., HMIs (SIS and BPCS), SIS interfaces (e.g., read only link from BPCS));
- documentation requirements (e.g., frequency of demands placed on SIF/SIS, procedures/methods/techniques, proof tests and inspections, test results, equipment identifiers down to the revision level, responsible persons/departments/organizations);
- bypass procedures;
- testing frequency for SIF/SIS;
- SIS functional description.

A SIS trip log was developed for operations and maintenance to record the demands and failures of the SIS. See Table F.21 below.

Spurious trips of SIF are included in this log, but are not counted as demands on the SIS.

Table F.21 – SIS trip log

Date	SIF	Demand/Spurious	Cause of trip	Incident report #	Recorded by
5/18/08	S-2	Demand	Operator error – overcharged reactor	Serious Incident Report # 18	L. Soft
8/03/08	S-3	Spurious	Transmitter 200PT failure	None	J. Doe
2/28/09	S-1	Demand	Failure of coolant control loop	Serious Incident Report #43	T. Rex

A tracking system was put in place to identify recurrent problems with SIS devices as they are detected during testing. The results are logged as shown in Table F.22 below.

Table F.22 – SIS device failure log

Date	Device	Safe/unsafe failure	Failure description	Recorded by
3/21/07	100TT	Safe	Out of calibration	T. Rex
5/18/08	100PV	Unsafe	Valve stem stuck – won’t open	L. Soft
8/03/08	100PV	Unsafe	Valve stem stuck – won’t open	J. Doe
2/28/09	100PV	Unsafe	Valve stem stuck – won’t open	T. Rex

As indicated in Table F.20, vent valve 100PV experienced frequent problems. After the third failure, a root cause failure analysis determined that the valve was defective. The valve was replaced, and has not exhibited any failures since.

Documentation of the current control and safety logic implemented in both the BPCS and the SIS is maintained at all times. Any changes are documented at the time they are implemented. Hard copies of the documentation, fully describing the systems and their functions, are maintained for reference.

An audit program was implemented that requires an examination of system documentation as part of the cyclic process hazard review. A report is issued describing the results of the audit and any recommendations from the audit are flagged for follow-up (at quarterly intervals) until they are completed. The audit includes:

- review of all changes made since the last review and verification of correct documentation status;

- review of all problems with equipment or logic associated with the SIS since the last review to ascertain if potential problems are developing that might degrade the system's function in the future;
- review of operating personnel's understanding of the system's function and operation;
- review of SIS demand Log to validate the demand rate assumptions used in the LOPA;
- review of SIF test results to validate the device failure rate assumptions used in the PFD_{avg} calculations.

Following is a list of the supporting documentation that will be included in the audit. This documentation will be available to operating personnel and kept current.

– H&RA documentation (What Ifs (Table I.4), HAZOP (Table F.5));

– tolerable risk ranking used (i.e., Table F.8);

– documentation of risk allocation to protection layers – determination of SIL for each SIF (LOPA) (i.e., Table F.9);

– P&I diagrams (i.e., Figures F.3 and F.10);

– SIF system diagram (i.e., Figure F.12);

– AP printout (ladder diagrams) (i.e., Figure F.11 (sheets 1,2,3,4, and 5));

– safety manuals;

– SIS hardware/AP/installation/maintenance documentation (e.g., Table F.20-box 6;

– systematic capability documentation;

– SIL verification calculations (i.e., PFD_{avg}) for each SIF including bubble diagrams (i.e., Figures F.4, F.5, F.6, F.7, F.8, and F.9);

– test procedure for each SIF;

– process demands on each SIF (i.e. Table F.12);

– failure data for SIF devices (i.e. Table F.13).

Periodic testing and inspection of the SIS is carried out at the frequency specified in the PFD_{avg} calculations (i.e., every six months). Layers of protection identified in the LOPA are also tested at the same six-month frequency.

Operations maintain records that demonstrate that proof tests and inspections were completed as required. These records should include the following information as a minimum:

a) description of the tests and inspections performed;

b) dates of the tests and inspections;

c) name of the person(s) who performed the tests and inspections;

d) serial number or other unique identifier of the system tested (e.g., loop number, tag number, equipment number, and SIF number);

e) results of the tests and inspection (e.g., "as-found" and "as-left" conditions);

f) current AP running in the SIS logic solver.

F.30 Step F.7: SIS Modification

Table F.23 – SIS safety life-cycle – Box 7

Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs
Figure F.2, box 7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modification

Table F.23 provides the objectives, inputs, outputs, and reference to the related clauses and subclauses for SIS modification.

The plant has a functional management of change process in place consistent with OSHA 29 CFR 1910.119. Any modification of the SIS will require re-entering the SIS safety life-cycle at the appropriate step.

F.31 Step F.8: SIS decommissioning

Decommissioning key devices are outlined in Table F.24.

Table F.24 – SIS safety life-cycle – Box 8

Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs
IEC 61511-1:— Figure F.2, box 8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remain appropriate	18	As-built safety requirements and process information	SIF placed out of service

The plant has experience with decommissioning hazardous processes and understands the need to do a H&RA and an engineering analysis followed by decommissioning planning. Once this is complete, proper authorization(s) and scheduling follow prior to the beginning of decommissioning.

F.32 Step F.9: SIS verification

Verification (Table F.25) is an activity that is carried on throughout the life-cycle of the SIS.

Table F.25 – SIS safety life-cycle – Box 9

Safety life-cycle phase or activity		Objectives	Requirement clause or subclause of IEC 61511-1:2016	Inputs	Outputs
IEC 61511-1:— Figure F.2, box 9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.5	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase

The engineering, operations, and maintenance personnel jointly coordinate verification planning so that each organization can achieve its goals.

Engineering used verification to ensure:

- Its hardware, AP, and system design are correct and consistent with the SRS.
- Operations is involved in selected verification activities (e.g., AP development, HMI displays) at the outset so final approval does not result in surprises (e.g., major rework, delays).
- Maintenance has hands-on opportunities to work with SIS devices/subsystems/systems to gain familiarity with documentation, hardware location, AP functionality, while simultaneously facilitating verification.

Operations used verification activities:

- to establish the project is as planned and on schedule;
- as input in writing operating instructions.

Maintenance used verification to:

- familiarize their personnel with the process;
- identify areas where new training/tools are required;
- identify installation procedures not consistent with plant practices;
- develop maintenance procedures.

F.33 Step F.10: Management of functional safety and SIS FSA

Table F.26 – SIS safety life-cycle – Box 10

Safety life-cycle phase or activity		Objectives	Requirement clause or subclause of IEC 61511-1:2016	Inputs	Outputs
Figure F.2, box 10	Management of functional safety and SIS FSA	To ensure all steps of the SIS safety life-cycle are properly addressed, and to investigate and arrive at a judgement on the functional safety achieved by the SIS	5	Planning for SIS FSA SIS safety requirement	Results of SIS FSA

F.34 Management of functional safety

F.34.1 General

Management of functional safety (Table F.26) in this company is implemented under the Process Safety Management (PSM) program. Extensive corporate standards address all aspects of PSM, such as mechanical integrity, quality assurance, and training. These standards require that all new projects implemented at company manufacturing facilities comply with the requirements of IEC 61511 where applicable.

F.34.2 Competence of personnel

Management is required to ensure that persons responsible for carrying out and reviewing each of the SIS safety life-cycle activities are competent to carry out the activities for which they are accountable. This was accomplished by implementing the approach outlined in IEC 61511-1:2016, 12.5.2. The qualification items reviewed were:

- experience and training;
- engineering knowledge of the process;
- engineering knowledge of the SIS technology;
- safety engineering knowledge (e.g., corporate functional safety standards);
- management and leadership skills;
- understanding of the potential consequence of an event.

In addition, operations and maintenance personnel were trained on the hazards associated with the process as well as the operation of the BPCS and SIS prior to start-up.

F.35 Functional safety assessment

An FSA (also called a pre-start-up safety review) was performed prior to start-up of the process; see IEC 61511-1:20165.2.6.1. The overall objective of the FSA was to ensure that the SIS would operate in accordance with the requirements defined in the SRS so that the SIS can safely move from the installation phase to the production phase.

FSA was not begun until all verification activities were completed and approved.

Ongoing FSA will be performed on a periodic basis as described in Clause F.29, Step 6.

Annex G
(informative)

Guidance on developing application programming practices

G.1 Purpose of this guidance

In the process sector selection of PE devices (see IEC 61511-1:2016, 11.5 and 11.6) will either be based on an IEC 61508 compliant device (e.g. ‘’safety PLC’’) which will be supported by a safety manual, or else will be selected through prior use.

This Annex G provides examples of the considerations, called “generic safe application programming attributes” that should be addressed as appropriate, either in the safety manual as provided by the manufacturer, or as a project specific programming manual, in order to maintain the AP design within the scope of this standard and to contribute to the achievement of the AP expected safety systematic integrity.

NOTE This annex was previously identified as Annex A.

G.2 Generic safe application programming attributes

This annex describes generic, or language-independent, attributes of safe application programming. The attributes have been defined in a hierarchical, three- level framework. The four top-level attributes being:

Reliability: Reliability is the predictable and consistent performance of the AP under conditions specified in the design basis. This top level attribute is important to safety because it decreases the likelihood that faults causing unsuccessful operation will be introduced into the AP during implementation.

Robustness: Robustness is the capability of the AP to operate in an acceptable manner under abnormal process conditions or events. This top level attribute is important to safety because it enhances the capability of the AP to handle exception conditions, recover from internal failures, and prevent propagation of errors arising from unusual circumstances (not all of which may have been fully defined in the design basis).

Traceability: Traceability relates to the feasibility of reviewing and identifying the AP and library device origin and development processes i.e., that the delivered AP can be shown to be the product of a disciplined implementation process. Traceability also includes being able to associate AP with higher level design documents. This top level attribute is important to safety because it facilitates verification and validation, and other aspects of AP quality assurance.

Maintainability: The means by which the AP reduces the likelihood that faults will be introduced during changes made after commissioning. This top level attribute is important to safety because it decreases the likelihood of unsuccessful operation resulting from faults during adaptive, corrective, or perfective AP maintenance.

G.3 Reliability

G.3.1 General

In the AP context, reliability is either (1) the likelihood of successful execution over a defined interval of time and under defined conditions, or (2) the likelihood of successful operation upon demand. That the AP executes to completion is a result of its proper behavior with

respect to system memory and AP logic. That the AP produces timely output is a function of the automation engineer's understanding of the language constructs and run-time environment characteristics. Thus, the intermediate attributes for reliability set forth are:

- Predictability of memory utilisation: There is a high likelihood that the AP will not cause the logic solver to access unintended or un-allowed memory locations;
- Predictability of control flow: There is a high likelihood that the logic solver will execute instructions in sequences intended by the programmer;
- Predictability of timing: There is a high likelihood that the AP executing within the defined run-time environment will meet its response time and capacity constraints; predictability of mathematical or logical result: There is a high likelihood that the AP executing within the defined run-time environment will yield the automation engineer-intended mathematical or logical result.

G.3.2 Predictability of memory utilisation

G.3.2.1 Minimising dynamic memory allocation

Dynamic memory allocation is used in APs to temporarily claim (allocate) memory when necessary during run time and to free the memory (also during run time) for other uses when no longer needed. The safety concern is that when memory is dynamically allocated in a real-time system, the AP may not subsequently release all or some of it. This can happen either because:

- the AP allocates memory to itself but does not free it as part of normal execution paths, or
- an AP which has temporarily allocated memory to itself is interrupted in its execution prior to executing the statement which releases the memory.

Either of these situations will cause the eventual loss of all usable memory and a loss of all safety system functions. Dynamic memory allocation in digital safety systems should therefore be minimised.

If dynamic memory allocation is unavoidable IEC 61508-3 applies and the AP should include provisions to ensure that:

- all dynamically allocated memory during a specific execution cycle is released at the end of that cycle; and
- the possibility of interruption of execution between the point where memory is dynamically allocated and when it is released is minimized (if not totally eliminated); there should also be provisions in the AP that will detect any situation where dynamically allocated memory has not been released and release such memory.

This standard thus discourages the use of indirect addressing. IEC 61508-3 applies to APs using indirect addressing.

G.3.2.2 Minimising memory paging and swapping

Memory paging is the use of a part of memory to store infrequently used primary memory areas. When these memory areas are needed by a running AP, the logic solver causes them to be read from one part of the memory and loaded back into another part of the memory. Process swapping is the use of part of the memory to store the memory image of an entire inactive process (including its data areas such as a stack space and heap space).

When it is time for the process to be executed, the image is loaded from one part of the memory back into the primary memory for use by the logic solver. In any event, the specific usage of memory and the portion of storage used for swapping is indeterminate.

These capabilities are inappropriate for safety systems because these indeterminacies in memory and storage utilisation can, in turn, cause significant delays in response time and use complex interrupt-driven functions to handle the memory transfers.

If a logic solver that supports memory paging or process swapping is used in a SIS, this feature should be disabled at the logic solver level. There should be enough primary memory for all data and APs. If there is any question that these features were not disabled, IEC 61508-3 applies and there should be provisions in the AP ensuring that all critical functions and their data areas are in primary memory during the entire period of execution. Such provisions in the AP include logic solver calls ("pinning"), application programming tool directives, and logic solver scripts.

G.3.3 Predictability of control flow

G.3.3.1 General

Control flow defines the order in which statements in an AP are executed. A predictable control flow allows an unambiguous assessment of how the program will execute under specified conditions.

Related base attributes are:

- maximizing structure;
- minimizing control flow complexity;
- initializing variables before use;
- single entry and exit points for subprograms;
- minimizing interface ambiguities;
- use of data typing;
- accounting for precision and accuracy;
- order of precedence of arithmetic, logical, and functional operators;
- avoiding functions or procedures with side effects;
- separating assignment from evaluation;
- proper handling of program instrumentation;
- controlling class library size;
- minimizing use of dynamic binding;
- controlling operator overloading.

G.3.3.2 Maximising structure

AP with GOTO or equivalent execution control statements that cause an unstructured shift of execution from one branch of an AP to another should be avoided. The safety concern is that the execution time behavior is difficult to trace and understand. GOTO statements can cause undesirable side effects because they interrupt execution of a particular AP segment without assurance that subsequent execution will satisfy all conditions that caused entry into that segment. Standards discouraging or prohibiting such application programming practices have been in place for more than two decades. Structure is maximised by the elimination of GOTO statements and use of appropriate block structured AP. The case, if..then..else, do until, and do while constructs permit branching with a defined return and without introducing the uncertainty of control flow associated with GOTO or equivalent statements.

G.3.3.3 Minimising control flow complexity

An indication of control flow complexity is the number of nesting levels for branching or looping. Excessive complexity makes it difficult to predict the flow of an AP and impedes

review and maintenance. A specific safety concern is that the control flow may be unpredictable when unanticipated combinations of parameters are encountered. Excessive nesting can usually be avoided by the use of functions or subroutines in place of in-line branches. A specific limit on nesting as part of project or organisational programming guidelines should be defined in order to mitigate safety concerns

IEC 61511 thus limits the layers in the AP architecture to 2 layers:

- typicals;
- interlocks.

IEC 61508-3 applies to APs with a number of nesting levels over this defined limit.

G.3.3.4 Initialising variables before use

When variables are not initialised to a known value at the beginning of an execution cycle, safety is impaired because they may contain "garbage" values (residue from the previous use of that memory area). Run-time predictability requires that memory storage areas set aside for process data be set to known values before being accessed (set and used). The specific result of using unknown initial values of a variable depends upon how that variable is used in the AP. IEC 61508-3 applies to APs using non initialised variables.

G.3.3.5 Single entry and exit points for subprograms

Multiple entry and exit points in subprograms introduce control flow uncertainties similar to those caused by GOTO statements.

Run-time execution flow predictability is enhanced by having only a single entry to and exit from each AP. Because predictability of execution flow is a characteristic important to safety, multiple entry and exit points in subroutines or functions are undesirable even if the language supports them. IEC 61508-3 applies to APs with multiple entry and exit points.

G.3.3.6 Minimising interface ambiguities

Interface faults include mismatches in argument lists when calling other subprograms, communicating with other tasks or passing messages among objects. An example of such a fault is reversing the order of arguments when calling a subroutine. Previous research on AP failures has shown that this category of faults is quite significant. Application programming practices that can reduce or eliminate the likelihood of interface faults include:

- Ordering arguments to alternate different data types (reducing the chance that two adjacent arguments will be placed in an incorrect order).
- Using named notation rather than ordering or position notation for languages that support such notation.
- Testing for the validity of input arguments at the beginning of the subprogram.

Routines should have adequate pre- and post-conditions specified. A pre-condition is an assurance that all local variables are initialised and all input variables meet appropriate reasonableness checks. A post-condition is an assurance that all output variables meet appropriate reasonableness checks.

G.3.3.7 Use of data typing (data structures)

Use of data structures that differ from those intended to be used by an AP can cause failures, and such failures that occur during an exception condition may have particularly adverse effects on safety. This concern can be addressed by declaration of data types. Originally, the primary advantage of declaring data types was to allow compilers to reserve the correct amount of memory. However, data typing is useful for improved definition of interfaces, increased legibility (for reviews), and compile time and run time checking. These originally ancillary uses have now become the primary motivators for data typing and have prompted

the use of strong typing in which additional declarations, at least that of a valid range, are required. The safety issues associated with data typing include:

- Limiting the use of anonymous types (e.g., general integer or floating point without upper and lower limits) in strongly typed languages.
- Ensuring that the limits on data types are not excessively constrained so that spurious exceptions or error messages are not generated (this is an issue in strongly typed languages).
- Minimizing type conversions, and eliminating implicit or automated type conversions (e.g., in assignments and pointer operations).
- Avoiding mixed-mode operations. If such operations are necessary, they should be clearly identified and described using prominent comments in the AP.
- Ensuring that expressions involving arithmetic evaluations or relational operations have a single data type, or the proper set of data types for which conversion difficulties are minimized.

Limiting the use of indirect referencing for example array indices, pointers, or access objects to situations where there are no other reasonable alternatives and performing validation on indirectly addressed data prior to setting or use to ensure the correctness of the accessed locations. Strongly typed pointers, array indices, and access types reduce the possibility of referencing invalid locations.

G.3.4 Accounting for precision and accuracy

G.3.4.1 General

The AP implementation should provide adequate precision and adequate accuracy for the intended safety application. This applies to both the measurement of physical properties and to any floating point arithmetic within the AP. Safety concerns are raised when the declared precision of floating point variables is not supported by analysis, particularly when small differences between large values are used (e.g., when computing rate of change from the difference between current and previous values, calculating variances, or performing filtering operations such as moving averages).

G.3.4.2 Order of precedence of arithmetic, logical, and functional operators

The default order of precedence of arithmetic, logical, and other operations varies among languages. Developers or reviewers may make incorrect precedence assumptions. Therefore the use of mechanisms for ensuring a clear statement of the order of evaluation of operations should be used.

G.3.4.3 Avoiding functions or procedures with side effects

A side effect is a change to any variable not returned by that function that persists after the completion of the function. This includes changes to files, hardware registers, etc. An example of such a side effect would be a change in a global variable not in the function parameter list. Side effects can lead to problems with unplanned dependencies and can cause bugs that are hard to find.

G.3.4.4 Separating assignment from evaluation

Assignment statements should be separated from evaluation expressions. The separation can be violated when subprograms are used as part of the evaluation. For example, a filtering function may be used as part of an evaluation rather than simply the sensor value. A related attribute is minimization of the use of global variables discussed below.

G.3.4.5 Proper handling of application program auxiliary functions

AP instrumentation collects and outputs certain internal state values of an AP during execution and allows the developer to check if particular aspects of the specification have been correctly implemented. Specific safety related issues are:

Minimising run-time perturbations: Auxiliary functions that interfere with the normal execution flow are undesirable in safety applications. For example, extensive "write" or other output statements can result in the execution of a significant amount of library AP associated with outputting values; a less intrusive means may be to write such values to external memory locations where they can be processed later. It may also mean writing data in binary format for off-line format processing (i.e., conversion to human-readable text and numeric values). To minimise differences in behavior between test and normal operation, it may be desirable to keep certain auxiliary functions AP in place in the actual environment.

Maintaining visibility of auxiliary functions in runtime AP: Some AP tools alter logic solver generated object (or executable) files in order to insert auxiliary functions. This is generally not acceptable in a safety system because the impact of such changes is not visible in the AP and its effect on execution cannot be reviewed.

Conforming to AP auxiliary functions guidelines: Review is facilitated (and therefore safety is enhanced) if the auxiliary functions practices are described in project specific engineering notebooks. Guidelines should identify what types of output mechanisms are to be used, and under which conditions they should not be used. For example, a measure mentioned above for minimising runtime interference is at odds with the data abstraction and error containment attributes described later in Annex G.

G.3.4.6 Controlling class library size

Control of class library size is important to avoid a system that becomes unmanageable or has large performance penalties because it has too many classes and objects. Safety is enhanced if project-specific guidelines limit the number of classes and objects and the actual AP conforms to these guidelines.

G.3.4.7 Minimising use of dynamic binding

Binding denotes the association of a name with a class. Dynamic binding permits the name/class association to be deferred until the object designated by the name is created at execution time. The unpredictability of the name/class association creates safety concerns. It also reduces the predictability of the runtime behavior of an object-oriented program and it complicates debugging, understanding, and tracing. Restrictions on, or elimination of, dynamic binding is desirable for safety-critical applications. IEC 61508-3 applies to APs using dynamic binding.

G.3.4.8 Controlling operator overloading

Polymorphism (operator overloading) can improve readability and reduce complexity by allowing a single subprogram or operator or object behavior to be used for different data types. However, it can also be problematic from the perspective of predictability because it is unclear how a logic solver will bind AP for different polymorphisms (e.g., how would a multiply operation on a multidimensional array be bound to scalars or one-dimensional arrays).

Guidance on use of operator overloading in a project-specific or organisational application programming standards manual is therefore desirable for safety-related applications, together with verification that the AP complies with this standard.

G.3.5 Predictability of timing

G.3.5.1 General

Predictability of timing is crucial in a safety system used in real time control. Base attributes related to object oriented programming that have relevance to this intermediate attribute are described under previous headings:

- controlling class library size;
- minimizing use of dynamic binding;
- controlling operator overloading.

Two additional base attributes related to timing discussed in the following subclauses are:

– minimizing the use of tasking;
– minimizing the use of interrupt driven processing.

G.3.5.2 Minimising the use of tasking

Although tasking provides an attractive model for concurrent processing, its use is undesirable in safety-critical applications for the following reasons:

- The sequence of execution is uncertain when several calling alternatives are waiting to be executed because it is not always clear which call will be selected.
- Tasking allows time critical errors such as race conditions and deadlocks to develop. Such differences are difficult to debug.

Therefore, tasking is to be avoided in safety systems unless there is a compelling justification.

G.3.5.3 Minimising the use of interrupt driven processing

Using interrupt driven processing to handle the acceptance and processing of plant and operator input can reduce average response time, but usually leads to non-deterministic maximum response times. Interrupt driven processing was implicated in at least some accidents.

Reference documents and standards related to digital system safety generally discourage or prohibit its use (IEC 60880:2006). Avoiding interrupt driven processing facilitates analysis of synchronisation and run-time behavior, and avoids the non-determinism of response time inherent in interrupt driven processing.

G.4 Predictability of mathematical or logical result

Predictable mathematical or logical result means that the results realised at the completion of execution of the low level of AP being examined are the results intended and expected by the programmer who wrote the AP. The term "logical" is intended to extend the term "results" to the case where the AP is manipulating Boolean data and will yield a Boolean result. Therefore a safety AP should be strictly static. IEC 61508-3:2010 applies to APs using flip-flop memories whether explicit or implicit.

Heavy use of interlocks alters the predictability of the results and increases the complexity of the demonstration of independence between AP structures. SIF should not be interlocked between themselves.

Use of timers should be limited and not cascaded or interlocked.

G.5 Robustness

G.5.1 General

Robustness refers to the capability of the AP to continue execution during off-normal or other unanticipated conditions. A synonym for robustness is survivability. Robustness is an important attribute for a safety system because unanticipated events can happen during an accident or excursion, and the capability of the AP to continue monitoring and controlling a system in such circumstances is vital.

The intermediate attributes for robustness are:

- controlling use of diversity;
- controlling use of exception handling;
- checking input and output.

G.5.2 Controlling use of diversity

G.5.2.1 General

The decision to employ diverse AP implementations is a design-level function and is therefore outside the scope of this guidance. However, if diversity is called for in the design or requirements, it should be controlled in its application. The principal issue with the use of diversity in AP is the possibility that common-mode AP failures may cause redundant safety systems to fail in such a way that there is a loss of safety function.

The possibility of common-mode failures between independently developed AP routines is not easily eliminated. Any shared specification can lead to common-mode failures. The same problem exists in developing test data to check the AP – the testers may omit the same off-nominal or unusual cases that the developers overlooked. Further, in order to use the approach where the outputs of multiple versions of AP can be compared in real time (or to be able to compare intermediate results), the designs from independent teams may be over specified. Such detailed common specifications may result in little AP design diversity. This is often found in corporate programming standards.

In addition, multiple versions of the AP written independently from the same requirements specification are effective only against application programming errors (and sometimes only a limited set of these). On the other hand, empirical evidence suggests that most safety problems (and most errors found in operational AP) stem from errors in the AP requirements, especially misunderstandings about the required operation of the AP. AP intended to provide redundancy may not achieve this goal but may simply duplicate the misunderstandings. In reviewing safety-critical AP, analysis of AP diversity to determine common-mode failures is important.

There are two base attributes:

- controlling internal diversity;
- controlling external diversity.

G.5.2.2 Controlling internal diversity

When only internal diversity is used, the interfaces to all versions should be identical. In other words, any sensor data or parameters from calling procedures should be passed identically to all versions, and output data from any version should be accepted and used by other parts of the system. However, internal operations and storage of local data should occur diversely in the multiple module versions or instantiations. Internal diversity is facilitated by an object-oriented approach in which the same messages and methods are used, but the internal algorithms and data representations differ. Internal diversity should be implemented in accordance with the design and with project-specific guidelines. These should address:

- Diverse algorithms: Using different algorithms, unit conversions, and process parameters (when calls for or allowed in the requirements or design) minimises the possibility of a design or implementation-related failure.
- Diverse data validation: Using alternate schemes for sensor (or other input) data and output data validation minimizes the possibility of a designer implementation-related failure.
- Diverse exception handling routines: This measure reduces the likelihood that an error in the exception handling or processing will occur simultaneously on multiple versions.
- Different data types, structures, and storage allocation: This measure reduces the possibility that unanticipated interactions between the object AP generated by the application programming tool and the logic solver will cause data or AP to be inadvertently overwritten simultaneously on multiple versions.
- Diverse libraries and subroutines: Avoiding use of the same AP subroutines, compiler-supplied library routines, and logic solver provided application programming interfaces. This measure reduces the possibility of a simultaneous failure due to a defect in such routines.
- Diverse order of arithmetic operation: Changing the order of arithmetic operations in conversions, arithmetic, and assignment statements by using commutative, associative, and distributive properties reduces the possibility of simultaneous failures due to unanticipated overflow conditions generated by intermediate results or problems in numerical precision.
- Diverse order of input and output operation: Performing I/O operations in different orders reduces the possibility of simultaneous timing-related failures (such as a deadlock) or data-driven failures (i.e., an AP crash due to a particular data value).

The limitation to diversity is the fact that on a given platform all these languages are actually only a diverse representation of the same algorithms. The use of diversity of languages thus mitigates only the weaknesses of each language before compilation. The AP can thus be written in two different languages to compare their behavior.

G.5.2.3 Controlling external diversity

Where external diversity is used, safety is enhanced if it is implemented in a disciplined manner in accordance with design documents. The design documents should reflect the diversity imposed by requirements, hazard analyses, and similar sources. External diversity is achieved by using different interfaces among the versions, and may be combined with internal diversity. External diversity is necessary when different languages are used for different versions, and may also be used to obtain sensor data through a different channel. Uncontrolled or unspecified external diversity can lead to a proliferation of interfaces which impact safety due to difficult maintenance, testing, verification, and validation.

G.5.3 Controlling use of exception handling

G.5.3.1 General

Exception handling deals with abnormal system states and input data. Exception handling provisions in some languages facilitate the establishment of an alternate execution path in the event of conditions which, although unexpected, result in states that can be defined in advance. Problems can arise in the use of exception raising and handling, however, because execution flow during exception conditions is often difficult to trace.

Base attributes with respect to exception handling include:

- handling of exceptions locally;
- preserving external control flow;
- handling of exceptions uniformly.

G.5.3.2 Handling of exceptions locally

Propagation of exceptions through several levels of an AP can cause the precise nature of the exception to be misinterpreted at the place where the exception handling is implemented. This cause of system failure (with potentially serious safety implications) is avoided if exceptions are handled locally.

G.5.3.3 Preserving external control flow

Interruption of control flow external to the routine in which the exception was raised creates uncertainty in the execution subsequent to the exception handling. Safety is enhanced by preservation of control flow external to the module responsible for the exception.

G.5.3.4 Handling of exceptions uniformly

Undisciplined use of exception handling can result in inconsistent processing of the same exception condition in different parts of the AP. At worst, it can result in some exceptions being raised and not handled. These problems can be avoided by guidance on the use of exceptions as part of the application programming practices procedures of the organisation or the specific project. Topics to be included in this guidance are:

- general and project specific exceptions which have been defined and are allowed;
- placement of exception handling AP;
- enumerating all intended side effects and verifying that there are no other side effects;
- ensuring the integrity of critical state data during exception processing.

Criteria for distinguishing what conditions should be handled through control flow constructs as part of normal processing versus abnormal conditions where use of exception handling is appropriate.

G.5.4 Checking input and output

G.5.4.1 General

Data corruption due to a transient failure or an invalid result can have serious consequences on subsequent processing if allowed to propagate. The base attributes related to input and output checking mitigate such consequences by containing the error. The two base attributes discussed in G.5.4.2 anf G.5.4.3 are:

- input data checking, and
- output data checking.

G.5.4.2 Input data checking

Input data includes data from another routine, data from the external environment, and data stored in memory from a previous iteration. Input data should be checked for validity before processing. Such checks reduce the likelihood of incorrect results or corrupted data being propagated. At a minimum, the values of the inputs should be checked for data type and being within an acceptable range. If possible, reasonableness checks on the data should also be performed. Provisions should exist in the AP to detect invalid input and to bring the module to a known state (i.e., default or previously valid values) as defined in the higher-level design.

G.5.4.3 Output data checking

Output data – whether to the external environment, to another routine or stored for use in a subsequent iteration – should be checked for validity. At a minimum, this validity check should ensure that the values are of the appropriate data type and are within acceptable ranges. It is more desirable that the values also be checked for reasonableness. However, such reasonableness checks should not be so restrictive that they spuriously reject correct values.

Provisions for handling rejected output values according to the design should also be present in the AP.

G.6 Traceability

G.6.1 General

As defined earlier in this annex, traceability refers to attributes of safety AP which support verification of correctness and completeness compared with the AP design. The intermediate attributes for traceability are:

- readability;
- controlling use of built-in functions (G.6.2);
- controlling use of compiled libraries (G.6.3).

Since readability is also an intermediate attribute of maintainability, it is discussed in G.3.4.8. The latter two attributes and their relevance to safety are discussed in G.6.2 and G.6.3.

G.6.2 Controlling use of built-in functions

Nearly all languages include built-in functions for frequently used programming tasks to maximise programmer productivity. However, the limitations of these functions and the way in which they handle exceptions may not be as well-known as those of the basic language constructs. Thus, the use of such functions raises safety concerns.

Concerns over the use of built-in functions can be addressed through organisational or project specific guidelines. Regression test cases make it possible to establish conformance with expected results of new releases of compilers and runtime libraries. Thus, test cases, procedures, and results of previous testing for allowable built-in functions should be retained. Testing should also assess behavior for out-of-bounds and marginal conditions (e.g., negative arguments on a square root routine; improperly terminated strings for a string copy routine, etc.) in the specific runtime environment.

G.6.3 Controlling use of compiled libraries

Compiled libraries are routines written and compiled by an entity other than the development group. Applications of compiled libraries include input/output operations, device drivers, or mathematical operations that are not defined in the standard language. Such libraries can be supplied by application programming tool vendors, third parties, or other departments of the development organisation. Concerns for such libraries are similar to those for built-in functions.

Concerns over the use of compiled libraries can be addressed by controlling the use of function calls to such libraries through organisational or project-specific guidelines.

Like built-in functions, a set of test cases, procedures, and results should be maintained. The test cases should assess behavior for normal, out-of-bounds, and marginal conditions in the specific runtime environment. Regression testing should be performed for each new release of the compiled library.

G.7 Maintainability

G.7.1 General

AP maintainability reduces the likelihood that errors will be introduced while making changes. The intermediate attributes related to maintainability that affect safety include:

- readability: those attributes of the AP that facilitate the understanding of the AP by project personnel;
- data abstraction: the extent to which the AP is partitioned and modularised so that the collateral impact and likelihood of unintended side effects due to AP changes are minimised;
- functional cohesiveness: the appropriate allocation of design level functions to AP devices in the AP (one procedure; one function);
- malleability: the extent to which areas of potential change are isolated from the rest of the AP;
- portability: the major safety impact of which is the avoidance of non-standard functions of a language.

G.7.2 Readability

G.7.2.1 General

Readability allows AP to be understood by qualified development personnel other than the writer. The importance of readability for maintainability can be seen through studies in which manual AP reading (desk checking) was found to be more effective than structural or functional testing for finding application programming faults. It is reasonable to extrapolate that readability would also enhance identifying AP to be changed during corrective or adaptive maintenance and would reduce the likelihood of introducing new faults during such maintenance.

There are no general standards for readability that can be mandated or even recommended. However, organisational or project-specific application programming style and practice manuals (or related guidelines) are expected for SISs. The following base attributes are related to readability.

- conforming to indentation guidelines;
- using descriptive identifier names;
- commenting and internal documentation;
- limiting subprogram size;
- minimizing mixed language programming;
- minimizing obscure or subtle programming constructs;
- minimizing dispersion or related devices;
- minimizing use of literals.

G.7.2.2 Conforming to indentation guidelines

Appropriate indentation facilitates the identification of declarations, control flows, non-executable comments, and other devices of AP. Indentation guidelines are generally part of a project specific or organisational programming style or standards. Significant issues to be addressed by indentation practices are the handling of:

- programming blocks (sequences of statements bounded by begin and end);
- comments;
- branching constructs (e.g., if...then...else, case statements, loops, etc.);
- multiple levels of nesting (e.g., a do loop within a do loop);
- variable and subroutine declarations;
- application programming tool directives;
- exception raising and handling.

G.7.2.3 Using descriptive identifier names

Names for variables, procedures, functions, data types, constants, exceptions, objects, methods, labels, and other identifiers that are not easily understood can impede review and maintenance. Safety concerns arising from naming practices can be alleviated when names are required to be descriptive, consistent, and traceable to higher-level (i.e., AP design) documents. Naming conventions are an important part of the application programming style and practices manual.

Examples of issues to be addressed include:

- identification of plant input data (e.g., should the variable refer to a sensor, or should it be called loop1_hot_leg_TC1);
- how looping variables should be named (e.g., “i,j,k” or longer titles);
- local renaming of identifiers (e.g., “average procedure mean” renamed as “mean”);
- distinguishing between different categories of identifiers (e.g., a suffix on all data types with an _T to distinguish them from variables);
- lists of project-specific terminology and reserved words (e.g., restrictions on the use of the terms "alarm", "limit", etc.).

Use of the same name for a different purpose is to be avoided unless obviously advantageous and, when employed, should be accompanied by clear, consistent, and unambiguous notations. Multiple use of the same name can be confusing. A further problem can occur if the language supports precompiled units. A variable with the same name in two different packages, one of which is used by the other may be interpreted by the application programming tool in a different manner than intended by the program writer. In some cases, the programmer may have omitted the declaration of a name in a package. Thus, another package can cause a different variable with the same name to be used in a totally unintended manner. If the particular branch or execution path is not encountered frequently, it is possible that such a fault would not be discovered until it causes a run-time failure.

Use of reserved words for user-selected identifiers (in languages where this feature is allowed) is undesirable.

G.7.2.4 Commenting and internal documentation

Incomplete comments, inconsistent formats, and comments that are not updated to reflect the current AP impede review and raise safety concerns. These problems can be minimised by guidance in the organisational or project application programming standards that controls comments and internal (to the AP) documentation. Examples of items, when incorporated, that should be located in the prologue section include the following:

- the subprogram or unit purpose and how achieved;
- functions and performance requirements, and external interfaces that the subprogram or unit helps implement;
- other subprograms or units called and their dependencies;
- use of global and local variables and, if applicable, memory and register locations together with special maintenance instructions;
- the responsible programming department or section;
- date of creation of the unit;
- date of latest revision, revision number, problem report number, and title associated with the revision, intended failure behavior and related information for all major segments of the AP;
- inputs and outputs, including data files referenced during unit entry of execution;

- comments on the purpose, scope, and limitations on each argument (for subprograms with arguments);

Similar examples for documentation within the AP include:

– reference to higher level design documentation in comments associated with data type, variable, and constant declarations;

– purpose and expected results at the beginning of branches and programming blocks;

– detailed in-line comments explaining unusual constructs and deviations from programming practices.

G.7.2.5 Limiting subprogram size

Some documents recommend specific limits on the AP of each subprogram or unit. For example, an average of 100 non-expandable statements and a maximum of more than 200 such statements have been recommended. Concern with the size of subprograms was one of the motivators for the adoption of structured programming. Small subprograms (one or two pages) are easier to review than longer ones. However, the limits on allowable size should also take into account the nature of the program and the language. In process safety and control systems, a given AP should frequently handle a multitude of sensed quantities, and the data declarations (with required comments) for these can by themselves amount to more than a page. The criterion for this base attribute is therefore that guidance on size be provided, rather than a universal numerical threshold.

G.7.2.6 Minimising mixed language programming

Mixed language programming (e.g., “sequential function chart” for sequential controls, ladder for boolean logic and “function block” for more sophisticated functions (scaling, means, etc…) presents difficulties for reviewers and maintainers and is therefore a safety concern. When this practice cannot be avoided, the difficulties can be minimised by placing the "foreign" language AP adjacent to the dominant language routine with which it interfaces (e.g., an in-line assembly application programming tool directive in the input processing routine associated with an interrupt) so that readability is enhanced.

When this practice cannot be avoided, the difficulties can be minimised by placing the "foreign" language AP embedded within the dominant language routine with which it interfaces (e.g., structured text embedded within a function block in a function block diagram) so that readability is enhanced.

G.7.2.7 Minimising obscure or subtle programming constructs

Obscure application programming constructs can generally be characterised as the use of indirect techniques to decrease the amount of application programming or logic solver processing required achieving a result. Such application programming practices present problems in review and maintenance and hence are a safety concern. For example shifting an integer to the left is equivalent to doubling its value. However, the former construct would be obscure if the design calls for doubling the value (i.e., it would be preferable to perform the multiplication); the latter construct would be obscure if the design calls for shifting the value to the left (i.e., it would be preferable to perform the shifting operation in the AP rather than multiplying by 2). Appropriate commenting can minimise the impact of obscure or marginally obscure application programming changes (e.g., adding the value to itself as a means of doubling it).

Inversion of sensor or actuator actual states in logic states through “NOT” functions should be avoided as well as multiplexing booleans in integers and latching outputs.

G.7.2.8 Minimising dispersion of related devices

If related devices of the AP are dispersed in a program, it is necessary to refer to multiple locations within an AP listing during reviews and maintenance. However, the specific nature of

the dispersion varies by language. For example, some languages allow for interface specifications separated from the body of the AP; others allow for "prototyping" for a similar purpose. In languages with strong data typing, it may be desirable to centralise all type declarations in a single file (or set of files); in object-oriented languages, it may be desirable to segregate base classes from derived classes. Review is facilitated and safety is enhanced if project-specific guidance is provided on the placement of related devices in the AP.

G.7.2.9 Minimising use of literals

Literals (i.e., an actual number or string in the AP) are more difficult to identify than names to which a constant value is assigned at the beginning of the module. Literals impact safety because they decrease readability and complicate maintainability, particularly if the literal is associated with a process parameter which may be tuned or a conversion factor which may be changed upon recalibration of an instrument. It is far easier to change one value set at the beginning of a file than it is to guarantee that all literals associated with such a parameter have been changed completely and correctly throughout all relevant files.

G.7.3 Data abstraction

G.7.3.1 General

Data abstraction is the combination of data and allowable operations on that data into a single entity, and establishment of an interface which allows access, manipulation and storage of the data only through the allowable operations. It is an important contributor to safety by virtue of reducing or eliminating potential side effects of changing variables either during runtime or in AP maintenance activities. This principle is associated with the following specific base attributes:

- minimizing the use of global variables;
- minimizing the complexity of the interface defining allowable operations.

G.7.3.2 Minimising the use of global variables

It is desirable to limit the use of global variables in safety related programs because of the potential for unintended side effects. Readability is enhanced if variables are set and used in the same routine. These variables can be made available to other routines through established and controlled interfaces which minimise the possibility of unintended interactions. For the same reasons, dependencies among internal stored data of different routines should be avoided or controlled.

To avoid potential safety concerns, local variables within different programs should not share the same storage locations.

Global variables that can be written from more than one logic instance should be avoided in AP because of the potential for unintended side effects.

G.7.3.3 Minimising the complexity of interfaces

Interfaces are a frequent cause of AP failures. Complex interfaces are difficult to review and maintain and are therefore not desirable in safety related programs. Characteristics that contribute to complexity include:

- large numbers of arguments used in calling routines;
- use of terse expressions when different modes or options are used;
- lack of easily understood restrictions and limitations on the use of allowable operations.

G.7.4 Functional cohesiveness

G.7.4.1 General

Functional cohesiveness refers to a clear correspondence between the functions of an AP and the structure of its devices. Functional cohesiveness has a single base attribute.

G.7.4.2 Single purpose function and procedures

Review and maintenance are facilitated when every given procedure, subprogram, or function implements only one task or purpose specified in the AP design.

Subprograms, functions, or procedures that perform multiple tasks should be separated and written as separate functions. A simple way to test if a function is a single purpose function is to check to determine if the function can be summarised by a sentence in the following form:

"verb + object(s)"

IEC 61511 expects the typicals to be iterated and a SIF to be implemented on a single logic solver.

G.7.4.3 Single purpose variables

The principle of single purpose functions should be applied to variables. A variable should be used for a single purpose only.

G.7.5 Malleability

G.7.5.1 General

Malleability is the ability of an AP to accommodate changes in functional requirements. Malleability extends data abstraction with the motivation toward isolating areas of potential change. To implement a malleable AP system, it is necessary to identify what is expected to be constant and what is expected to be changed, and to isolate what is expected to be changed into easily identifiable areas that can be altered with a minimum of collateral changes. Malleability has a single base attribute.

G.7.5.2 Isolation of alterable functions

Review and maintenance are facilitated when functions that can be altered are isolated, so that changes in these do not affect other AP or data. In many cases, such functions are hardware-related functions that should be changed when the platform changes, the system changes, or when new devices are used to replace old devices such as a more powerful logic solver of the same product line from a manufacturer.

To a large extent, the isolation of alterable functions is a design issue related to data abstraction. As such, a detailed discussion is beyond the scope of this guidance.

G.7.6 Portability

G.7.6.1 General

From the perspective of safety, the benefits of portability are the adherence to standard programming constructs that yield predictable and consistent results across different operating platforms. Thus, AP which is reused or converted to run on a different platform will be easier to maintain. Attributes related to portability which have been discussed elsewhere include:

- minimizing the use of built-in functions;

- minimizing the use of compiled libraries;
- minimizing dynamic binding;
- minimizing tasking;
- minimizing asynchronous constructs (interrupts).

The single base attribute related to portability is avoiding use of non-standard, or "enhanced" constructs specific to a particular application programming tool or a application programming tool in combination with the execution platform.

G.7.6.2 Isolation of non-standard constructs

Where non-standard constructs are necessary, they should be clearly identified together with the rationale, limitations, and version dependencies.

Bibliography

[1] IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

[2] IEC 61025:2006, *Fault tree analysis (FTA)*

[3] IEC 61078:2006, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

[4] IEC 61131-3:2013, *Programmable controllers – Part 3: Programming languages*

[5] IEC 61165:2006, *Application of Markov techniques*

[6] IEC 61506, *Industrial-process measurement and control – Documentation of application software*

[7] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[8] IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

[9] IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

[10] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[11] IEC 61882:2001, *Hazard and operability studies (HAZOP Studies) – Application guide*

[12] IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[13] IEC 62502:2010, *Analysis techniques for dependability – Event tree analysis (ETA) –*

[14] IEC 62551:2012, *Analysis techniques for dependability – Petri net techniques*

[15] ISO 9000:2015, *Quality management systems – Fundamentals and vocabulary*

[16] ISO 10418:2003, *Petroleum and natural gas industries – Offshore production installations – Analysis, design, installation and testing of basic surface process safety systems*

[17] ISO TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

[18] ISO 17776:2000, *Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment*

[19] ISO 31000:2009, *Risk management – Principles and guidelines*

[20] API RP14C:2001(R2007), *Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms*

[21] ISA TR84.00.02:2002, *Part 1 Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 1: Introduction* (note updated 2015 version below)

[22] ISA TR84.00.02:2002, *Part 2: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 2: Determining the SIL of a SIF via Simplified Equations* (note updated 2015 version below)

[23] ISA TR84.00.02:2002, *Part 3: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 3: Determining the SIL of a SIF via Fault Tree Analysis* (note updated 2015 version below)

[24] ISA TR84.00.02:2002, *Part 4: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 4: Determining the SIL of a SIF via Markov Analysis* (note updated 2015 version below)

[25] ISA TR84.00.02:2002, *Part 5: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 5: Determining the PFD of SIS Logic Solvers via Markov Analysis* (note updated 2015 version below)

[26] ISA TR84.00.02:2015, *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions ISBN: 1-55617-802-6*

[27] ISA TR84.00.03:2012, *Mechanical Integrity of Safety Instrumented Systems (SIS)*

[28] ISA TR84.00.04:2015, *Part 1: Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

[29] ISA TR84.00.09: 2013, *Security Countermeasures Related To Safety Instrumented Systems (SIS)*

[30] NFPA 85:2015, *Boiler and combustions systems hazards code*

[31] CCPS/AICHE, *Human Factors Methods for Improving Performance in the Process Industries (1st edition), John Wiley & Sons (2007), ISBN 0 4701 1754 0*

[32] CCPS/AIChE, *Guidelines for Preventing Human Error in Process Safety (1st edition), John Wiley & Sons (2004), ISBN 08169 0461 8*

[33] CCPS/AIChE, *Guidelines for Chemical Process Quantitative Risk Analysis* (second edition), New York: American Institute of Chemical Engineers (2000), 0 8169 0720 X

[34] CCPS/AIChE*, Guidelines for Safe Automation of Process Applications, 1993*

[35] CCPS/AIChE, *Guidelines for Safe Storage and Handling of High Toxic Hazard Material*

[36] CCPS/AIChE, *Guidelines for Vapor Release Mitigation*

[37] CCPS/AIChE, *Guidelines for the Technical Management of Chemical Process Safety*

[38] CCPS/AIChE, *Layer of Protection Analysis, Simplified Process Risk Assessment, 2001*

[39] HSE, *Reducing Risk Protecting People, Health and Safety Executive, London (2001) ISBN No. 07176-2151-0*

[40] HSE, *Reducing error and influencing behavior, HSG48, Health and Safety Executive, London (2009), ISBN 978 0 7176 2452 2*

[41] NAMUR recommendation NE130:2011, *"Prior use"-Devices for Safety Instrumented Systems and simplified SIL Calculation*

[42] OSHA 29 CFR 1910.119:2013, *Process safety management of highly hazardous chemicals*

_____

SOMMAIRE

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

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

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

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

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

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

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

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

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

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

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

AVANT-PROPOS

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

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

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

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

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

Le texte de cette norme est issu des documents suivants:

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

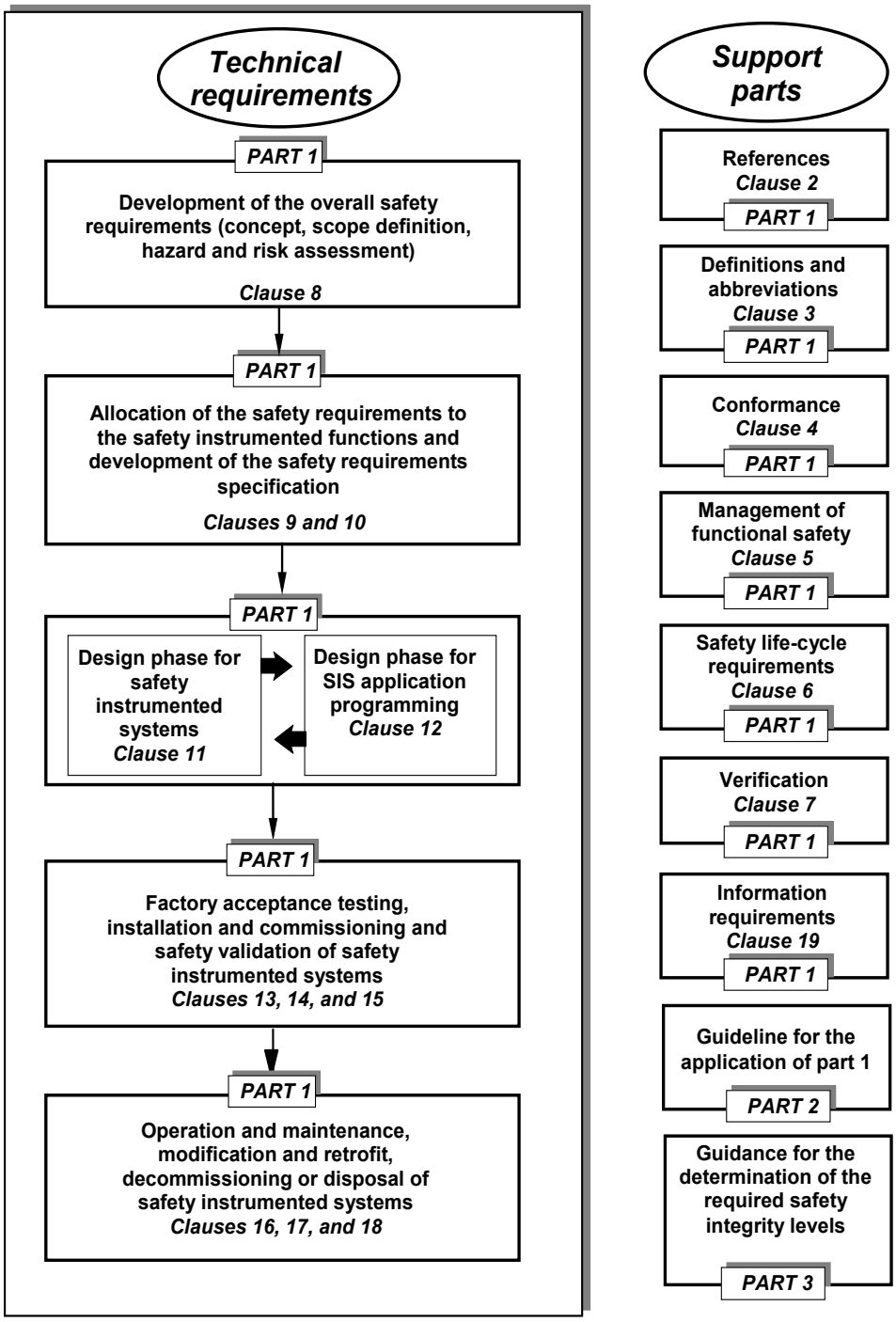
Dans la plupart des cas, la meilleure sécurité est obtenue, chaque fois que cela est possible, par des processus à conception à sécurité intrinsèque combinée, au besoin, avec un certain nombre de systèmes de protection, fondés sur différentes technologies (par exemple, chimique, mécanique, hydraulique,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

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

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

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

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



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

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

Figure 1 – Cadre général de la série IEC 61511

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

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

1 Domaine d'application

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

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

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

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

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

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

2 Références normatives

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

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

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, définitions et abréviations donnés dans l'IEC 61511-1:2016, Article 3 s'appliquent.

Annexe A
(informative)

Lignes directrices pour l'IEC 61511-1

NOTE Les numéros d'articles et de paragraphes indiqués à l'Annexe A sont les mêmes que ceux de l'IEC 61511-1:2016pour faciliter le référencement croisé.

A.1 Domaine d'application

Aucune autre ligne directrice n'est fournie.

A.2 Références normatives

Aucune autre ligne directrice n'est fournie.

A.3 Termes, définitions et abréviations

Aucune autre ligne directrice n'est fournie.

A.3.2.66
fonction de sécurité
il convient qu'une fonction de sécurité prévienne l'arrivée d'un événement dangereux spécifié. Par exemple, "empêcher que la pression dans le réservoir #ABC456 ne dépasse 100 bars". Une fonction de sécurité peut être obtenue par:

- un SIS unique, ou
- un ou plusieurs SIS et/ou d'autres couches de protection.

Chaque SIS ou toute autre couche de protection doit pouvoir réaliser la fonction de sécurité et la combinaison globale doit permettre d'obtenir la réduction de risque exigée (cible de sécurité du processus).

A.3.2.67
fonction instrumentée de sécurité
les fonctions instrumentées de sécurité (SIF) sont dérivées de la fonction de sécurité, ont un niveau d'intégrité de sécurité (SIL) associé et sont réalisées par un système instrumenté de sécurité (SIS) spécifique. Par exemple, "fermer la vanne #XY123 en 5 s, lorsque la pression dans le réservoir #ABC456 atteint 100 bars". Les appareils d'un SIS peuvent être utilisés par plusieurs SIF.

A.4 Conformité à l'IEC 61511-1:2016

Aucune autre ligne directrice n'est fournie.

A.5 Gestion de la sécurité fonctionnelle

A.5.1 Objectif

Aucune autre ligne directrice n'est fournie.

A.5.2 Lignes directrices relatives aux "Exigences"

A.5.2.1 Généralités

Lorsqu'un organisme est chargé d'une ou de plusieurs activités nécessaires à la sécurité fonctionnelle et que cet organisme travaille selon des procédures d'assurance qualité, de nombreuses activités décrites à l'Article 5 de l'IEC 61511-1:2016seront déjà réalisés à des fins de qualité. Lorsque c'est le cas, il se peut qu'il soit inutile de répéter ces activités dans un but de sécurité fonctionnelle. Dans de tels cas, il convient que les procédures d'assurance qualité soient passées en revue pour s'assurer qu'elles conviennent, de manière que les objectifs de la sécurité fonctionnelle soient atteints.

A.5.2.2 Organisation et ressources

Il convient que la structure organisationnelle associée aux SIS au sein d'une entreprise/d'un site/d'une installation/d'un projet soit définie et que les rôles et les responsabilités de chaque personne/service soient clairement compris et soient communiqués. Dans la structure, il convient que les différents rôles soient identifiés individuellement, que leurs buts soient précisés et qu'ils soient décrits. Il convient que les responsabilités incombant à chaque rôle soient identifiées très clairement; il convient également que des responsabilités spécifiques soient identifiées. En outre, il convient de définir à qui chaque personne rend compte et de désigner la personne responsable des affectations. Le but est d'assurer que chaque personne, dans une organisation, comprend son rôle et ses responsabilités vis-à-vis des SIS.

Il convient que les compétences et les connaissances exigées pour mettre en œuvre toutes les activités du cycle de vie de sécurité relatives aux SIS soient identifiées; et, pour chaque qualification, il convient que les niveaux exigés de compétence soient définis. Il convient que les ressources soient évaluées par rapport à chaque qualification vis-à-vis des compétences et également par rapport au nombre de personnes exigées par qualification. Lorsque des différences sont identifiées, il convient que des programmes d'aménagement soient établis pour permettre aux niveaux de compétence exigés d'être obtenus à temps. Il convient que les personnes soient disponibles pendant toute la phase dont elles sont responsables afin de garantir un transfert d'expérience et un arrière-plan de cycle de vie. En cas de pénurie de compétences, le personnel convenablement qualifié et expérimenté peut être recruté ou employé sous contrat.

A.5.2.2.1 Aucune autre ligne directrice n'est fournie.

A.5.2.2.2 Aucune autre ligne directrice n'est fournie.

A.5.2.2.3 Aucune autre ligne directrice n'est fournie.

A.5.2.3 Evaluation et gestion des risques

Les exigences établies en 5.2.3 de l'IEC 61511-1:2016visent à identifier les dangers, à évaluer les risques et à déterminer la réduction de risque nécessaire. Il est admis qu'il y a de nombreuses méthodologies différentes et disponibles pour effectuer ces évaluations. L'IEC 61511-1:2016ne privilégie aucune méthodologie particulière. Voir A.8.2.1 pour d'autres lignes directrices.

A.5.2.4 Planification de la sécurité

Le Paragraphe A.5.2.4 a pour objet de s'assurer que, dans le projet global, une planification adéquate de la sécurité est conduite, de sorte que toutes les activités exigées pendant chaque phase du cycle de vie soient traitées (conception technique, exploitation en installation, par exemple). La norme n'exige aucune structure particulière pour ces activités de planification, mais elle en exige une revue ou une mise à jour périodique.

A.5.2.5 Mise en œuvre et surveillance

A.5.2.5.1 Le Paragraphe 5.2.5.1 de l'IEC 61511-1:2016a pour objet de s'assurer que des procédures efficaces de gestion sont en place pour:

- veiller à ce que toutes les recommandations résultant de l'analyse de danger, de l'évaluation de risque, de toute autre évaluation et activité d'audit, de vérification et de validation, aient été prises en compte d'une manière satisfaisante;
- vérifier que le SIS fonctionne bien selon la spécification des exigences de sécurité (SRS) durant toute sa vie opérationnelle.

A.5.2.5.2 Il est à noter que, dans ce contexte, les fournisseurs pourraient inclure des entreprises de conception et des entreprises de maintenance, ainsi que des fournisseurs d'appareils. Il convient que les éléments matériels et logiciels des composants SIS soient fabriqués selon un système de gestion de la qualité reconnu (la série de normes ISO 9000, par exemple).

Il convient qu'une revue des performances du SIS soit périodiquement entreprise pour s'assurer que les hypothèses d'origine, faites pendant le développement de la SRS, continuent d'être respectées. Par exemple, il convient qu'une revue périodique du taux de défaillances estimé de différents appareils dans un SIS soit effectuée, pour s'assurer qu'il demeure tel qu'il a été défini à l'origine. Si les taux de défaillances sont plus mauvais que ceux prévus à l'origine, une modification de la conception peut être nécessaire. De même, il convient que le taux de sollicitation sur le SIS soit revu. Si le taux est plus élevé que celui qui a été estimé à l'origine, un ajustement du SIL peut alors être nécessaire.

A.5.2.5.3 Aucune autre ligne directrice n'est fournie.

A.5.2.5.4 Aucune autre ligne directrice n'est fournie.

A.5.2.6 Evaluation, audits et révisions

Les évaluations et les audits sont des outils destinés à la détection et à l'élimination des erreurs. Les alinéas ci-dessous font clairement la distinction entre ces activités.

L'évaluation de la sécurité fonctionnelle (FSA, Functional Safety Assessment) vise à évaluer si les dispositions prises pendant les phases du cycle de vie qui sont prévues sont adéquates pour la réalisation de la sécurité ou non. Les décisions finales sont prises par des examinateurs sur la base des décisions prises par les responsables de la réalisation de la sécurité fonctionnelle. Il s'agit, par exemple, de procéder à une évaluation avant la mise en service, afin de déterminer si les procédures de maintenance sont adéquates ou non.

Les auditeurs de la sécurité fonctionnelle détermineront à partir des dossiers du projet ou de l'installation si les procédures nécessaires ont été appliquées ou non, à la fréquence spécifiée, par des personnes ayant la compétence nécessaire. Il n'est pas exigé que les auditeurs portent des jugements sur l'adéquation du travail qu'ils sont en train d'étudier. Si toutefois ils se rendent compte qu'il pourrait être bénéfique de faire des changements, il convient alors qu'une observation soit incluse dans le rapport.

Il convient de noter que dans de nombreux cas il peut y avoir une superposition du travail de l'examinateur et de l'auditeur. Par exemple, un évaluateur ou un auditeur peut devoir déterminer non seulement si un opérateur a reçu la formation nécessaire, mais en plus porter un jugement quant à savoir si la formation a eu comme résultat l'obtention de la compétence exigée.

A.5.2.6.1 Evaluation de la sécurité fonctionnelle (FSA)

L'utilisation de l'évaluation de la sécurité fonctionnelle (FSA) est fondamentale pour démontrer qu'un SIS remplit ses exigences concernant les SIF et les SIL. L'objectif de base

de cette évaluation est de démontrer la conformité aux normes et aux pratiques agréées, par l'intermédiaire d'une évaluation indépendante du processus de développement du système. Une évaluation d'un SIS peut être nécessaire à différentes étapes du cycle de vie. Afin de conduire une évaluation efficace, il convient de développer une procédure qui définit le domaine d'application de cette évaluation, ainsi que quelques lignes directrices sur le profil de l'équipe d'évaluation.

Les attributs suivants sont considérés comme étant de bonne pratique pour la FSA:

a) Il convient d'établir un plan pour chaque FSA, en identifiant les dispositions telles que le domaine d'application de l'évaluation, les évaluateurs, leurs compétences et les informations à générer par l'évaluation.

b) Il convient que la FSA prenne en compte d'autres normes et usages, qui peuvent être contenus dans des normes externes ou internes à l'entreprise, des guides, des procédures ou des recueils d'instructions de bonne pratique. Il convient que le plan de la FSA définisse les éléments qui doivent être évalués pour le périmètre particulier de l'évaluation/du système/de l'application.

c) La fréquence des FSA peut varier en fonction des différents développements de système, mais il convient qu'un minimum soit toujours fixé, avant que les dangers ne se présentent au système. Certaines sociétés souhaitent également procéder à une évaluation avant la phase de construction/installation, pour éviter une reprise ultérieure et coûteuse dans le cycle de vie.

d) Il convient que la fréquence et la rigueur de la FSA soient définies en tenant compte de certains attributs du système comme:

   - la complexité;
   - l'importance de la sécurité;
   - l'expérience précédente de systèmes semblables;
   - la normalisation des caractéristiques de conception.

e) Il convient qu'une justification suffisante des activités de conception, d'installation, de vérification et de validation soit disponible avant l'évaluation. La disponibilité d'une justification suffisante pourrait être en elle-même un critère d'évaluation. Il convient que la justification représente l'état courant/approuvé de la conception ou de l'installation du système:

   - Il convient que l'indépendance du/des évaluateur(s) soit réelle.
   - Il convient que le/les évaluateur(s) aient une expérience et une connaissance appropriées de la technologie et du domaine d'application du système en cours d'évaluation.
   - Il convient qu'une approche systématique et cohérente de la FSA soit maintenue tout au long du cycle de vie et pour tous les systèmes. La FSA étant une activité subjective, il convient de définir des lignes directrices détaillées, éventuellement par l'utilisation de listes de contrôle établissant ce qui est acceptable pour une organisation, afin d'éliminer dans toute la mesure du possible tout jugement subjectif.
   - Des techniques d'inspection pour montrer que les fonctions du programme d'application remplissent les exigences de danger du processus.
   - Des essais fonctionnels pour montrer que le programme d'application a exécuté les fonctions exigées et, autant que possible, qu'une fonctionnalité supplémentaire dans le programme d'application ou dans le logiciel intégré ne risquerait pas d'avoir comme conséquence des conditions dangereuses.
   - Des essais structuraux (voir A.12.5.3) pour montrer que le programme d'application a exécuté les fonctions exigées dans les temps nécessaires et pour identifier si des zones n'ont pas encore été soumises à l'essai dans le programme d'application, ce qui (parce qu'elles n'ont pas encore été soumises à l'essai) peut être à l'origine de conditions dangereuses.

- Une analyse de défaillance fonctionnelle et une analyse "et si" visant à montrer que les fonctions du programme d'application ne risqueraient pas de donner lieu à des conditions dangereuses.
- Des procédures sont en place pour montrer qu'un processus maîtrisé de développement et de vérification est en place, mais aussi que la bonne version du programme d'application et que la bonne version du logiciel intégré sont utilisées.
- La planification et les procédures d'audit ont été spécifiées.

Avant le début de la phase suivante du cycle de vie, il convient que les informations enregistrées produites à partir de la FSA soient complètes et que les conclusions soient agréées par les responsables de la gestion de la sécurité fonctionnelle concernant le SIS.

Le recours à une personne indépendante de l'équipe de projet a pour but d'accroître l'objectivité de l'évaluation. Le recours à une personne compétente de haut niveau (par exemple, expérience, position) a pour but d'assurer que les préoccupations exprimées par l'équipe de projet seront dûment prises en compte et traitées. Comme la Note de l'IEC 61511-1:2016 , 5.2.6.1.3 le suggère également, pour les équipes impliquées dans certains grands projets ou certaines évaluations importantes, il peut être nécessaire d'avoir plusieurs personnes compétentes de haut niveau dans ces équipes, qui soient indépendantes de l'équipe de projet d'origine.

En fonction de l'organisation et de l'expertise au sein de l'entreprise, un organisme externe peut devoir être sollicité pour satisfaire à l'exigence d'un examinateur indépendant. Inversement, les entreprises disposant d'instances internes compétentes dans les domaines de l'évaluation des risques et de l'application des SIS, indépendantes et distinctes (de par leur gestion et autres ressources) des instances responsables du projet, peuvent avoir la possibilité d'utiliser leurs propres ressources pour satisfaire aux exigences d'un organisme indépendant.

La profondeur de l'évaluation dépend de la taille et de la complexité du projet. Il peut être parfois possible d'évaluer les résultats de différentes phases en même temps. Cela est particulièrement vrai dans le cas de petits changements au sein d'une installation en fonctionnement.

Dans certains pays, une FSA entreprise à l'étape 3 est souvent nommée "Revue de sécurité de prédémarrage" (Pre-Startup-Safety-Review ou PSSR).

Voir le Tableau F.1, case 10. Il convient que les termes de référence de la FSA fassent l'objet d'un accord dans la planification de la sécurité.

Il convient que les membres de l'équipe d'évaluation aient accès à toutes les informations qu'ils considèrent comme nécessaires pour conduire l'évaluation. Il convient d'inclure des informations issues de l'analyse de danger et de risque, de la phase de conception jusqu'à l'installation, la mise en service et la validation.

A.5.2.6.1.1 Dans certains cas, l'équipe de FSA peut être composée d'une seule personne, à condition qu'elle dispose des compétences et de l'expérience exigées pour l'activité.

A.5.2.6.1.2 Le nombre de personnes compétentes de haut niveau dans l'équipe d'évaluation peut varier, en fonction de différents éléments tels que la taille de l'application, les technologies associées, les exigences de communication (avec utilisateur/propriétaire, intégrateur, fabricant, par exemple) et du planning du projet.

Il convient que la personne compétente de haut niveau soit compétente dans les différentes technologies couvertes par l'application et dans les réglementations applicables, mais aussi qu'elle soit disponible pour satisfaire aux demandes de planification du projet.

A.5.2.6.1.3 Aucune autre ligne directrice n'est fournie.

A.5.2.6.1.4 Aucune autre ligne directrice n'est fournie.

A.5.2.6.1.5 Aucune autre ligne directrice n'est fournie.

A.5.2.6.1.6 Les outils utilisés dans la conception, le développement, le fonctionnement et la maintenance du SIS peuvent affecter l'intégrité du SIS par l'introduction d'anomalies dans le système final. Les outils peuvent provoquer une "imbrication" directe d'une partie de la fonctionnalité de l'outil dans le SIS (par exemple, bibliothèque utilisateur, interprètes) ou être "hors ligne" – c'est-à-dire, être utilisés pour générer des informations qui peuvent être vérifiées séparément (par exemple, outils de calcul de variables sur le terrain, outils d'essai); il peut également s'agir d'outils qui peuvent être connectés à un SIS d'exploitation – par exemple, des outils de maintenance. Dans chaque cas, il est important de comprendre les modes de défaillance potentielle et leurs effets, ainsi que les moyens de les contrôler. Des approches types de contrôle des anomalies dans des outils incluent:

- la confirmation de la traçabilité avec des normes nationales et internationales (cela pouvant inclure l'étalonnage et/ou des normes fonctionnelles, en fonction de la nature de l'outil);
- la prise en compte des rapports d'expérience des groupes d'utilisateurs et des preuves historiques sur les utilisations précédentes de l'outil;
- la revue et les essais fonctionnels des résultats obtenus suite à l'utilisation de l'outil;
- l'utilisation de la diversité dans les outils de développement et/ou d'essai (utilisation d'un code déduit de différents compilateurs, inspection de la sortie d'un outil de conception via l'utilisation d'un autre type d'outil d'inspection, par exemple);
- l'outil est fourni comme partie intégrante d'un appareil IEC 61508-2:2010 et IEC 61508-3:2010.

Il convient que l'activité de la FSA examine la stratégie qui a été adoptée pour maintenir l'intégrité de la sortie des outils, selon qu'ils sont "imbriqués" ou "hors ligne" et qu'ils portent un jugement sur le niveau nécessaire d'assurance de l'outil qui a été atteint.

A.5.2.6.1.7 Aucune autre ligne directrice n'est fournie.

A.5.2.6.1.8 Aucune autre ligne directrice n'est fournie.

A.5.2.6.1.9 Aucune autre ligne directrice n'est fournie.

A.5.2.6.1.10 Aucune autre ligne directrice n'est fournie.

A.5.2.6.2 Révision et audit de la sécurité fonctionnelle

a) Catégories d'audits

Les audits des SIS fournissent des informations intéressantes pour la direction de l'installation, pour les ingénieurs de maintenance et de conception des instruments. Cela permet aux membres de la direction de mettre en place une gestion proactive et de se rendre compte du degré d'implication et de l'efficacité de leurs SIS. De nombreux types d'audits peuvent être effectués. Il convient que le type réel, le domaine d'application et la fréquence des audits de toute activité reflètent l'impact potentiel de cette dernière sur l'intégrité de sécurité.

Les types d'activités d'audit peuvent inclure:

- les inspections;
- les visites de sécurité (par exemple, tour de visite de l'installation et revue d'incident);
- études SIS (via des questionnaires).

Il convient de faire une distinction entre "la surveillance et la vérification" et les activités d'audit. La surveillance et la vérification se concentrent sur l'évaluation des performances des activités spécifiques du cycle de vie (par exemple, inspecteur vérifiant l'achèvement de l'activité de maintenance avant que l'appareil ne soit renvoyé pour réparation). En revanche, les activités d'audit sont plus complètes et se concentrent sur la mise en œuvre globale des SIS dans le cadre du cycle de vie de sécurité SIS. Le fait de savoir si le programme de surveillance et de vérification a été exécuté ou non pourrait être déterminé par un audit.

Les audits et les inspections peuvent être effectués par le propre personnel de l'entreprise/du site/de l'installation/du projet (par exemple, auto-audit) ou par des personnes indépendantes (par exemple, auditeurs de services aux entreprises, département d'assurance qualité, organismes de contrôle, clients ou tiers).

Il se peut que les membres de la direction, à divers niveaux, désirent appliquer le type adéquat d'audit pour accéder à des informations sur l'efficacité de la mise en œuvre de leurs SIS. Les informations des audits pourraient être utilisées pour identifier les procédures qui n'ont pas été correctement appliquées et conduire à une amélioration de la mise en œuvre.

b) Stratégie d'audit

Un site/une installation/un projet mettant en œuvre des programmes d'audit peut considérer des programmes continus, indépendants ou d'auto-audit et d'inspection.

Les programmes continus sont mis à jour régulièrement pour refléter les performances des SIS précédents et les résultats d'audit, les préoccupations courantes et les priorités. Ils couvrent toutes les activités et tous les aspects relatifs au site/à l'installation/au projet concernant les SIS, dans une période de temps et à un degré d'approfondissement appropriés.

La raison première et la valeur ajoutée des audits proviennent du fait qu'il est possible d'agir en temps voulu sur les informations qu'ils fournissent. Les actions visent à renforcer l'efficacité des SIS, par exemple, pour aider à réduire au minimum le risque de blessure ou de mort encouru par les employés ou les personnes du public, contribuent à améliorer la culture de sécurité, à prévenir tout dégagement évitable de substance dans l'environnement.

En résumé, la stratégie d'audit peut être un panachage de différents types d'audits, conduite par la direction (le client) et a pour but de réintroduire des informations pertinentes en haut de la chaîne de direction pour initier une action en temps voulu.

c) Processus et protocoles d'audit

Le but général est d'établir le degré de conformité avec l'IEC 61511-1 et d'atteindre la valeur maximale de performance de l'audit, qui ne peut être obtenue que lorsque toutes les parties (y compris les auditeurs, le contact désigné, les directeurs de l'installation et le chef de départements/service, etc.) en comprennent le besoin et peuvent influencer chaque audit. Les processus et les protocoles d'audit suivants pourraient participer à assurer une certaine cohérence dans les démarches visant à atteindre ces objectifs. Ils portent sur les cinq principales étapes suivantes du processus d'audit:

1) Stratégie et programme d'audit:
   - il convient que le but de chaque audit soit clairement défini et que les groupes d'audit soient identifiés, ainsi que les rôles et les responsabilités de chacun d'eux;
   - il convient qu'il y ait une stratégie pour conduire les audits;
   - il convient qu'il y ait un programme d'audits;
   - il convient de procéder à des revues régulières du processus d'audit, du programme et de la stratégie de mise en œuvre.
2) Préparation de l'audit et planification préalable:

- Avant le début d'un audit, il convient qu'un cadre supérieur du site/de l'installation/du projet et/ou que le coordonnateur ad hoc de l'audit identifie un préposé aux contacts.
- Il convient que les auditeurs et le préposé aux contacts, dans un premier temps, examinent, comprennent et soient d'accord sur:
  - le domaine d'application de l'audit;
  - le calendrier d'exécution de l'audit;
  - les personnes qu'il convient de rendre disponibles;
  - les bases de l'audit ou la norme de l'audit;
  - le fait de consentir un effort supplémentaire lors de l'étape de préparation et de faire participer le personnel de l'installation, ce qui augmentera les chances de réussite de l'audit.
- Il convient de se baser sur les proportions indiquées ci-dessous pour répartir de façon appropriée le temps imparti à chaque étape:
  - la préparation de l'audit: 30 %;
  - la conduite de l'audit: 40 %;
  - compte rendu des résultats: 20 %;
  - le suivi de l'audit: 10 %;
- Il convient que l'auditeur se prépare à l'audit en rassemblant des informations, des procédures/des instructions, des données, puis en préparant des listes de contrôle, le cas échéant.
- Il convient que l'auditeur mette en avant et explique comment un changement éventuel au domaine d'application de l'audit peut avoir lieu pendant l'audit, si des observations/des défectuosités graves sont découvertes.

3) Conduite de l'audit:

- L'auditeur doit conduire l'audit sur plusieurs jours consécutifs pendant la période fixée pour l'audit, en tenant compte de l'éventuelle indisponibilité des personnes du site/de l'installation/du projet.
- Il convient que le préposé aux contacts soit périodiquement mis au courant des résultats identifiés pendant l'audit, évitant de ce fait des surprises à la fin de l'audit.
- Il convient que l'auditeur tente d'impliquer le personnel de l'installation dans le processus d'audit, afin que le personnel de l'installation s'approprie les résultats de l'audit.
- Le comportement de l'auditeur est crucial vis-à-vis du succès de l'audit: il convient qu'il tente d'être utile, constructif, courtois, objectif et d'aller en profondeur tout en étant sélectif.
- Il convient au minimum que l'auditeur essaie de respecter le domaine d'application et l'emploi du temps convenus – il convient de négocier les variantes.

4) Compte rendu de résultats:

- Il convient que l'auditeur tienne une réunion de conclusion à la fin de l'audit ou plus tard, mais avant que le compte rendu final ne soit publié.
- Il convient que des membres ad hoc de la direction aient l'opportunité de présenter leurs observations sur le projet de compte rendu et sur les résultats et de les discuter/commenter lors d'une réunion formelle de clôture, si cela est souhaité.
- Une pratique habituelle veut qu'il soit requis que le site/l'installation/le projet mette en place un plan d'action pour tenir compte des résultats du compte rendu.

5) Suivi de l'audit:

- Les comptes rendus d'audit exigent habituellement une réponse sous forme de plan d'action. L'auditeur pourrait vérifier l'achèvement satisfaisant de l'action à la date prévue ou au prochain audit, l'échéance la plus appropriée étant choisie.

- Des systèmes de suivi de site/d'installation/de projet peuvent être utilisés pour vérifier la mise en œuvre des plans d'action.
- Il convient que, périodiquement, une revue/un récapitulatif des résultats d'audit de chaque groupe d'audit soit considéré(e) et que ses résultats soient largement communiqués.
- Les résultats/conclusions des audits peuvent être utilisés pour passer en revue la fréquence des audits, et constituent des entrées utiles pour revoir la gestion des SIS.

A.5.2.6.2.1 Aucune autre ligne directrice n'est fournie.

A.5.2.6.2.2 Le FSA peut être réalisé par le personnel de l'entreprise/du site/de l'installation/du projet (auto-audit, par exemple) ou par des personnes indépendantes (des auditeurs de services aux entreprises, un département d'assurance qualité, des organismes de contrôle, des clients ou des tiers, par exemple). Voir l'IEC 61508-1:2010, Tableau 4 et Tableau 5 pour d'autres lignes directrices

A.5.2.6.2.3 Les Paragraphes 5.2.6.3, 5.2.6.4 et 5.2.6.5 de l'IEC 61511-1:2016renforcent le rôle que la gestion des changements joue dans le processus d'audit. Si l'analyse du danger d'origine a pris en compte les couches de sécurité non SIS qu'il convient d'enregistrer dans, par exemple, le BPCS ou les procédures d'opérateur et les alarmes, il convient de surveiller tous les changements apportés à ces systèmes pour garantir qu'ils ne réduisent pas la protection fournie par les couches de protection non SIS. De plus, des changements apparemment mineurs dans les numéros de version ou de mod dans le SIS ou les systèmes d'interface peuvent introduire des incompatibilités entre le programme d'application, le logiciel intégré et le matériel (voir par exemple combien il est difficile de revenir à des versions antérieures d'un programme logiciel). Il est donc important de vérifier que non seulement les éléments individuels sont maîtrisés, mais également que la configuration globale des éléments est maîtrisée. En particulier, la version d'AP et du logiciel doit être cohérente avec la version du matériel, avec les procédures d'exploitation et avec les interfaces pour lesquelles elle a été conçue.

A.5.2.6.2.4 Aucune autre ligne directrice n'est fournie.

A.5.2.7 Gestion de configuration du SIS

A.5.2.7.1 Pour gérer et maintenir la traçabilité des appareils pendant le cycle de vie, un mécanisme d'identification, de contrôle et de suivi du modèle/des versions de chaque appareil peut être établi.

A l'étape la plus en amont possible du cycle de vie de sécurité SIS, il convient qu'une identification unique de l'installation soit donnée à chaque appareil. Dans certains cas, les modèles/les versions antérieurs toujours en service peuvent également faire l'objet de contrôles et de maintenance. Il convient que ce soit la première étape dans le programme de gestion de configuration qui devrait intégrer les considérations suivantes.

Le système de gestion de configuration peut inclure:

a) une disposition pour une procédure d'identification de tous les appareils pendant toutes les phases du cycle de vie;

b) l'identification unique, du modèle/de la version et de l'état à la construction de chaque appareil comprenant le logiciel intégré et utilitaire et le programme d'application, le fournisseur, la date et, le cas échéant, les changements du modèle/de la version spécifiés à l'origine;

c) l'identification et le suivi de tous les actions et changements résultant des observations d'anomalies et des audits;

d) le contrôle de l'édition d'une révision mise en service, identifiant l'état et le modèle/la version des appareils associés;

e) des sauvegardes qui ont été établies pour s'assurer que des changements/des modifications non autorisés ne sont pas apportés au SIS, alors qu'il est en fonction;

f) l'identification des versions de chaque partie du programme d'application qui, ensemble, constituent une version spécifique d'un programme d'application complet;

g) une disposition pour la coordination de la mise à jour de plusieurs SIS dans une ou plusieurs installations;

h) l'autorisation documentée de la version mise en service;

i) une liste autorisée de signatures pour la version de l'appareil mis en service;

j) les appareils de l'étape/de la phase qui sont présentés sous contrôle de configuration;

k) le contrôle de la documentation associée livrable;

l) l'identification de chaque modèle/version d'un appareil;

   – la spécification fonctionnelle;

   – la spécification technique;

m) une liaison vers la gestion de la procédure de changement.

Il convient que tous les services/départements/organismes impliqués dans la gestion et la maintenance du SIS soient identifiés et que les responsabilités soient affectées et comprises.

En principe, les exigences de gestion de la configuration du programme d'application sont les mêmes que celles relatives aux appareils matériels du système. Néanmoins, le programme d'application mérite souvent une approche plus rigoureuse que nécessaire pour le matériel seul, car:

- la nature "logique" plutôt que "physique" inhérente du programme d'application est telle que sa configuration réelle est difficile à "observer", sauf en faisant référence à ses documents de support;
- il est facile à modifier (il n'est pas inhabituel qu'un programmeur puisse publier plusieurs versions différentes le même jour);
- la fonctionnalité de l'application dépend entièrement du bon fonctionnement du programme d'application, et le fait qu'il soit correct est donc essentiel pour une exploitation correcte du SIS dans son ensemble;
- elle peut réagir différemment avec des versions différentes du système PE, avec des changements des interfaces sur le monde externe, avec des plages de données d'entrée et de sortie différentes, voire avec des versions différentes de ses propres outils de développement;
- elle peut être spécifique à un jeu de spécification, une configuration de version, un sous-système SIS, un environnement et un lieu, mais ne peut pas pour autant être différentiée sauf par sa version et sa révision de gestion de configuration.

En plus des exigences normalisées de gestion de la configuration pour l'identification, le contrôle de la version et de la révision et la compatibilité entre les éléments, il convient d'utiliser des aspects types pour maintenir le contrôle sur le programme d'application, dont:

- l'utilisation de codes intégrés dans le programme d'application pour garantir qu'il ne peut être téléchargé que dans son hôte matériel prévu (particulièrement utile quand de nombreuses configurations différentes pourraient être utilisées en fonction des sites);
- l'utilisation de notes de version qui exigent une autorisation par des autorités nommées avant de pouvoir charger de nouvelles versions du programme dans le SIS;
- le maintien d'enregistrements sur le statut et la version de tous les éléments utilisés pour le développement, les essais et la maintenance du programme d'application traçables vers les spécifications adéquates et les résultats de vérification associés à la configuration complète;
- le maintien de sauvegarde, de sorte qu'un système puisse revenir à une version précédente;

- l'utilisation de cycles de modification commandés, où les changements seront organisés dans des versions définies, l'avantage étant que plusieurs versions différentes peuvent être en développement à différents niveaux de maturité sans interaction entre les différentes versions et ce qui permet également au cycle d'essai d'amener un certain niveau de stabilité à une version donnée avant sa sortie sur site.

A.5.2.7.2 Aucune autre ligne directrice n'est fournie.

A.6 Exigences relatives au cycle de vie de sécurité

A.6.1 Objectifs

Dans toute fonction de processus, la sécurité fonctionnelle obtenue dépend d'un certain nombre d'activités exécutées de manière satisfaisante. L'adoption d'une approche systématique du cycle de vie de sécurité vis-à-vis d'un SIS vise à s'assurer que toutes les activités nécessaires pour obtenir la sécurité fonctionnelle sont conduites et qu'il peut être démontré pour les autres qu'elles ont été exécutées dans un ordre approprié. L'IEC 61511-1:2016définit un cycle de vie type dans sa Figure 7 et son Tableau 2. Les exigences pour chaque phase de cycle de vie sont données aux Articles 8 à 18 de l'IEC 61511-1:2016 .

La norme admet que les activités spécifiées pourraient être structurées de différentes manières, à condition que toutes les exigences soient satisfaites. Cette restructuration peut être bénéfique si elle permet aux activités de sécurité d'être mieux intégrées dans les procédures habituelles du projet. L'Article 6 de l'IEC 61511-1: — a pour objet de s'assurer que, si un cycle de vie de sécurité SIS différent est utilisé, les entrées et la sortie de chaque phase du cycle de vie sont définies et que toutes les exigences importantes sont intégrées.

A.6.2 Lignes directrices relatives aux "Exigences"

A.6.2.1 La considération principale consiste à définir à l'avance le cycle de vie de sécurité du SIS qui va être utilisé. L'expérience a montré que des problèmes sont susceptibles d'apparaître, sauf si cette activité est planifiée bien à l'avance et si des accords sont conclus avec toutes les personnes, services/départements et organismes qui en prennent la responsabilité. Dans le cas le plus favorable, certains travaux seront retardés ou devront être refaits; dans le cas le plus défavorable, la sécurité peut être compromise.

Il convient que la hiérarchie de responsabilité dans chacune des phases du cycle de vie soit identifiée et communiquée aux parties concernées (par exemple, sous-fournisseurs, intégrateurs systèmes, utilisateurs finals), afin qu'elles soient au courant de leurs responsabilités, de la façon dont leurs activités sont relatives les unes aux autres et aux phases du cycle de vie de sécurité, mais aussi sur la façon dont leurs livraisons contribuent aux exigences globales de sécurité fonctionnelle et d'intégrité de la sécurité.

A.6.2.2 Bien qu'il ne s'agisse pas d'une exigence, il est généralement avantageux, à une étape précoce, d'établir une correspondance entre le cycle de vie de sécurité du SIS proposé et le projet de cycle de vie du processus, comprenant l'identification des cases de la Figure 7 de l'IEC 61511-1:2016qui s'appliquent au projet. Ce faisant, il convient de prendre en compte toutes les informations nécessaires pour commencer une activité de cycle de vie de sécurité du SIS, ainsi que les personnes susceptibles de pouvoir les fournir, afin de pouvoir attribuer les responsabilités du cycle de vie de sécurité aux personnes concernées. Dans certains cas, il peut ne pas être possible de déterminer des informations précises sur un point particulier jusqu'à une étape avancée dans la phase de conception. Dans ce cas, il peut être nécessaire de faire une estimation basée sur une expérience précédente et ensuite de confirmer les données à une date ultérieure. Lorsque c'est le cas, il est important de le noter dans le cycle de vie de sécurité SIS.

A.6.2.3 Une autre partie importante de la planification du cycle de vie de sécurité du SIS consiste à identifier les techniques qui seront utilisées au cours de chaque phase. L'identification de ces techniques est importante, car il est souvent nécessaire d'utiliser une

technique particulière, qui exige le recours à des personnes ou des services/départements ayant des compétences et des expériences particulières. Par exemple, les conséquences dans une application particulière peuvent dépendre de la pression maximale développée à la suite d'un cas de défaillance; la seule manière qui peut déterminer cela est de développer un modèle dynamique du processus. Les exigences relatives aux informations concernant la modélisation dynamique auront alors un impact important sur le processus de conception.

A.6.2.4 Comme la conception détaillée, la vérification, la validation et la preuve d'essai ont été développées depuis d'autres phases du cycle de vie de sécurité, il est important de confirmer, après chaque changement, que chacune des phases du cycle de vie de sécurité reste cohérente, qu'aucun nouveau danger n'a été introduit et que l'application s'exécute toujours comme exigé.

A.6.3 Lignes directrices des "exigences relatives aux cycles de vie de sécurité du SIS du programme d'application"

A.6.3.1 Le cycle de vie de sécurité du SIS du programme d'application démarre à la phase 3 du cycle de vie de sécurité du SIS ("Spécification des exigences de sécurité du SIS") et se termine à l'étape 3 FSA.

A condition que le cycle de vie de sécurité du programme d'application satisfasse aux exigences du Tableau 3 de l'IEC 61511-1:2016 , il est acceptable d'adapter la profondeur, le nombre et la quantité de travail des phases du modèle en V (voir la Figure A.1), afin de tenir compte de l'intégrité de sécurité et de la complexité du projet.

Le type de langage de programme d'application utilisé et la proximité du langage avec les fonctions d'application peuvent avoir un impact sur le domaine d'application des phases du modèle en V. Par exemple, lorsque des LVL conformes à l'IEC 61131-3:2013, le langage à contacts ou le diagramme de bloc fonctionnel est utilisé pour concevoir, mettre en œuvre, vérifier et valider le programme d'application, seuls deux niveaux de modèle en "V" de programme d'application normalisé peuvent s'appliquer:

- le "développement du module d'application" dans le modèle en "V" est interprété comme la conception et la mise en œuvre de la nouvelle fonction; et
- les "essais du module d'application" sont interprétés comme la vérification et les essais de la nouvelle fonction.

Si une nouvelle fonction doit être écrite dans un FVL et qu'un processus de développement de programme d'application (c'est-à-dire, un code logiciel) plus détaillé est donc nécessaire, il convient que le développeur suive toutes les phases du cycle de vie et toutes les procédures définies dans l'IEC 61508-3:2010. Le SRS du programme d'application peut être inclus dans le SRS du SIS.

A.6.3.2 Il convient que le choix des méthodes et des techniques dépende de circonstances spécifiques. Les facteurs intervenant dans cette décision sont susceptibles d'inclure:

- la taille du programme d'application;
- le degré de complexité;
- le SIL de la SIF à mettre en œuvre;
- le degré de normalisation des outils de conception (par exemple outil de configuration);
- le type de langage d'application (par exemple bloc fonctionnel à l'Annexe B; diagramme de cause à effet à la Figure D.2 et au Tableau F.14; relais à la Figure F.11).

Voir des exemples de techniques et de mesures en A.12.6.2.

A.6.3.3 Aucune autre ligne directrice n'est fournie.

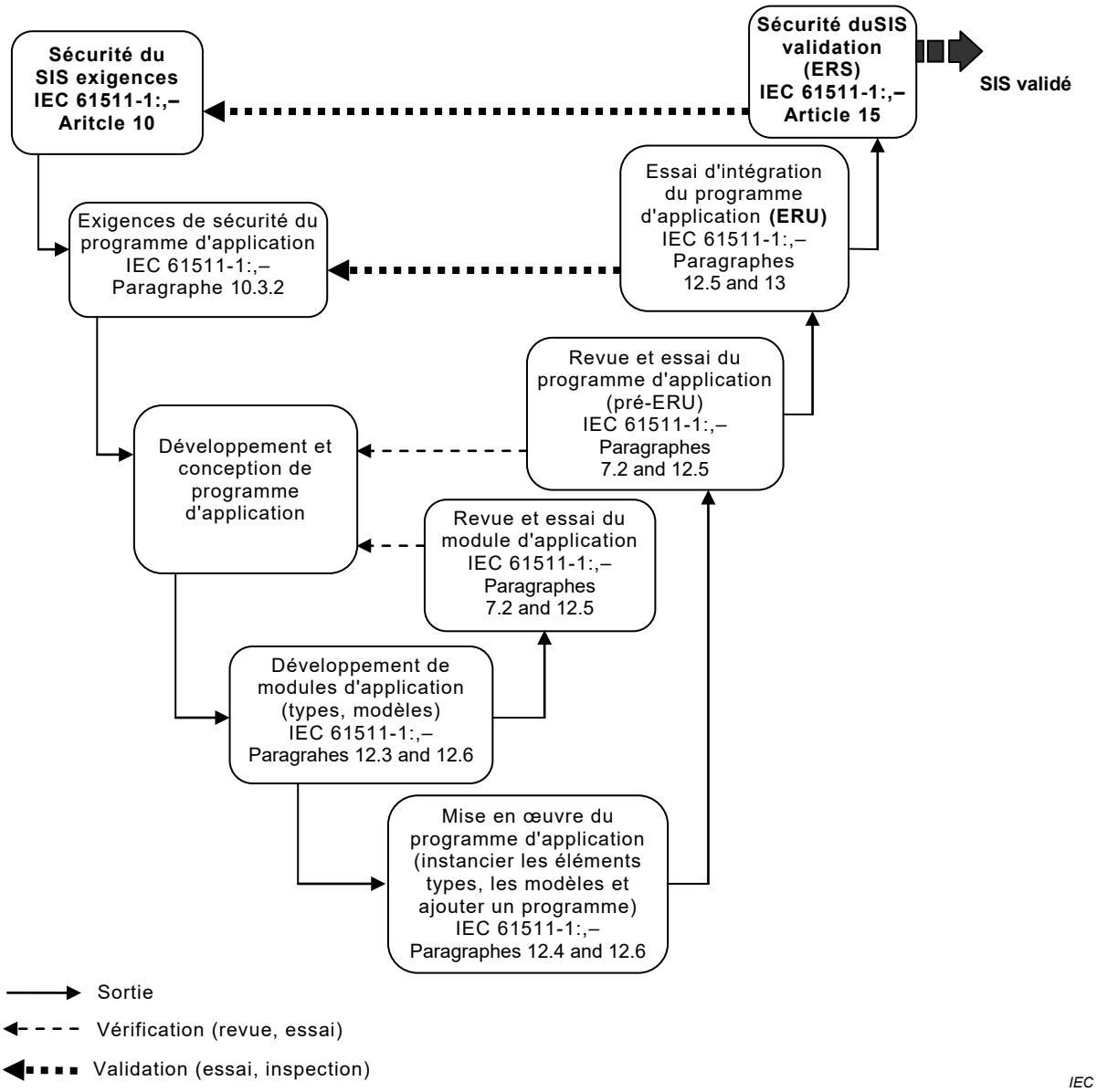


Figure A.1 – Modèle en V du programme d'application

A.7 Vérification

A.7.1 Objectif

Le but de la vérification est de s'assurer que les activités, pour chaque phase du cycle de vie de sécurité du SIS, conformément au plan de vérification, ont bien été réalisées et que les sorties exigées de la phase, qu'elles soient ou non sous forme de documentation, de matériel ou de programme d'application, ont été générées et conviennent aux besoins de livrables de phase.

A.7.2 Lignes directrices relatives aux "Exigences"

A.7.2.1 L'IEC 61511-1:2016admet que les organismes disposeront de leurs propres procédures de vérification et n'exigent pas toujours d'eux qu'elles soient toujours effectuées de la même manière. L'Article 7 de l'IEC 61511-1:2016a plutôt pour objet de faire en sorte que toutes les activités de vérification soient planifiées à l'avance, avec toutes les procédures, les mesures et les techniques qui doivent être utilisées.

A.7.2.2 Afin de révéler et d'éliminer les erreurs qui existent déjà dans le programme d'application, une vérification est exigée tout au long du cycle de vie du développement. En général, afin d'assurer l'aptitude aux essais, il est recommandé d'examiner les spécifications d'essai d'intégration du programme d'application pendant la phase de conception et de développement. Le domaine d'application des essais peut prendre en compte les essais préalablement réalisés.

A chaque phase distincte du cycle de développement du programme d'application (y compris les essais), il convient que la vérification confirme que la phase a abouti. En général, la vérification est accomplie par une équipe de vérification qui se compose d'une ou de plusieurs personnes, en fonction des besoins de l'application.

Pour réduire des erreurs dues aux idées préconçues, il convient que la vérification soit effectuée par une personne qualifiée, qui n'est pas impliquée dans la production du code d'application et, pour les applications SIL 3, par une personne avec un itinéraire de génération de rapport indépendant.

Si les outils de développement du programme d'application incluent certaines opérations de vérification automatiques (la vérification d'une double utilisation d'étiquettes (variables nommées), par exemple), il convient que l'équipe de vérification confirme que les outils ont été correctement utilisés et que des résultats corrects ont été obtenus.

Pour tous les SIL, il est recommandé que la couverture des essais englobe toutes les réponses des SIF du programme d'application et du SIS aux défaillances (défaillances de l'alimentation en énergie, défaillance du processeur, défaillance du matériel d'une entrée, défaillance du matériel d'une sortie et défaillances de communication, par exemple). Toutefois pour réduire encore davantage les erreurs restantes du programme d'application, il est recommandé d'effectuer les essais supplémentaires suivants:

- essai basé sur la structure interne (algorithmes internes, états internes, par exemple); et
- "essai de contrainte" (conditions de plage anormale des variables d'entrée et des variables internes, combinaisons anormales des entrées, séquences anormales et chargements anormaux, par exemple).

Pour tous les SIL, il est recommandé de faire en sorte que la documentation de vérification et d'essai montre que la vérification et les essais ont été effectués avec succès. Il est également recommandé que:

- la documentation permette d'évaluer l'adéquation de la vérification et de l'essai; et
- la documentation permette à une personne indépendante de répéter les essais et de passer en revue la couverture obtenue.

La vérification des données inclut la confirmation que les données utilisées dans le programme d'application sont correctes et uniques, le cas échéant (par exemple que les noms de balise sont affectés de manière unique, que les données ne sont pas mal utilisées par les fonctions suivantes et que les constantes, telles que des points de consigne d'alarme, sont valides et correctes).

La vérification de la protection contre un changement non autorisé pourrait inclure la vérification que les mécanismes existent bien (par exemple, protection par mot de passe avec des niveaux d'accès) et que ces mécanismes ont été utilisés de manière adéquate.

Un système de processus peut avoir un ou plusieurs systèmes intégrés conforme(s) à différentes normes (l'IEC 62061:2005 pour les machines ou la NFPA 85:2015 pour les brûleurs, par exemple). Une intégration soignée du matériel, du programme d'application et du logiciel intégré est exigée. Une façon de le faire consiste à traiter les systèmes non-processus (c'est-à-dire les systèmes qui doivent être conformes à d'autres normes, comme les machines, les brûleurs, etc.) comme des équipements de processus dans l'analyse de

danger et de risque, afin de garantir que tous les dangers possibles sont identifiés et que toute la protection supplémentaire identifiée soit fournie.

A.7.2.3 Aucune autre ligne directrice n'est fournie.

A.7.2.4 Aucune autre ligne directrice n'est fournie.

A.7.2.5 Lorsque le programme d'application atteint les phases de vérification et d'essai du cycle de vie, toute modification ou tout changement apporté au programme d'application pourrait invalider les preuves développées à une phase précédente. Une approche peut être de répéter tout le cycle de vie depuis le début, mais cela coûte cher, génère des retards dans le programme et provoquerait presque systématiquement une grande quantité de travail inutile. Au lieu de cela, il convient qu'une analyse d'impact identifie les zones qui pourraient avoir été impactées et se focalise sur les efforts nécessaires pour garantir que ces zones soient revalidées.

A.7.2.6 Il est important que les résultats de la vérification soient disponibles, de manière à pouvoir démontrer qu'une véritable vérification a eu lieu à toutes les phases du cycle de vie de sécurité SIS.

A.8 Analyse de danger et de risque (H&RA)

A.8.1 Objectifs

L'objectif global consiste à établir la nécessité de disposer de fonctions de sécurité et du niveau objectif de défaillances afin de garantir la sécurité du processus. Les fonctions de sécurité sont attribuées aux couches de protection conformément à l'Article 9 de l'IEC 61511-1:2016 . Il est normal, dans le secteur des industries de transformation, de disposer de plusieurs couches de protection, de sorte que la défaillance d'une seule couche ne pourra pas avoir de conséquences préjudiciables ou ne pourra pas les permettre. Des couches de protection types sont représentées à la Figure 9 de l'IEC 61511-1:2016 .

A.8.2 Lignes directrices relatives aux "Exigences"

A.8.2.1 Les exigences en matière d'analyse de danger et de risque sont uniquement spécifiées en termes de résultats. Cela signifie qu'un organisme peut utiliser toute technique qu'il considère comme efficace, à condition qu'elle permette une description claire des fonctions de sécurité et du niveau objectif de défaillances associé.

Il convient qu'une analyse de danger et de risque identifie et tienne compte des événements dangereux qui pourraient se produire dans toutes les circonstances raisonnablement prévisibles (y compris les états d'anomalie et un mauvais usage raisonnablement prévisible). Il convient de prendre en considération les incidents passés, y compris les causes, les défaillances systèmes et les leçons tirées pour éviter toute nouvelle occurrence.

Sur un projet type du secteur des industries de transformation, il convient de procéder à une analyse de danger et de risque préliminaire, au début de la conception du processus de base. A cette étape, une hypothèse consiste à dire que les dangers ont été éliminés ou réduits autant que cela est raisonnablement réalisable, par l'application des principes de sécurité inhérents et par l'application des règles de l'art (cette activité de réduction de danger n'est pas dans le domaine d'application de l'IEC 61511). Pour le SIS, cette analyse préliminaire de danger et de risque est importante, l'établissement, la conception et la mise en œuvre d'un SIS étant des tâches complexes et pouvant prendre un temps considérable. Une autre raison d'entreprendre tôt ce travail est que les informations sur l'architecture du système seront nécessaires avant que les diagrammes du processus et de l'instrumentation ne soient finalisés.

En règle générale, les informations seront suffisantes pour permettre l'analyse préliminaire de danger et de risque après réalisation d'un schéma de procédé et mise à disposition de toutes les données du processus initial. Il convient de reconnaître que des événements dangereux supplémentaires peuvent être mis en évidence suite aux résultats de la conception détaillée. Une analyse finale de danger et de risque peut donc être nécessaire une fois que les schémas de tuyauterie et d'instrumentation ont été finalisés. Cette analyse finale utilise généralement une procédure formelle et entièrement documentée, telle que l'étude de danger et d'exploitabilité (HAZOP – voir l'IEC 61882:2003). Il convient qu'elle confirme que les couches de protection, telles qu'elles sont conçues, permettent de gérer les risques de l'installation. Lors de cette analyse finale, il doit être considéré si les défaillances des couches de protection (ou des activations réussies des couches de protection) introduisent de nouvelles demandes ou de nouveaux événements dangereux. Si de nouveaux événements dangereux sont révélés à cette étape, il peut être nécessaire de définir de nouvelles fonctions de sécurité. Une autre conclusion plus probable est que des causes supplémentaires sont identifiées, ce qui conduit à des événements dangereux qui ont déjà été identifiés à une étape préliminaire. Il sera alors nécessaire d'étudier si une révision quelconque des fonctions de sécurité et des exigences du niveau objectif de défaillances qui ont été déterminées dans l'analyse originale est nécessaire.

L'approche utilisée pour identifier les événements dangereux dépendra de l'application considérée. Pour certains processus simples, pour lesquels l'expérience en exploitation d'une conception normalisée est importante (les plates-formes pétrolières simples en mer, par exemple), il peut être suffisant d'utiliser les listes de contrôle développées par l'industrie (les listes de contrôle d'analyse de sécurité de l'ISO 10418:2003 et de l'API RP 14C:2001, par exemple). Si la conception est plus complexe ou si un nouveau processus est considéré, une approche plus rigoureuse peut être nécessaire (par exemple ISO 31000:2009).

NOTE De plus amples informations relatives au choix des techniques appropriées sont données dans l'ISO 17776:2000, "Industries du pétrole et du gaz naturel – Installations des plates-formes en mer – Lignes directrices relatives aux outils et techniques pour l'identification et l'évaluation des risques".

Lorsque les conséquences d'un événement dangereux particulier sont envisagées, il convient de considérer tous les résultats possibles et de distribuer la fréquence de l'événement dangereux de manière adéquate parmi les résultats possibles. Il convient d'ignorer ou de mettre de côté toute sortie non crédible. Par exemple, le fait de soumettre des conduits ou des réservoirs à des pressions supérieures à celles pour lesquelles ils ont été conçus n'aura pas toujours comme conséquence une perte catastrophique du confinement. Dans de nombreux cas, les équipements auront été soumis à une pression d'essai supérieure à la pression pour laquelle ils ont été conçus et la seule conséquence peut être une fuite de substances inflammables, conduisant à une possibilité d'incendie. Lors de l'évaluation des conséquences, il convient que les personnes chargées de l'intégrité mécanique de l'installation soient consultées. Il convient de tenir compte de la pression d'essai d'origine, mais également du fait que la conception d'origine a inclus des surépaisseurs de corrosion ou non et qu'un programme de gestion de la corrosion est en place ou non. Dans le cas où les conséquences seraient fondées sur de telles hypothèses, il serait important que cela soit clairement énoncé, de sorte que des procédures appropriées puissent être incorporées au système de gestion de la sécurité.

Une autre question, lorsque les conséquences sont étudiées, sera le nombre de personnes susceptibles d'être menacées par un danger particulier. Dans bien des cas, le personnel opérationnel et de maintenance sera le seul présent dans la zone dangereuse, de manière peu fréquente. Ce fait peut être pris en considération lors de la prévision des conséquences. Il est nécessaire de faire attention lorsque cette approche statistique est utilisée, puisqu'elle ne sera pas valide dans tous les cas, comme dans celui où l'événement dangereux peut se produire pendant la mise en marche, alors que le personnel est souvent présent. En outre, il convient de prendre en considération l'augmentation potentielle du nombre de personnes se trouvant à proximité de l'événement dangereux pour étudier les symptômes pendant sa formation et jusqu'à l'événement lui-même.

Il convient d'évaluer les modes de fonctionnement du processus prévus, par exemple le démarrage, le fonctionnement continu, l'arrêt, la maintenance et les cycles de nettoyage. Il

convient que des sources raisonnablement prévisibles de sollicitation sur le SIS soient considérées, par exemple, défaillances d'équipement, système de commande, autres couches de protection, erreurs de maintenance, interventions manuelles (par exemple, fonction de commande BPCS en manuel) et perte d'alimentation (par exemple, d'air, d'eau de refroidissement, d'azote, de secteur, de vapeur, de moyen de chauffage, etc.) pendant chacun des modes de fonctionnement du processus prévus.

Lorsque la fréquence des sollicitations est étudiée, il peut être nécessaire, dans certains cas complexes, d'entreprendre une analyse par arbre des défaillances. Cela est souvent nécessaire lorsque des conséquences graves ne résultent que de la défaillance simultanée (ou plus tard masquée) de plusieurs événements (lorsque des collecteurs de décharge ne sont pas conçus pour le cas le plus défavorable, c'est-à-dire décharge de toutes les sources, par exemple). Il convient de porter un jugement à ce sujet, lorsque les erreurs de l'opérateur doivent être incluses comme des causes initiatrices des événements dangereux, ainsi que la fréquence à utiliser pour ces événements. Il est également nécessaire de faire attention lorsqu'une confiance est apportée à la réduction de la fréquence de sollicitation du fait de l'action de l'opérateur. Cette confiance est limitée par des considérations de facteurs humains, telles que la vitesse à laquelle la décision d'une action peut être prise et la complexité des tâches impliquées. Il convient que l'analyse de la fiabilité humaine soit effectuée quand un crédit >10 est revendiqué pour une action d'opérateur. Si une réduction de risque > 10 est revendiquée, il convient de concevoir le système conformément à l'IEC 61511-1:2016 . Le système qui exécute la fonction de sécurité comprendrait alors le capteur qui détecte la condition dangereuse, la présentation de l'alarme, la réponse humaine et l'équipement utilisé par l'opérateur pour mettre fin à une situation anormale. Il convient de noter qu'une réduction du risque ≤ 10 pourrait être revendiquée sans nécessairement être conforme à l'IEC 61511. Si ce type de revendication est formulé, il convient de veiller à tenir compte du facteur humain. Il convient que toutes les revendications relatives à la réduction de risque, suite à une couche de protection d'alarme, s'appuient sur une description documentée de la réponse nécessaire à l'alarme, sur la justification qu'un temps suffisant est laissé à l'opérateur pour engager l'action corrective et sur l'assurance que l'opérateur sera formé (au départ, puis de façon régulière) pour prendre des mesures préventives.

Un système d'alarme peut servir de moyen de réduction du risque, car il permet de réduire de taux de sollicitation sur le SIS, mais aussi de fonction de sécurité pour la couche de protection, car il permet de réduire le risque global du scénario. Il convient de prendre en considération la conception du système d'alarme:

- le capteur utilisé pour le système d'alarme et les éléments terminaux utilisés pour prendre des actions sur le processus ne sont pas utilisés pour les fonctions de commande pour lesquelles une perte de contrôle conduirait à une sollicitation sur le système d'alarme, à moins qu'une analyse n'ait eu lieu pour indiquer si le risque global est acceptable. Il convient d'aborder les questions de cause commune et de mode commun;
- le capteur utilisé pour le système d'alarme et les éléments terminaux utilisés pour prendre des actions sur le processus ne sont pas revendiqués pour la réduction de risque dans le cadre du SIS pour le même événement dangereux, sauf si la défaillance de cause commune a été prise en compte lors de l'analyse de la réduction du risque;
- des limitations ont été prises en compte par rapport à la réduction de risque pouvant être revendiquée pour la gestion et la conception du système d'alarme, par exemple des dispositions pour la sécurité de l'accès, la gestion des changements et des inspections, la maintenance préventive et les essais.

Des exemples de techniques qui peuvent être utilisées pour établir le SIL des SIS sont présentés dans l'IEC 61511-3:—, qui contient également des lignes directrices sur les éléments à prendre en compte au moment du choix de la méthode à utiliser pour une application particulière.

En établissant si la réduction de risque est exigée ou non, une certaine cible de sécurité pour le processus et une cible environnementale doivent être prises en considération. Celles-ci peuvent être spécifiques au site particulier ou à l'entreprise d'exploitation et seront comparées au niveau du risque sans fonction supplémentaire de sécurité. Après avoir établi

le besoin de réduction de risque, il faudra considérer quelles sont les fonctions qui doivent être exécutées pour que le processus revienne à un état de sécurité. En théorie, les fonctions peuvent être décrites d'une façon générale, sans référence à une technologie particulière. Dans le cas d'une protection de surpression par exemple, la fonction peut être décrite comme un moyen de prévention contre l'élévation de pression au-dessus d'une valeur spécifiée. Une soupape de sécurité ou un système instrumenté de sécurité (SIS) pourrait alors remplir cette fonction. Si la fonction est décrite comme ci-dessus, le choix du type de technologie à utiliser serait décidé lors de l'étape suivante du cycle de vie (affectation des SIF aux couches de protection). En pratique, les exigences fonctionnelles seraient différentes selon le type de système choisi; cette étape et la suivante peuvent dans certains cas être combinées.

En résumé, il convient que l'analyse de danger et de risque tienne compte de ce qui suit:

a) chaque événement dangereux déterminé et les séquences d'événements qui y contribuent;
b) les conséquences et la vraisemblance des séquences d'événements avec lesquelles chaque événement dangereux est associé; celles-ci peuvent être exprimées quantitativement ou qualitativement;
c) aucune autre ligne directrice n'est fournie;
d) la réduction de risque nécessaire pour chaque événement dangereux;
e) les mesures prises pour réduire ou éliminer les dangers et les risques;
f) les hypothèses faites pendant l'analyse de risque, y compris les taux estimés de sollicitation et les taux de défaillances des équipements; il convient de détailler toute prise en compte des contraintes opérationnelles ou des interventions humaines;
g) aucune autre ligne directrice n'est fournie;
h) les références aux informations importantes sur les systèmes relatifs à la sécurité, à chaque phase du cycle de vie du SIS (les activités de vérification et de validation, par exemple).

Il convient de documenter les informations et les résultats qui constituent l'analyse de danger et de risque.

Il peut être nécessaire de répéter l'analyse de danger et de risque à différentes étapes du cycle de vie global de sécurité du SIS, car des décisions sont prises et les informations disponibles deviennent plus précises. Il convient également de procéder à des revalidations périodiques de l'analyse de danger et de risque et de les documenter, afin de garantir que les hypothèses correspondent réellement à l'expérience pratique (voir 5.2.5.3 de l'IEC 61511-1:2016) et au plan de gestion de la sécurité fonctionnelle en cours (voir 5.2.5.1 de l'IEC 61511-1:2016).

A.8.2.2 Le BPCS inclut tous les appareils nécessaires pour exploiter le processus et son équipement associé de la manière souhaitée (voir l'IEC 61511-1:2016 , 3.2.3). En règle générale, les appareils BPCS ne sont pas qualifiés conformément à l'IEC 61511-1:2016(voir l'IEC 61511-1:2016 11.2.4). Par conséquent, par hypothèse, le taux de défaillances dangereuses ne peut pas être $< 10^{-5}$ par heure.

Dans le secteur des industries de transformation, une défaillance de BPCS est une cause importante de sollicitation qu'il convient de prendre en considération dans l'analyse de danger et de risque. Une défaillance du BPCS peut être causée par n'importe quel élément responsable d'un bon fonctionnement du BPCS, par exemple un capteur, une vanne, une erreur de l'opérateur ou le solveur logique.

L'IEC 61511-1:2016limite le taux de défaillances dangereuses pour le BPCS comme source initiatrice à 10^{-5} par heure, sauf si le BPCS est mis en œuvre selon les exigences de la présente norme. Cette limite s'explique par le fait le système de gestion de la sécurité fonctionnelle de l'IEC 61511-1:2016et ses mesures et techniques prescrites sont nécessaires pour réduire la probabilité de défaillances systématiques à un niveau suffisamment faible pour

prendre en charge une revendication de taux de défaillances dangereuses $< 10^{-5}$ par heure. La limite garantit que des niveaux élevés de confiance ne sont pas placés dans un BPCS qui ne satisfait pas aux exigences de l'IEC 61511-1:2016 .

A.8.2.3 Aucune autre ligne directrice n'est fournie.

A.8.2.4 Pour d'autres lignes directrices, voir l'ISA TR84.00.09:2013.

A.9 Affectation des fonctions de sécurité aux couches de protection

A.9.1 Objectif

Afin de déterminer la nécessité d'une SIF et de spécifier ses exigences d'intégrité de sécurité associée, il est important de considérer les couches de protection planifiées (ou installées), ainsi que la quantité de réduction du risque qu'elles apportent. Si une couche de protection pour le SIS est nécessaire, il convient de déterminer les SIL pour chaque SIF affectée au SIS.

A.9.2 Lignes directrices relatives aux "Exigences relatives au processus d'allocation"

A.9.2.1 L'exigence est d'identifier les couches de protection à utiliser, puis d'affecter la réduction du risque à la SIF. En pratique, les fonctions de sécurité ne sont affectées qu'aux SIS présentant des problèmes lorsqu'ils utilisent des conceptions à sécurité intrinsèque ou des systèmes avec d'autres technologies.

Des exemples de ces problèmes comprennent les limitations concernant la capacité de formation de torchères ou la protection contre des réactions exothermiques. Il convient que toute décision d'utiliser des systèmes instrumentés plutôt que des approches plus traditionnelles telles que des soupapes de sécurité soit justifiée par de bonnes raisons qui s'opposeront aux organismes de réglementation.

Comme indiqué ci-dessus, l'analyse de danger et de risque et l'affectation peuvent être des activités simultanées ou l'affectation peut, dans certaines circonstances, avoir lieu avant l'analyse de danger et de risque. Les décisions concernant l'affectation des fonctions de protection aux couches de sécurité sont souvent prises sur la base de ce qui s'est avéré réalisable par l'organisme de l'utilisateur. Il convient que la bonne pratique industrielle en la matière soit également prise en considération. Les décisions concernant les SIS seront alors prises, en prenant en compte les performances des autres couches de sécurité. Par exemple, dans le cas où des soupapes de sécurité auraient été installées et auraient été conçues et montées selon les bonnes pratiques industrielles, il peut alors être décidé qu'elles conviennent à elles seules, pour obtenir la réduction de risque ad hoc. Les SIS limiteraient alors uniquement la pression, si les dimensions ou les performances des soupapes de sécurité étaient insuffisantes pour l'application ou si le dégagement dans l'atmosphère doit être proscrit.

A.9.2.2 Aucune autre ligne directrice n'est fournie.

A.9.2.3 Lorsqu'une fonction de sécurité est affectée à un SIS, il sera nécessaire de se demander si l'application est en mode à faible sollicitation ou en mode à sollicitation élevée/en mode continu. Dans le secteur des industries de transformation, les fonctions de sécurité fonctionnent souvent en mode à faible sollicitation lorsque les sollicitations sont normalement peu fréquentes. Dans ces cas, le Tableau 4 de l'IEC 61511-1:2016donne les valeurs appropriées à utiliser. Un nombre croissant d'applications fonctionnent en mode à sollicitation élevée, lorsqu'il est plus approprié de considérer l'application en mode continu parce que les événements dangereux se produisent généralement dès que les SIS ne fonctionnent plus. Dans ces cas, le Tableau 5 de l'IEC 61511-1:2016donne les valeurs appropriées à appliquer. Les applications en mode continu, où la défaillance aurait comme conséquence un danger immédiat, sont rares. Les fonctions de commande de vitesse de la turbine ou du brûleur peuvent être spécifiées comme des applications en mode continu qui

doivent être conformes à l'IEC 61511-1:2016si la fréquence moyenne de défaillance exigée pour atteindre la fréquence d'événement dangereux spécifiée est inférieure à 10^{-5} par heure.

Le Tableau 4 de l'IEC 61511-1:2016définit le SIL en termes de PFD_{avg}. La PFD_{avg} cible est déterminée par la réduction de risque exigée. La réduction de risque exigée peut être déterminée via une comparaison du risque de processus sans SIS avec le risque tolérable. Cela peut être déterminé sur une base quantitative ou qualitative en utilisant les techniques de l'IEC 61511-3:—.

Le Tableau 5 de l'IEC 61511-1:2016définit le SIL en termes de fréquence moyenne de défaillances dangereuses pour exécuter la SIF. Cela est déterminé par le taux de défaillances tolérable du SIS, en tenant compte des conséquences de la défaillance dans une application particulière. Lorsque le Tableau 5 de l'IEC 61511-1:2016est utilisé pour déterminer le SIL exigé, la cible repose sur la fréquence de défaillance dangereuse pour le SIS. Lors de l'utilisation du Tableau 5 de l'IEC 61511-1:2016 , il est incorrect de convertir la fréquence de défaillance dangereuse en probabilité de défaillance dangereuse sur sollicitation en utilisant l'intervalle d'essais périodiques ou le taux de sollicitation. Alors que les unités peuvent sembler être correctes, il en résulte une conversion inappropriée du Tableau 5 de l'IEC 61511-1:2016 ,ce qui peut avoir comme conséquence une sous-spécification des exigences en matière de SIL.

Les cibles de probabilité moyenne de défaillance sur sollicitation ou de fréquence de défaillances dangereuses s'appliquent à la SIF et ne s'appliquent pas aux différents composants, appareils ou sous-ensembles SIS. Un composant, un appareil ou un sous-système SIS (par exemple, un capteur, un solveur logique, un élément terminal) ne peut pas avoir un SIL qui lui est affecté en dehors de son association avec une SIF spécifique. Un composant peut toutefois avoir une capabilité systématique relative aux mesures et aux techniques utilisées pour réduire la probabilité d'erreurs systématiques à l'origine d'une défaillance dangereuse du SIS.

Il convient que le résultat de l'analyse de danger et de risque et du processus d'affectation décrive clairement les fonctions de sécurité à exécuter sur les couches de protection. Pour les SIS, il convient que cette description inclue le mode de fonctionnement, c'est-à-dire en mode continu, à faible sollicitation ou à sollicitation élevée, ainsi que les exigences du SIL pour chaque SIF. Cela constitue la base de la SRS du SIS. Il convient que la description des fonctions de sécurité soit claire sur ce qu'il convient de faire pour garantir que les exigences d'intégrité de la sécurité et de sécurité fonctionnelle sont comprises.

A cette étape de la mise en œuvre, il est inutile de spécifier les détails architecturaux concernant les capteurs et les vannes. Les décisions relatives aux architectures sont complexes et définir si un système particulier nécessite ou non des capteurs 2oo3 et des vannes 1oo2 dépendra de nombreux facteurs.

A.9.2.4 Il convient que les implications du Tableau 4 et du Tableau 5 de l'IEC 61511-1:2016soient totalement comprises. En particulier, la PFD_{avg}, qui peut être revendiquée pour une SIF unique, est limitée à 10^{-5}, ce qui correspond à une réduction de risque de 10^5 (SIL 4). L'analyse de fiabilité peut indiquer qu'une PFD_{avg} peut être obtenue en raison de défaillances aléatoires du matériel de moins de 10^{-5}, mais l'IEC 61511-1:2016part du principe que les défaillances systématiques et les défaillances de mode commun limiteront la réduction de risque réel qui peut être obtenue. Dans le cas où l'analyse de risque montrerait qu'une aussi forte réduction de risque est nécessaire, il convient de noter – cela est même vivement recommandé – la difficulté de réaliser une SIF de SIL 4, dans le secteur des industries de transformation. Il convient de prendre en considération la suppression ou la réduction du danger à la source, l'introduction des mesures de réduction du risque non basée sur les SIS, la réduction de la probabilité des causes de l'événement dangereux ou l'utilisation de plusieurs SIF indépendantes, avec une intégrité de sécurité plus faible. Quand plusieurs SIF sont utilisées, il convient que les dépendances entre les SIF soient considérées, y compris les effets des essais périodiques synchronisés. Une façon de considérer l'effet consiste à modéliser la disposition globale par une approche holistique (voir l'IEC 61511-3:—, Annexe J).

A.9.2.5 Aucune autre ligne directrice n'est fournie.

A.9.2.6 Plusieurs SIF peuvent être utilisées pour atteindre des niveaux plus élevés de réduction de risque (supérieurs à 10^3, par exemple). Lors de l'utilisation de plusieurs SIF pour atteindre une réduction de risque plus élevée, il est important que chacune des SIF puisse indépendamment exécuter la fonction de sécurité et qu'il y ait une indépendance suffisante entre les SIS.

En outre, lorsque plusieurs SIF sont utilisées, il convient de tenir compte des défaillances de cause commune. De plus, il convient que toutes les autres exigences définies dans l'IEC 61511-1:2016soient satisfaites, y compris les exigences minimales de tolérance aux anomalies définies au Tableau 6 de l'IEC 61511-1:2016 .

L'exemple suivant présente la façon dont la combinaison de plusieurs SIF pourrait être utilisée pour atteindre des niveaux de réduction de risque plus élevés:

Un ensemble de transmetteurs 2oo3, un solveur logique 2oo3 et un ensemble d'éléments terminaux 1oo2 qui donnent une SIF avec un PFD_{avg} de $3{,}05 \times 10^{-4}$. Cette SIF permet d'obtenir une réduction du risque d'environ $3{,}3 \times 10^3$.

Il serait incorrect de prendre pour hypothèse qu'une utilisation conjointe de deux de ces systèmes donnerait une réduction de risque de 10×10^6 (c'est-à-dire, $3{,}3 \times 10^3 \times 3{,}3 \times 10^3$). Les facteurs de cause commune, tels que l'utilisation de technologies similaires, la conception des deux systèmes à partir de la même spécification fonctionnelle, les facteurs humains (par exemple, programmation, installation, maintenance), les facteurs externes (par exemple, la corrosion, les branchements, le gel sur les lignes aériennes, la foudre) et les dépendances dues aux essais périodiques synchronisés limiteront l'amélioration du système. Il est également nécessaire de tenir compte de tous les composants partagés entre les deux systèmes.

Une solution plus facilement réalisable peut consister à utiliser un deuxième système non redondant, en utilisant des appareils aussi divers que possible (afin de réduire au minimum les problèmes potentiels de cause commune). L'utilisation de différents composants peut toutefois rendre la maintenance plus difficile. Il convient de réaliser une analyse approfondie pour sélectionner la meilleure solution pour l'application individuelle.

Des lignes directrices supplémentaires sur la façon d'évaluer la dépendance et la cause commune entre les couches de protection sont fournies à l'Annexe J de l'IEC 61511-3:—.

A.9.2.7 Voir les lignes directrices sur la façon d'évaluer les dépendances et les effets de cause commune entre les couches de protection à l'Annexe J de l'IEC 61511-3:—.

A.9.2.8 Aucune autre ligne directrice n'est fournie.

A.9.2.9 Aucune autre ligne directrice n'est fournie.

A.9.3 Lignes directrices relatives aux "Exigences relatives au système de commande de processus de base en tant que couche de protection"

A.9.3.1 Le BPCS peut être identifié en tant que couche de protection suivant certaines conditions.

Les SIF peuvent ne pas être mises en œuvre dans le BPCS sauf si le BPCS a été conçu conformément à la norme. L'IEC 61511-1:2016 , 11.2.4 indique que "s'il est prévu de ne pas qualifier le BPCS par rapport à la présente norme, il convient que le SIS soit conçu pour être distinct et indépendant, de telle sorte que l'intégrité de sécurité du SIS ne soit compromise." La conception et la gestion du BPCS en tant que SIS exigent l'application des exigences du cycle de vie dans la norme, y compris l'analyse de danger et de risque, la documentation de

la conception, la gestion de la sécurité fonctionnelle, la validation et la gestion des changements.

La réduction du risque ne peut être affectée qu'à une couche de protection BPCS, sauf si les exigences de 9.3.4 et de 9.3.5 de l'IEC 61511-1:2016sont satisfaites et si une analyse quantitative du risque supplémentaire est conduite, conformément à l'IEC 61511-1:2016 . Cette analyse n'est pas essentielle et implique une évaluation détaillée de la conception globale du BPCS, y compris le matériel, le logiciel, les communications, l'alimentation électrique, les interfaces, etc. Il convient au minimum que cette analyse prenne en compte l'intégrité du matériel, la séparation des couches de protection pour éviter les défaillances de cause commune, la gestion des erreurs systématiques de programmation d'application, la sécurité de l'accès au matériel et au logiciel, la gestion des changements, l'interaction de l'opérateur, le contrôle de configuration et la validation périodique.

Si une couche de protection BPCS est considérée, il convient d'évaluer la conception et la gestion du BPCS afin de garantir que la probabilité de cause commune, de mode commun et de défaillance systématique entre la couche de protection BPCS et la source initiatrice, mais aussi entre la couche de protection BPCS et les autres couches de protection, soit suffisamment faible comparée aux exigences globales de réduction du risque pour le BPCS.

A.9.3.2 Une réduction du risque ≤ 10 peut être revendiquée à partir d'une couche de protection BPCS sans nécessairement être conforme à l'IEC 61511-1:2016 . Cela permet d'utiliser le BPCS pour certaines réductions de risque sans nécessairement mettre en œuvre les couches de protection du BPCS selon les exigences de l'IEC 61511-1:2016 .

Il convient que la revendication de réduction du risque ≤ 10 pour la couche de protection BPCS soit justifiée en tenant compte des capacités de réduction du risque du BPCS (déterminées par l'analyse de fiabilité ou les données d'utilisation préalable) et par les procédures utilisées pour la configuration, la modification, le fonctionnement et la maintenance.

Il convient de documenter toute couche de protection BPCS dans une spécification fonctionnelle, qui décrit de quelle façon le BPCS est conçu, maintenu, inspecté, soumis à essai et exploité afin d'arriver à la réduction du risque affectée.

Les défaillances associées à des appareils de la couche de protection BPCS peuvent être révélées via l'exploitation des processus, les diagnostics automatisés, les activités d'intégrité mécanique ou de lancement d'un autre événement dangereux, mais pas celui utilisé pour la réduction du risque. Il convient qu'en cas de détection d'une anomalie la couche de protection BPCS mette en œuvre une action spécifiée afin d'atteindre ou de maintenir un état de sécurité. L'action spécifiée (comportement sur détection d'anomalie) exigée pour obtenir ou maintenir un état de sécurité peut consister, par exemple, en l'arrêt de sécurité du processus (ou de la partie du processus qui repose sur le sous-système SIS présentant une défaillance pour la réduction du risque) ou sur une mesure compensatoire spécifiée qui garantit une exploitation sûre en attendant que la réparation soit terminée. Il convient que le comportement sur détection d'anomalie puisse prendre effet dans une durée inférieure au temps de sécurité du processus.

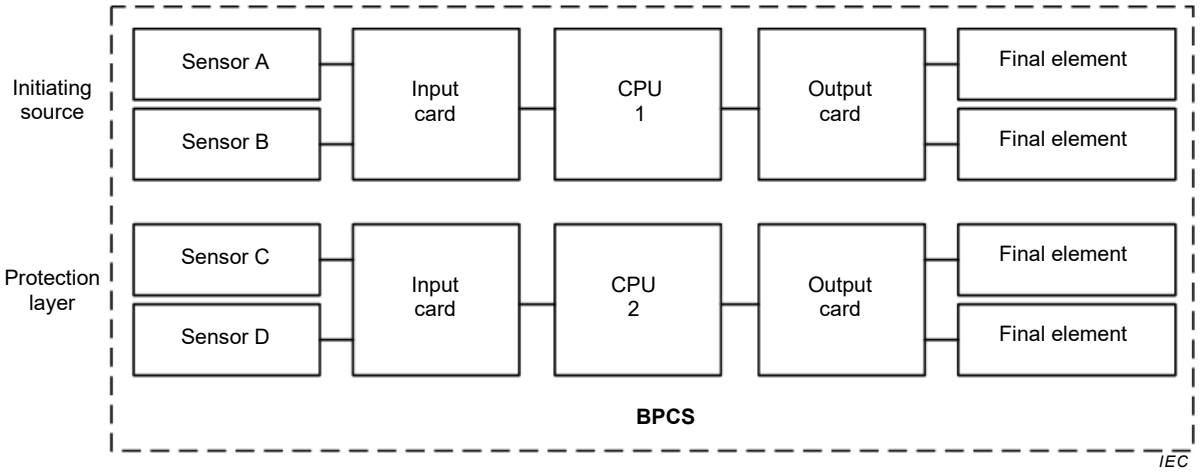
Lorsque la réduction de risque est affectée à une couche de protection BPCS, il est important de s'assurer qu'une sécurité d'accès et une gestion des changements sont fournies. Il convient d'utiliser des contrôles administratifs pour contrôler l'accès à la couche de protection et sa modification dans le BPCS. Il convient que la dérivation d'une couche de protection BPCS (par exemple, le passage de la fonction BPCS en manuel) exige une approbation et il convient de mettre en place des mesures compensatoires avant la dérivation afin de garantir le maintien de la réduction exigée du risque. Il convient de fournir des moyens pour valider la fonctionnalité de la couche de protection après des changements apportés au BPCS qui pourraient affecter l'exploitation de la couche de protection BPCS.

A.9.3.3 Aucune autre ligne directrice n'est fournie.

A.9.3.4 La réduction de risque qui peut être revendiquée pour une couche de protection BPCS est également contrainte par le degré d'indépendance entre la couche de protection BPCS, d'autres couches de protection et la source initiatrice de l'événement dangereux.

Il convient qu'une analyse détaillée du BPCS global démontre que les appareils de protection et de commande du BPCS sont suffisamment indépendants et séparés, de telle sorte qu'il peut être conclu qu'une défaillance du BPCS en tant que source initiatrice a une probabilité suffisamment faible de provoquer la défaillance de la couche de protection BPCS. Dans ces cas, il peut être approprié de prendre en compte une couche de protection BPCS, même si le BPCS peut lancer l'événement dangereux.

Si un BPCS est la source initiatrice, pas plus d'une couche de protection BPCS ne peut être revendiquée pour le même événement dangereux, sauf si le BPCS est conçu et géré conformément à l'IEC 61511-1:2016 . La Figure A.2 présente l'indépendance de la couche de protection BPCS et une cause initiatrice dans le BPCS.



Anglais	Français
Initiating source	Source initiatrice
Sensor	Capteur
Input card	Carte d'entrée
CPU	Unité centrale
Output card	Carte de sortie
Final element	Elément terminal
Protection layer	Couche de protection
BPCS	BPCS

Figure A.2 – Indépendance d'une couche de protection BPCS et d'une source initiatrice dans le BPCS

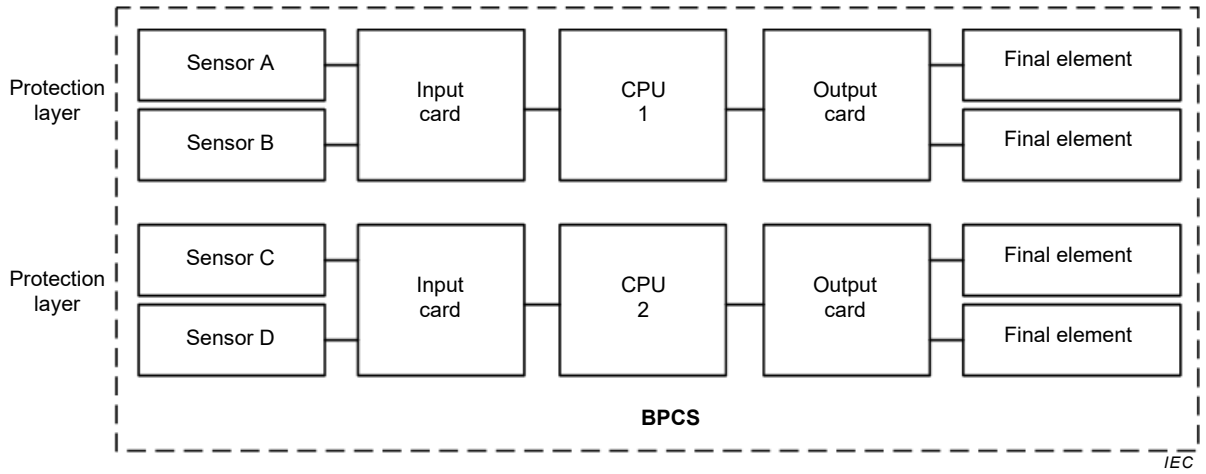
Par exemple, considérons le cas où une boucle de commande de débit est la source initiatrice. Cette source initiatrice inclut un transmetteur de débit, un solveur logique BPCS et une vanne de commande. Afin d'affecter la réduction de risque à un évent de pression du BPCS, il convient que le transmetteur de pression soit câblé à un solveur logique BPCS indépendant, modulant un élément terminal indépendant (par exemple, une vanne de mise à l'air libre d'une torchère). La couche de protection peut aussi être une fonction d'alarme et de réponse de l'opérateur.

En cas de revendications de BPCS comme source initiatrice et couche de protection pour le même événement dangereux, il convient que le BPCS global (y compris ses appareils,

comme représenté à la Figure A.2) soit conçu et géré de telle sorte qu'il supporte la fréquence de défaillance moyenne revendiquée ($\leq 10^{-5}$/h $\times \leq 10^{-1} = \leq 10^{-6}$/h, par exemple). Il convient que la revendication soit justifiée par une analyse quantitative du BPCS qui considère la probabilité de défaillances de cause commune et de mode commun entre les appareils qui composent le BPCS. Une cause commune due à des défaillances aléatoires et systématiques peut limiter la capacité du BPCS à atteindre la fréquence moyenne revendiquée de défaillance.

Si la source initiatrice n'est pas liée à la défaillance d'un BPCS, pas plus de deux couches de protection BPCS ne peuvent être revendiquées pour le même événement dangereux, sauf si le BPCS est conçu et géré conformément à l'IEC 61511-1:2016 . La Figure A.3 ci-dessous représente l'indépendance de deux couches de protection BPCS affectées au BPCS.

A.9.3.5 Si des revendications sont formulées pour deux couches de protection BPCS correspondant au même événement dangereux, il convient que le BPCS global (y compris les appareils, comme représenté à la Figure A.3) soit conçu et géré de manière à supporter la réduction du risque revendiquée ($\leq 1/10 \times \leq 1/10 = \leq 1/100$, par exemple). Les conditions et considérations de l'IEC 61511-1:20169.4.1 et 9.4.2 s'appliquent aux deux couches de protection BPCS. Il convient que la réduction du risque revendiquée soit justifiée par une analyse quantitative du BPCS qui considère la probabilité de défaillances de cause commune et de mode commun entre les appareils qui composent le BPCS. Une cause commune due à des défaillances aléatoires et systématiques peut limiter la capacité du BPCS à atteindre la réduction du risque revendiquée.



Anglais	Français
Protection Layer	Couche de protection
Sensor	Capteur
Input Card	Carte d'entrée
CPU	Unité centrale
Output Card	Carte de sortie
Final element	Elément terminal
BPCS	BPCS

Figure A.3 – Indépendance de deux couches de protection affectées au BPCS

A.9.4 Lignes directrices relatives aux "Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes"

A.9.4.1 Une question importante à considérer à une étape précoce est de savoir s'il existe ou non des défaillances de cause commune entre les parties redondantes de chaque couche

(entre 2 soupapes de sécurité de surpression sur le même réservoir, par exemple), entre couches de sécurité ou entre les couches de sécurité et le BPCS. Par exemple, lorsque la défaillance d'une mesure d'un BPCS pourrait provoquer une sollicitation sur le SIS et qu'un appareil, avec les mêmes caractéristiques, est utilisé dans le SIS. Dans de tels cas, il sera nécessaire d'établir s'il y a des modes de défaillance crédibles qui pourraient provoquer la défaillance des deux appareils en même temps. Si une cause de défaillance commune est identifiée, les actions suivantes peuvent être entreprises.

a) La cause commune peut être réduite en modifiant la conception du SIS ou du système de commande de processus de base. La diversité de la conception et la séparation physique sont deux méthodes efficaces pour réduire la probabilité des défaillances de cause commune. C'est habituellement l'approche préférentielle.

b) Il convient de prendre en considération la vraisemblance de l'événement de cause commune lors de la détermination du caractère adéquat ou non de la réduction de risque globale. Cela peut exiger une analyse par arbre des défaillances, qui inclut les causes de sollicitation, ainsi que les défaillances du système de protection. Les défaillances de cause commune peuvent être représentées sur ces arbres de défaillances, et leur effet sur le risque global peut être quantifié par des méthodes de modélisation appropriées.

Il convient de noter qu'il est très probable que tous les capteurs ou actionneurs partagés par le BPCS et le SIS introduisent des défaillances de cause commune.

A.9.4.2 Les considérations énumérées ci-dessous s'appliquent lorsqu'une évaluation est effectuée sur la probabilité de défaillances de cause commune, de défaillances de mode commun et de défaillances dépendantes. L'ampleur, la forme et la profondeur de l'évaluation dépendront du SIL de la fonction envisagée. L'effet des défaillances de cause commune, des défaillances de mode commun et des défaillances dépendantes peut être dominant pour SIL 3 ou SIL 4. Il convient d'étudier les points suivants:

- l'indépendance entre les couches de protection – il convient d'effectuer une analyse des modes de défaillance et de leurs effets pour établir si un événement unique peut provoquer la défaillance de plus d'une couche de protection ou la défaillance du BPCS et d'une couche de protection. La profondeur et la rigueur de l'analyse dépendront du risque;
- la diversité entre les couches de protection – il convient que le but soit la diversité entre les couches de protection et le BPCS, mais cela n'est pas toujours réalisable. Une certaine diversité peut être obtenue en utilisant des équipements de différents fabricants, mais si les capteurs du SIS et du BPCS sont connectés au processus en utilisant le même type de branchement, alors la diversité peut être de valeur limitée;
- la séparation physique entre les différentes couches de protection – la séparation physique réduira l'impact des défaillances de cause commune dues aux causes physiques. Il convient que les localisations des connexions de mesure pour le BPCS et le SIS soient données pour une séparation physique maximale, suivant les besoins fonctionnels, tels que précision et temps de réponse.

A.10 Spécification des exigences concernant la sécurité du SIS

A.10.1 Objectif

Le développement de la SRS du SIS est l'une des activités les plus importantes de tout le cycle de vie de sécurité. C'est par l'intermédiaire de cette spécification que l'utilisateur peut définir la manière dont il souhaite que chaque SIF soit conçue et intégrée dans un SIS.

Cette spécification constitue également le document de référence principal qui est utilisé pour la validation finale, montrant que toutes les exigences du SIS ont été satisfaites.

A.10.2 Lignes directrices relatives aux "Exigences générales"

La SRS du SIS peut être un document unique ou un ensemble de plusieurs documents comprenant des procédures, des schémas ou des normes/règlements internes à l'entreprise.

Ces exigences peuvent être développées par l'équipe d'analyse de danger et de risque et/ou par l'équipe de projet elle-même.

A.10.3 Lignes directrices relatives aux "Exigences de sécurité du SIS"

A.10.3.1 Comme cela est décrit dans l'IEC 61511-1:-, il convient de définir un certain nombre d'exigences de conception au début d'un projet pour s'assurer que la SIF apporte la protection désirée.

Certaines considérations se rapportant aux SRS sont les suivantes:

a) Les premiers éléments qu'il convient de définir sont la SIF et son SIL. Un exemple de SIF est "protéger le réacteur contre une surpression en fermant les vannes d'entrée sur la pression élevée". Généralement, la description de la fonction comportera les rubriques suivantes:

   - Les paramètres de processus qu'il convient de surveiller pour détecter les conditions dangereuses.

     EXEMPLE Une hausse de pression au-dessus d'une valeur spécifiée est détectée. La valeur du paramètre auquel une action est entreprise est en dehors de la plage d'exploitation normale et inférieure à la valeur qui aura comme conséquence la condition dangereuse. Une affectation est faite pour la réponse du système et pour la précision de la mesure. Lors de la définition de la limite, une discussion avec les responsables de la conception et de la mise en œuvre du SIS a eu lieu.

   - Les actions qu'il convient de prendre et le moment auquel il convient de les prendre afin d'éviter l'événement dangereux. Un exemple simple pourrait être de diminuer le débit de vapeur vers un rebouilleur en un temps spécifié. Il convient de noter qu'il n'est habituellement pas suffisant d'énoncer que le débit de vapeur vers le rebouilleur doit être interrompu. Le concepteur devra savoir ce qui est nécessaire pour obtenir une exploitation satisfaisante. Dans des services de chauffage, par exemple, il peut être suffisant de réduire le débit à moins de 10 % dans un délai d'une minute. Dans d'autres exemples, il peut être nécessaire d'avoir une fermeture étanche, en quelques secondes.

   - Les actions non nécessaires pour prévenir l'événement dangereux, qui peuvent être bénéfiques pour des raisons opérationnelles. Ces actions peuvent inclure la présentation des alarmes, l'arrêt d'unités en amont ou en aval pour réduire des sollicitations vis-à-vis d'autres systèmes de protection ou des actions qui permettront un démarrage rapide une fois que la cause du danger aura été éliminée. Il est important de séparer ces actions de non-sécurité des actions nécessaires pour prévenir la condition dangereuse, de manière à restreindre la frontière du SIS à ce qui est nécessaire.

   - Tous les états ou séquences du processus identifiés relatifs à l'exploitation du SIS, qu'il convient d'empêcher parce qu'ils auront comme conséquence des situations dangereuses. Il convient de faire une nouvelle analyse de risque après la conception du SIS pour considérer si des défaillances partielles ou si une exploitation parasite du SIS pourrait résulter dans un nouveau danger ou être une cause additionnelle d'un danger déjà identifié.

b) Il convient que cette spécification définisse l'état de sécurité du processus pour chaque fonction identifiée en termes de débits qui devraient être initiés ou arrêtés, de vannes du processus qui devraient être ouvertes ou fermées et d'état de fonctionnement de tous les équipements tournants (pompes, compresseurs, agitateurs). Si le fait d'amener le processus à un état de sécurité implique un séquencement, ce dernier peut également être identifié. En définissant les éléments terminaux, les avantages que procure la diversité peuvent être pris en compte, par exemple, en coupant le flux de produit et en arrêtant le débit de vapeur pour réduire la pression élevée.

c) Au début, l'exigence relative à un intervalle d'essais périodiques souhaité peut être définie, la conception du SIS pouvant ainsi le prendre en compte. Par exemple, si les essais périodiques doivent être exécutés pendant des arrêts planifiés (par exemple, tous les 3 ans), la conception pourrait exiger plus de redondance que si l'intervalle des essais périodiques doit être annuel.

   Les éléments suivants peuvent être pris en considération:

- la durée de l'essai;
- l'état de l'appareil soumis à l'essai (hors ligne/en ligne);
- l'état du processus pendant l'essai;
- la détection des défaillances de cause commune;
- la prévention des erreurs (par exemple, le SIS reste isolé une fois l'essai terminé);
- les exigences pour la documentation d'essai;
- l'archivage des exigences;
- le besoin de garantir que la direction est au courant de ce qui est planifié;
- le besoin de garantir que les zones adjacentes et que les autres zones impactées sont au courant de l'essai à venir;
- la qualification technique et l'expérience des personnes qui développent les procédures d'essai;
- la qualification technique et l'expérience des personnes qui mettent en œuvre les procédures d'essai.

d) Le temps de réponse maximal admis d'un SIS commence quand le processus est en condition de déclenchement; il se termine la dernière fois que les éléments terminaux atteignant leurs états de sécurité peuvent encore prévenir le danger. Il convient de définir les exigences pour pouvoir amener manuellement le processus à un état de sécurité. Par exemple, s'il y a une exigence pour que l'opérateur puisse manuellement arrêter un équipement à partir de la salle de commande ou d'un endroit sur le terrain, il convient alors de le spécifier. Il convient également que toute exigence relative à l'indépendance des commutateurs manuels d'arrêt à partir du solveur logique du SIS soit définie.

e) Il convient de spécifier toutes les exigences pour remettre en marche le processus après un arrêt. Par exemple, certains utilisateurs disposent d'interrupteurs électroniques de réarmement sur le panneau de commande principal ou sur le terrain, et d'autres préfèrent utiliser des solénoïdes avec des manettes de verrouillage. En présence d'une exigence spécifique, comme cette action de réarmement, il convient que cette exigence fasse partie de la SRS.

f) S'il existe une fréquence cible pour les déclenchements intempestifs, il convient qu'elle soit également définie par la SRS. Cela sera un facteur à prendre en compte dans la conception du SIS.

g) Il convient que les interfaces entre le SIS et l'opérateur soient totalement décrites, y compris les alarmes (alarmes préliminaires à l'arrêt, alarmes d'arrêt, alarmes de dérivation, alarmes des appareils de diagnostic), les graphiques, l'enregistrement des séquences d'événements.

h) Il peut être nécessaire d'avoir des dérivations pour permettre au SIS d'être soumis à l'essai ou maintenu, pendant que le processus fonctionne. En cas d'exigences spécifiques en matière de dérivation des appareils (un interrupteur à clé ou des mots de passe, par exemple), il convient également de les préciser dans la SRS.

i) Il convient de définir les modes de défaillance et la réponse du SIS en cas de détection d'anomalies. Par exemple, un transmetteur peut être configuré pour passer en défaillance en allant vers une condition de déclenchement ou en partant d'une condition de déclenchement. S'il est conçu pour passer en défaillance en partant de la condition de déclenchement, il est alors important que l'opérateur obtienne une alarme lors de la défaillance du transmetteur et qu'il soit formé pour entreprendre les actions correctives nécessaires. Voir également l'IEC 61511-1:2016 , 11.3, qui concerne les exigences relatives à la détection d'une anomalie.

A.10.3.2 Aucune autre ligne directrice n'est fournie.

A.10.3.3 Le présent paragraphe traite des lignes directrices de sécurité du programme d'application. Le SRS d'un programme d'application identifie les capacités minimales de la fonctionnalité du programme d'application PE et contient également les contraintes de

développement d'une fonctionnalité qui donnerait lieu à une condition non sûre. Les exigences de sécurité du programme d'application qui ont déjà été spécifiées dans les exigences relatives au SIS peuvent ne pas être répétées sous forme de SRS de programme d'application séparée.

En règle générale, la SRS du programme d'application prend en compte l'architecture système du SIS. L'architecture système définit les principaux appareils, les sous-systèmes SIS, le logiciel intégré et le programme d'application, ainsi que la manière dont ils sont interconnectés et dont les attributs exigés (en particulier l'intégrité de sécurité) sont obtenus. Des exemples de modules logiciels intégrés sont les systèmes d'exploitation, les bases de données et les sous-systèmes SIS. Les modules de programme d'application sont, par exemple, les fonctions d'application qui sont répliquées dans toute l'installation.

Il convient que l'architecture du programme d'application soit également déterminée par l'architecture sous-jacente du/des sous-système(s) SIS donnée par le/les fournisseur(s). Il convient que l'architecture du programme d'application ne gêne pas la redondance matérielle. Par exemple, si la redondance du processeur est plus faible (1 sur 1, par exemple) que la redondance du capteur (2 sur 3, par exemple), il convient que le programme d'application facilite le vote exigé des capteurs (c'est-à-dire, 2 sur 3).

Les exigences détaillées de sécurité fonctionnelle pour chaque SIF peuvent en général être définies au moyen de diagrammes logiques ou de schémas "de cause à effet" (voir la Figure D.2). Dans de nombreux cas, les langages de programmation livrés par le constructeur du solveur logique peuvent être utilisés pour définir les exigences. Les langages types qui peuvent être utilisés sont les diagrammes de bloc fonctionnel ou les matrices de cause à effet. Des formats spécialisés, par exemple Unified Modelling Language (UML), sont aussi disponibles et utiles quand l'utilisation de techniques de vérification du modèle est prévue. Il convient que le langage choisi livré par le constructeur satisfasse à l'application. L'utilisation des langages livrés par le constructeur pour définir les exigences détaillées peut souvent éviter les erreurs qui se produisent dans la traduction des exigences à partir d'autres formes de documentation. Il convient qu'une large utilisation des commentaires soit faite pour définir les fonctions de sécurité et de non-sécurité et les exigences du SIL de toutes les fonctions de sécurité.

Il peut être approprié de mettre en œuvre des exigences supplémentaires en plus de celles nécessaires pour le comportement fonctionnel de la SIF individuelle de base (par exemple, pour gérer l'arrêt et le démarrage de l'installation) dans le BPCS ou dans une partie totalement distincte du programme d'application de la SIF, avec des liens clairs vers la SIF. En outre, le programme d'application peut inclure des fonctions de mise en œuvre de l'architecture globale du SIS, des diagnostics de bout en bout et du comportement dans des conditions anormales. Par exemple, l'architecture des capteurs (principe de vote: 1oo2, 2oo3, etc.) associée à la SIF conjointement au principe de sécurité "désactiver pour déclencher" ou "activer pour déclencher" définit la façon dont il convient de réaliser le vote du capteur dans le programme d'application. Il est important de garantir qu'aucune combinaison des fonctions supplémentaires ne peut annuler les fonctions de sécurité de base de l'application.

Si plusieurs SIS sont utilisés pour mettre en œuvre des SIF, il convient que la documentation soit fournie pour expliquer quelles fonctions doivent être mises en œuvre dans chaque SIS. Si plusieurs SIS sont utilisés pour mettre en œuvre la même SIF (par exemple, pour combiner deux SIF de SIS de SIL inférieur pour réaliser un SIL plus élevé), il convient de documenter l'interaction et l'indépendance de chaque SIS. Il convient que cette documentation spécifie le SIL attendu, qu'il convient que chaque SIS atteigne. (Voir l'Article F.4, Architecture système et l'IEC 61511-3:—, Annexe J).

NOTE 1 La SRS d'un programme d'application identifie les capacités minimales de la fonctionnalité du programme d'application PE et les contraintes de développement d'une fonctionnalité qui donnerait lieu à une condition non sûre.

NOTE 2 Les exigences de sécurité du programme d'application qui ont déjà été spécifiées dans les exigences relatives au SIS peuvent ne pas être répétées.

NOTE 3 L'architecture système définit les principaux appareils et sous-systèmes SIS du logiciel intégré et du programme d'application, la manière dont ils sont interconnectés et dont les attributs exigés (en particulier l'intégrité de sécurité) sont obtenus.

NOTE 4 L'architecture du programme d'application peut également tenir compte de l'architecture sous-jacente du/des sous-système(s) SIS donnée par le/les fournisseur(s).—Il convient que l'architecture du programme d'application ne gêne pas la redondance matérielle. Par exemple, si la redondance du processeur est plus faible (1 sur 1, par exemple) que la redondance du capteur (2 sur 3, par exemple), il convient que le programme d'application facilite le vote exigé des capteurs (2 sur 3, par exemple).

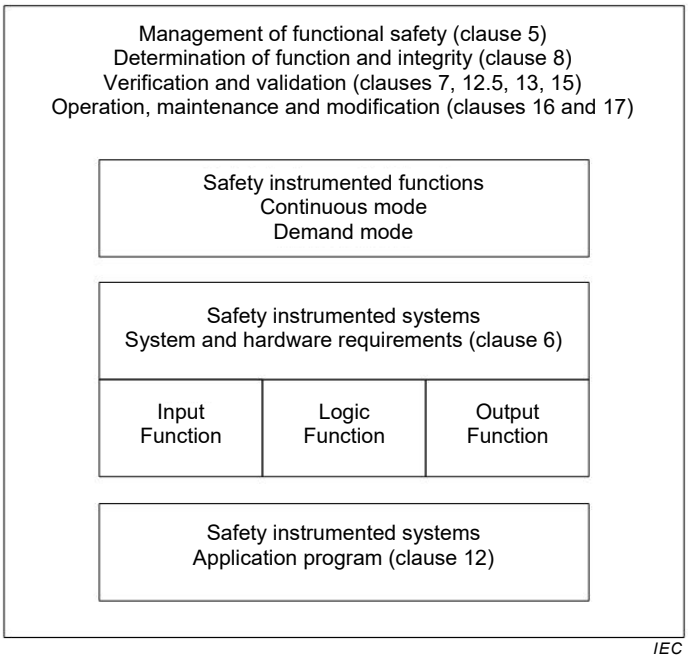
NOTE 5 En règle générale, un SIS est composé de trois sous-systèmes SIS architecturaux: des capteurs, un solveur logique et des éléments terminaux. En outre, les sous-systèmes SIS pourraient avoir des appareils redondants pour atteindre le niveau d'intégrité exigé.

NOTE 6 Une architecture matérielle de SIS avec des capteurs redondants peut imposer des exigences supplémentaires sur le solveur logique du SIS (mise en œuvre d'une logique 1oo2, par exemple).

Il convient de résoudre tous les conflits, toutes les divergences et toutes les omissions dans la SRS du SIS portés à la connaissance des concepteurs du programme d'application. Un exemple pourrait être l'effet de l'ordre d'exécution de la SIF dans le programme d'application. Un autre exemple serait la réponse du programme d'application en fonction des pannes d'alimentation.

NOTE 7 Les concepteurs du programme d'application peuvent passer en revue les informations contenues dans la spécification pour s'assurer que les exigences sont sans équivoque, cohérentes et compréhensibles. Tous les défauts détectés dans les exigences de sécurité spécifiées peuvent être spécifiés au concepteur du SIS.

NOTE 8 Au fur et à mesure que les exigences de sécurité du programme d'application et que l'architecture possible du programme d'application se précisent, il peut y avoir un impact sur l'architecture du matériel du SIS (voir la Figure A.4 ci-dessous). C'est la raison pour laquelle une étroite collaboration entre le développeur de l'architecture du SIS, le fournisseur de sous-système SIS et le développeur du programme d'application peut être essentielle.



Anglais	Français
Management of functional safety (clause 5)	Gestion de la sécurité fonctionnelle (Article 5)
Determination of function and integrity (clause 8)	Détermination de la fonction et de l'intégrité (Article 8)
Verification and validation (clauses 7, 12.5, 13, 15)	Vérification et validation (Article 7, Paragraphe 12.5, Article 13, Article 15)
Operation, maintenance and modification (clauses 16 and 17)	Fonctionnement, maintenance et modification (Articles 16 et 17)

Anglais	Français
Safety instrumented functions	Fonctions instrumentées de sécurité
Continuous mode	Mode continu
Demand mode	Mode sollicitation
Safety instrumented systems	Systèmes instrumentés de sécurité
System and hardware requirements (clause 6)	Exigences liées au système et au matériel (Article 6)
Input Function	Fonction d'entrée
Logic Function	Fonction logique
Output Function	Fonction de sortie
Safety instrumented systems	Systèmes instrumentés de sécurité
Application program (clause 12)	Programme d'application (Article 12)

Figure A.4 – Relations du système, du matériel du SIS et du programme d'application du SIS

Il convient que la SRS du programme d'application inclue toutes les fonctions nécessaires pendant tous les modes de fonctionnement du processus protégé, y compris les permissions de démarrage, le fonctionnement, l'arrêt et les essais périodiques de la SIF. Cela exige habituellement la définition des capacités de maintenance prioritaire; ainsi, les capteurs et les éléments terminaux peuvent être soumis à l'essai sans arrêter le processus. Les points à traiter comprennent:

a) les exigences de fonctionnalité et de relations temporelles qui sont nécessaires pour mettre en œuvre la SIF définie par l'utilisateur;

b) l'interface du système du programme d'application avec le processus et les personnes;

c) les relations entre les dangers liés au processus et la fonctionnalité fournie par le programme d'application;

d) les limites du comportement du programme d'application qui sont admises, afin de rester dans l'enveloppe de sécurité du processus (doit pouvoir traiter des conditions d'entrée incorrectes, par exemple);

e) la fonctionnalité admissible du logiciel utilitaire fourni au sein du solveur logique (hiérarchisation de la logique de sécurité et des E/S par rapport aux communications, gestion des erreurs et diagnostics du solveur logique, par exemple);

f) la plate-forme matérielle et le logiciel intégré sur lesquels le programme d'application exécute la configuration du matériel et du logiciel intégré;

g) les dangers qui pourraient survenir dans le processus en raison de la fonctionnalité du système dont le programme d'application fait partie (modes de défaillance inappropriés du matériel lors d'une coupure d'alimentation, par exemple);

h) les contraintes sur les méthodes et les procédures qui pourraient être utilisées par les concepteurs, découlant du manuel de sécurité pour le solveur logique de soutien;

i) les contrôles de vraisemblance et d'intégrité des données par exemple, contrôles de bout en bout des liaisons de communication, contrôles de limitation de zones adressables des entrées de capteur, contrôles de limitation de zones adressables des paramètres de données et exécution diverse des fonctions de l'application;

j) les critères de détection et la réponse aux pannes matérielles détectées du solveur logique et à l'intégrité des données en échec et aux vérifications de vraisemblance.

Afin d'éviter les difficultés aux stades ultérieurs du processus de développement, il est également important de considérer la stratégie par laquelle il est prévu de montrer que les exigences du programme d'application ont été satisfaites.

A.10.3.4 Dans le cas des appareils FPL (capteurs intelligents, transmetteurs intelligents, panneaux synoptiques IHM, par exemple), les exigences de configuration des appareils peuvent être spécifiées dans le cadre de la SRS.

A.10.3.5 L'Article B.1, l'Article F.17, l'Article F.20 et l'Article G.2 donnent des lignes directrices supplémentaires relatives à la mise en œuvre de l'IEC 61511-1:2016 10.3.2.3 et aux exigences de sécurité du programme d'application. Les lignes directrices supplémentaires fournies sont diverses en termes de portée du domaine d'application, de langage du programme d'application et d'application de processus, et de complexité, afin de dépeindre l'éventail des possibilités susceptibles de les satisfaire.

A.10.3.6 Pour un exemple de structure des exigences de sécurité du programme d'application, voir l'Annexe B.3.2.1 et l'Annexe F, Etape F.3.

A.11 Conception et ingénierie du SIS

A.11.1 Objectif

Le Paragraphe A.11.1 a pour objet de donner des lignes directrices relatives à la conception du SIS. Chaque SIF a son propre SIL. Un appareil d'un SIS, par exemple, un solveur logique, peut être utilisé par plusieurs SIF avec différents SIL.

A.11.2 Lignes directrices relatives aux "Exigences générales"

A.11.2.1 Aucune autre ligne directrice n'est fournie.

A.11.2.2 Pour les lignes directrices relatives au programme d'application, voir A.12.2.4. .

A.11.2.3 Si le programme d'application d'un SIS doit mettre en œuvre des fonctions instrumentées de sécurité (SIF) avec des SIL différents, il convient qu'elles soient clairement identifiées. Cela permet au programme d'application de chaque SIF de remonter au capteur adéquat et à la redondance de l'élément terminal. Cela permet également aux essais fonctionnels et de validation des fonctions d'être proportionnés au SIL. Il convient que la SIF et le SIL soient identifiés par des identifiants.

A.11.2.4 Les appareils du SIS sont parfois utilisés par le BPCS pour des raisons opérationnelles. L'IEC 61511–1:—, Article 11, donne un certain nombre d'exigences de conception pour un SIS. Un sujet de préoccupation est l'indépendance entre le SIS et le BPCS.

Le SIS est généralement distinct du BPCS pour les raisons suivantes:

a) Réduire les défaillances systématiques, de cause commune et de mode commun, ce qui réduit l'impact d'une défaillance du BPCS sur le SIS.

   NOTE 1 Un BPCS et un SIS séparés sont alignés avec le concept des couches de protection. Le SIS séparé est une couche de protection indépendante en cas de défaillance du BPCS.

b) Permettre de faire plus facilement des changements, assurer la maintenance, les essais et mettre à jour la documentation du BPCS.

   NOTE 2 Le SIS a généralement des exigences plus sévères que le BPCS, le but n'étant pas de soumettre le BPCS aux mêmes exigences sévères que celles qui sont exigées pour le SIS. Toutefois, des modifications non contrôlées du BPCS peuvent être la cause d'une augmentation des sollicitations sur le SIS.

   NOTE 3 La séparation du SIS et du BPCS permet de procéder à une maintenance séparée des différents systèmes, souvent par des équipes d'exploitation différentes.

   NOTE 4 L'accès aux fonctions de programmation ou de configuration du BPCS peut être limité pour satisfaire aux exigences de gestion des changements et de gestion de la configuration du SIS, si le BPCS est combiné avec le SIS.

   NOTE 5 Des moyens peuvent être prévus pour valider le SIS une fois les changements apportés aux appareils partagés entre le BPCS et le SIS.

c) Faciliter l'identification et la gestion des appareils du SIS, ce qui rend la validation et la FSA du SIS plus simples et plus claires.

d) Prendre en charge la sécurité de l'accès et améliorer la cybersécurité du SIS, de sorte que la révision des données ou des fonctions du BPCS n'ait aucun impact sur le SIS.

NOTE 6 Les interfaces et les appareils peuvent être partagés comme des appareils et des composants du SIS, sauf si la configuration matérielle et logicielle assure une séparation fonctionnelle.

NOTE 7 La restriction des écritures peut faire l'objet de considérations particulières afin d'éviter toute écriture non autorisée ou non souhaitée dans le SIS.

e) Réduire la quantité d'analyse qu'il convient d'avoir pour garantir que le SIS et que le BPCS sont correctement conçus, vérifiés et gérés.

NOTE 8 Si une défaillance des équipements communs peut entraîner une sollicitation sur le SIS, une analyse peut être réalisée pour s'assurer que la fréquence moyenne globale de défaillance est conforme aux prévisions. L'analyse peut couvrir tous les appareils du BPCS et du SIS (les capteurs, les solveurs logiques, les éléments terminaux, les communications de données, les sources d'alimentation, les stations opérateurs et les stations de travail ingénieurs, par exemple).

Si un appareil du BPCS est partagé avec le SIS, il convient de faire d'autres analyses pour démontrer que la conception et la gestion de l'appareil du BPCS:

- atteignent les exigences fonctionnelles de la fonction du BPCS et de la SIF;

  NOTE 9 La défaillance d'un matériel ou d'un logiciel en dehors du SIS ne peut pas empêcher d'exploiter correctement les SIF.

- satisfont aux exigences d'intégrité nécessaires pour atteindre la fréquence moyenne cible de défaillance pour le système combiné;

  NOTE 10 La défaillance d'un appareil BPCS ne peut pas être à l'origine de la cause initiatrice de l'événement dangereux ou de la défaillance dangereuse (ou mise en échec/dérivation) de la SIF qui protège contre l'événement spécifique en évaluation, à moins qu'un appareil redondant ne puisse activer le SIS. Une analyse peut être réalisée afin d'évaluer les effets du partage des appareils BPCS et SIS.

  NOTE 11 La probabilité de défaillances de mode commun, de cause commune ou dépendantes (les lignes de sortie branchées, l'activité de maintenance, y compris les dérivations, les vannes d'isolation de ligne mal exploitées, par exemple) peut être correctement évaluée et déterminée à un niveau suffisamment faible.

- sont gérées conformément à l'IEC 61511-1:2016 , y compris les essais périodiques, la sécurité de l'accès et la gestion des changements.

La séparation entre le SIS et le BPCS peut utiliser une séparation identique ou différente. Une séparation identique signifierait l'utilisation de la même technologie pour le BPCS et pour le SIS, tandis qu'une séparation différente signifierait l'utilisation de technologies différentes, issues d'un même fabricant ou de différents fabricants.

Comparée à la séparation identique, qui apporte une amélioration vis-à-vis des défaillances aléatoires, la séparation différente offre l'avantage supplémentaire de réduire la probabilité de défaillances systématiques qui affectent plusieurs canaux en même temps et/ou avec la même cause, ce qui réduit la défaillance corrélée de plusieurs canaux.

La séparation identique entre le SIS et le BPCS peut présenter certains avantages pour la conception et la maintenance, parce qu'elle réduit la vraisemblance des erreurs de maintenance. Cela est en particulier le cas si différents appareils doivent être choisis qui n'ont pas été utilisés auparavant au sein de l'organisation de l'utilisateur.

La séparation identique entre le SIS et le BPCS peut être acceptable pour des applications de SIL 1 et de SIL 2, bien qu'il convienne de vérifier les sources et les effets des défaillances de cause commune et de réduire leur probabilité. Quelques exemples de défaillances de cause commune sont:

- le raccordement des connexions des instruments et des lignes de sortie d'impulsion;
- la corrosion et l'érosion;
- les pannes matérielles dues à des causes environnementales;
- les erreurs logicielles;
- les alimentations en énergie et les sources de puissance;

  NOTE 12 L'alimentation (l'alimentation électrique, par exemple) peut être analysée par des méthodes de fiabilité conventionnelles. L'utilisation d'un facteur bêta n'est pas appropriée dans ce cas.

- les erreurs humaines.

Il y a quatre zones où la séparation entre le SIS et le BPCS est généralement octroyée:

- capteurs de terrain;
- éléments terminaux;
- solveur logique;
- câblage.

La séparation physique entre le BPCS et le SIS peut ne pas être nécessairement assurée si l'indépendance est maintenue et si les configurations des équipements et les procédures appliquées assurent que le SIS ne sera pas dangereusement affecté par:

- les défaillances du BPCS; et
- les travaux réalisés sur le BPCS, par exemple, maintenance, exploitation ou modification.

Dans le cas où des procédures sont nécessaires pour s'assurer que le SIS n'est pas dangereusement affecté, il convient que le concepteur du SIS indique les procédures à appliquer.

a) Capteurs de terrain

L'utilisation d'un capteur unique pour le BPCS et pour le SIS demande une revue et une analyse plus approfondies. Une revue et une analyse supplémentaires sont nécessaires, car une défaillance de cet unique capteur pourrait être à l'origine d'une situation dangereuse.

NOTE 13 Par exemple, un seul capteur de niveau utilisé tant pour le BPCS que pour le déclenchement à haut niveau du SIS pourrait créer une sollicitation en cas de défaillance du capteur au niveau faible (c'est-à-dire au-dessous du point de consigne du contrôleur de niveau). Du fait que le capteur se bloquerait au niveau faible, le contrôleur commanderait l'ouverture de la vanne. Puisque le même capteur est utilisé pour le SIS, il ne détectera pas l'état niveau haut résultant.

Si un seul capteur est utilisé tant pour le BPCS que pour une fonction du SIS, les exigences de l'IEC 61511-1:2016ne seront généralement satisfaites que si les diagnostics du capteur peuvent réduire suffisamment le taux de défaillances dangereuses et si le SIS est capable de placer le processus à l'un état de sécurité, dans le temps exigé.

Il convient que le capteur partagé (par exemple, le transmetteur, l'analyseur et le commutateur) soit alimenté par le SIS. Il convient également de prendre en considération les mesures compensatoires à mettre en œuvre pendant les périodes pendant lesquelles l'appareil partagé est hors service à cause d'anomalies détectées, de maintenance ou d'essais. Pour les SIL plus élevés, des capteurs séparés de SIS avec des redondances identiques ou différentes seront normalement nécessaires pour satisfaire à l'intégrité de sécurité exigée.

Quand un seul capteur de SIS est utilisé, il peut y avoir des avantages à répéter le signal au BPCS via des isolateurs adaptés ou d'autres moyens qui garantissent qu'aucune défaillance du BPCS ne provoque une défaillance dangereuse du SIS. Cette configuration peut conduire à améliorer la couverture du diagnostic, en permettant une comparaison de signal entre les capteurs du BPCS et du SIS.

Quand des capteurs de SIS redondants sont utilisés, les capteurs peuvent également être connectés au BPCS via des isolateurs adaptés ou d'autres moyens qui garantissent qu'aucune défaillance du BPCS ne provoque une défaillance dangereuse du SIS. Des algorithmes appropriés au sein du BPCS, tels que la "moyenne de trois", peuvent augmenter la sécurité en réduisant le taux de sollicitation sur le SIS.

Pour une SIF de SIL 2, de SIL 3 ou de SIL 4, des capteurs SIS séparés avec une redondance identique ou différente seront généralement nécessaires pour satisfaire aux exigences de tolérance aux défauts du matériel et à l'intégrité de sécurité exigée.

b) Elément terminal

Comme pour les capteurs, l'utilisation d'un seul élément terminal pour le BPCS et pour le SIS exige plus de revue et d'analyse, car la défaillance de l'élément terminal unique pourrait être à l'origine d'une situation dangereuse.

NOTE 14 Par exemple, l'utilisation d'une seule vanne pour le SIS et pour le BPCS peut créer une sollicitation en cas de défaillance de la vanne en position ouverte, et une défaillance dangereuse du SIS si la vanne ne se ferme pas comme spécifié lorsque la sollicitation se produit.

Si un seul élément terminal est utilisé tant pour le BPCS que pour le SIS, les exigences de l'IEC 61511-1:2016ne seront généralement satisfaites que si les diagnostics de l'élément terminal peuvent réduire suffisamment le taux de défaillances dangereuses et si le SIS est capable de placer le processus à l'état de sécurité dans le temps exigé.

Cela est, en pratique, difficile à obtenir pour les applications SIL 1 même lorsque la conception de l'élément terminal partagé garantit que l'action du SIS remplace l'action du BPCS. Il convient également de prendre en considération les mesures compensatoires à mettre en œuvre pendant les périodes pendant lesquelles l'appareil partagé est hors service à cause d'anomalies détectées, de maintenance ou d'essais. Pour une SIF SIL 2, SIL 3 ou SIL 4, des éléments terminaux SIS séparés avec une redondance identique ou différente seront généralement nécessaires pour satisfaire à l'intégrité de sécurité exigée. L'action du SIS qui remplace le BPCS peut, par exemple, être obtenue pour une vanne pneumatique par une connexion directe du SIS à une électrovanne qui vidange l'air de l'actionneur situé par exemple entre le positionneur de vanne et l'actionneur. Pour les électrovannes, le câblage peut permettre au SIS de placer et de maintenir la vanne de commande à l'état de sécurité jusqu'à son réarmement.

Lorsque des éléments terminaux redondants sont utilisés, les éléments terminaux peuvent être connectés au SIS et au BPCS. Même avec des éléments terminaux redondants, tenir compte des défaillances de cause commune entre le BPCS et le SIS. Le décalage des essais des vannes redondantes, à condition qu'une procédure adéquate soit mise en œuvre, peut réduire l'impact des défaillances de cause commune.

Quand l'élément terminal est une vanne, des considérations supplémentaires interviennent:

- La vanne est conçue de telle sorte qu'aucune défaillance du BPCS ne pourrait empêcher le SIS de pouvoir entrer en action avec la vanne partagée.
- La conception de la vanne est fonctionnellement compatible avec le service du SIS et du BPCS.

NOTE 15 Cela peut être difficile, de nombreuses vannes du BPCS étant installées pour du "fluide tendant à ouvrir" et de nombreuses vannes du SIS étant installées pour du "fluide tendant à fermer". Les exigences d'alimentation de l'actionneur pour une vanne du SIS peuvent être différentes de celles d'une vanne de commande.

- Les exigences de fermeture.

NOTE 16 Le taux de fuite du processus par la vanne de commande peut être tolérable quand il n'affecte pas la capacité de la SIF à exécuter la fonction spécifiée et à éviter le danger.

- Il convient que la conception de l'élément terminal partagé garantisse que l'action SIS passe outre l'action BPCS.
- L'expérience de fiabilité avec la vanne dans les applications de processus similaires.
- Les modes de défaillance hors sécurité de la vanne.
- Les procédures d'exploitation pour garantir l'intégrité du SIS.

NOTE 17 Par exemple, les vannes de dérivation peuvent être verrouillées en position fermée et faire l'objet de procédures de gestion et, de la même manière, les vannes situées dans les lignes de retour (hydrauliques, par exemple) d'une vanne à ressort de fermeture être verrouillées en position ouverte.

- Les exigences des essais périodiques.

NOTE 18 Les exigences des essais de course partielle ou des essais en ligne peuvent être prises en compte, mais également la façon dont cela peut affecter l'exploitation.

c) Solveur logique

La capacité à obtenir la séparation et l'indépendance avec les solveurs logiques du BPCS et du SIS varie en fonction de la technologie (c'est-à-dire, électrique, électronique et électronique programmable) utilisée dans l'application.

- Essais électriques

  De nombreux processus passés et certains processus existants utilisent des BPCS avec une technologie pneumatique et des SIS avec une technologie électrique. La

séparation et l'indépendance dans ce type d'application sont faciles à obtenir avec ces technologies, car elles exigent des enveloppes différentes, des dispositions physiques différentes et des communications par câblage direct.

- Electronique

  De nombreux processus passés et certains processus existants utilisent des BPCS avec une technologie électronique qui n'a aucune capacité d'électronique programmable imbriquée et des SIS avec une technologie électrique. La séparation et l'indépendance dans ce type d'application sont faciles à obtenir avec ces technologies. L'utilisation de SIS électroniques dans technologie électronique programmable imbriquée est aussi une approche viable.

- Electronique programmable (PE)

  Certaines applications utilisent la technologie PE pour leur BPCS et la technologie électrique pour leur SIS. Ces configurations sont intrinsèquement distinctes et indépendantes; en effet, les communications sont câblées et directes et un arrangement physique intégré n'est pas avantageux.

  A l'heure actuelle, l'arrangement technique BPCS/SIS préférentiel dans le secteur des industries de transformation consiste à utiliser la technologie PE pour le BPCS et pour le SIS. Cette configuration offre une flexibilité maximale, grâce à sa capacité à modifier à distance les programmes d'application du BPCS et du SIS, mais également à échanger des informations entre le BPCS et le SIS. Malheureusement, ces caractéristiques peuvent être contre-productives en cas de tentative de maintien de la séparation et de l'indépendance du BPCS et du SIS, sauf si une analyse appropriée est réalisée au stade de la conception du cycle de vie de sécurité et si l'indépendance fonctionnelle est démontrée (à l'aide d'une autre technologie, par exemple).

  Il convient que la SRS (Article 10 de l'IEC 61511-1:2016) donne les lignes directrices sur la manière d'obtenir la séparation et l'indépendance avec cette disposition technologique de BPCS et de SIS. Cet effort a en outre reçu un appui supplémentaire de l'introduction de nouveaux outils qui fournissent plus de sécurité au BPCS et au SIS. Voir l'ISA TR84.00.09:2013 pour les configurations de système de commande BPCS/SIS pratiques et les outils de sécurité, qui offrent différents niveaux de séparation et d'indépendance entre le SIS et le BPCS.

  Certains fournisseurs logiques de PE proposent des contrôleurs avec le BPCS et le SIS dans la même enveloppe physique. Il convient que cette approche soit précédée d'une analyse attentive du manuel de sécurité des solveurs logiques et de la façon dont les exigences dont font l'objet le fonctionnement et la maintenance du BPCS et du SIS satisfont aux critères de gestion de la sécurité des processus des installations et la SRS.

d) Câblage

Sur les systèmes "activer pour déclencher", le BPCS et le câblage relatif aux appareils de terrain sont généralement séparés du câblage allant au SIS et à ses appareils de terrain concernés en raison de la possibilité de désactiver accidentellement la fonction de sécurité, sans avis préalable. Les lignes directrices types pour ces types de systèmes comprennent l'installation de câbles multiconducteurs séparés et de boîtes de jonction dédiées au SIS et au BPCS. Dans le cas où le câblage ne serait pas séparé, il est alors recommandé d'utiliser de bonnes procédures d'identification et de maintenance pour réduire au minimum les erreurs potentielles provoquées pendant la maintenance et ayant pour résultat la désactivation du SIS.

NOTE 19 L'activation pour le déclenchement concerne les circuits de la SIF pour lesquels les sorties et les appareils sont désactivés en exploitation normale. L'application de l'énergie (par exemple, électricité, air) entraîne une action de déclenchement.

Le système de support de câble (par exemple, chemins de câbles, conduits), peut être commun à la fois aux systèmes "désactiver pour déclencher" et "activer pour déclencher", sauf si la séparation est exigée pour d'autres raisons (par exemple, interférences électromagnétiques). Sur les systèmes "activer pour déclencher", il convient qu'une adjonction de protection contre l'incendie des chemins de câbles soit étudiée dans des zones à risque d'incendie.

A.11.2.5 Les opérateurs, le personnel de maintenance, les superviseurs et les directeurs ont tous des rôles à jouer dans l'exploitation sûre de l'installation. Cependant, l'homme peut faire des erreurs ou peut être incapable d'accomplir une tâche, tout comme les instruments et les équipements sont sujets à un dysfonctionnement ou à une défaillance.

Les performances humaines constituent donc un élément de conception du système et un facteur d'intégrité. L'interface homme-machine (IHM) est particulièrement importante lors de la communication de l'état du SIS au personnel d'exploitation et de maintenance.

L'analyse de fiabilité humaine (HRA) identifie les conditions qui font que des personnes commettent des erreurs et fournit des évaluations de taux d'erreurs en s'appuyant sur des statistiques antérieures et sur des études comportementales. Quelques exemples d'erreurs humaines contribuant au risque sécuritaire d'un processus chimique sont donnés ci-après:

- des erreurs non détectées à la conception;
- des erreurs en exploitation (par exemple, faux point de consigne);
- une maintenance incorrecte (remplacement d'une vanne par une autre au comportement inadapté en cas de défaillance, par exemple);
- des erreurs d'étalonnage, d'essai ou d'interprétation de sortie de systèmes de commande;
- la défaillance de réponse à une urgence.

NOTE Des lignes directrices supplémentaires peuvent être consultées dans les références suivantes:

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

A.11.2.6 Aucune autre ligne directrice n'est fournie.

A.11.2.7 L'IEC 61511-1:2016 porte sur les dangers qui peuvent être générés en cas de redémarrage automatique du processus par un SIS immédiatement après correction de la condition de déclenchement. Il convient que chaque SIF soit analysée pour déterminer comment il convient de le réinitialiser une fois que la condition de déclenchement a été corrigée. Généralement, il convient que le redémarrage ne soit possible qu'après une action manuelle de l'opérateur.

Un exemple de fonction qui assurerait le processus reste à l'état de sécurité après y avoir été placé est présenté à la Figure F.11 - feuille 4 - ligne 1 de la présente norme comme ligne directrice.

A.11.2.8 Des moyens manuels indépendants tant du solveur logique du SIS que du système de commande du BPCS peuvent être fournis pour permettre à l'opérateur de procéder à l'arrêt en cas d'urgence. Les moyens d'exploitation manuels de l'élément terminal du SIS peuvent être pris en compte pour satisfaire aux exigences d'intégrité de la fonction de sécurité, mais les facteurs humains adéquats et les défaillances de cause commune doivent être correctement considérés. Les exigences pour l'arrêt manuel sont habituellement définies dans la SRS.

Dans certains cas, l'arrêt manuel peut exposer l'installation à un risque supplémentaire (si une séquence d'arrêt est exigée, par exemple), auquel cas, l'arrêt manuel peut être une entrée pour que le SIS assure un arrêt échelonné.

L'arrêt d'urgence peut être connecté au solveur logique électronique programmable (PE) du SIS (par exemple, lorsqu'un arrêt en séquence est exigé) à condition qu'il soit nécessaire et considéré comme approprié par l'équipe de H&RA.

A.11.2.9 L'IEC 61511-1:2016 indique la nécessité d'analyser l'indépendance entre le SIS et les autres couches de protection, et pas simplement entre le SIS et le BPCS (voir l'IEC 61511-1:2016 , Figure 9).

Le décalage des essais périodiques entre le SIS et les couches de protection réduira la probabilité de défaillances simultanées.

Dans certaines circonstances, il peut être acceptable d'avoir une séparation partielle entre le BPCS et le SIS. Cela est en particulier le cas lorsqu'une défaillance des équipements communs ne provoquera pas de sollicitation sur le SIS. Dans ce cas, des équipements communs ou partagés doivent être mis en œuvre conformément à l'IEC 61511-1:2016 .

Quand le même type d'équipement est utilisé pour le BPCS et le SIS, si une défaillance de cause commune de l'équipement commun peut conduire à un événement dangereux qui provoque une sollicitation sur le SIS, il convient d'effectuer une analyse pour vérifier que la fréquence moyenne globale de défaillance satisfait aux attentes. Pour définir les dangers associés aux défaillances dangereuses des équipements communs.

L'IEC 61511-1:2016 indique également la nécessité de garantir que la conception de l'interface entre le SIS et d'autres systèmes maintient l'indépendance nécessaire, c'est-à-dire que le BPCS ne sape pas l'indépendance de non-sécurité conçue dans le SIS. Par exemple, si les données d'application générées pour être utilisées dans le BPCS ou d'autres outils appareils non SIS sont utilisées dans la conception du SIS, il y aurait un potentiel à propager un mode commun de défaillance entre les deux systèmes. Un autre exemple serait un programme d'application qui permettrait le remplacement du BPCS à mettre en œuvre dans le système sans un commutateur "permissif" séparé du BPCS. D'autres exemples viennent d'une "mise en miroir" quand les données d'application "fuient" dans un autre système et que le démarrage est neutralisé.

A.11.2.10 L'IEC 61511-1:2016 donne des lignes directrices en guise d'avertissement sur l'utilisation d'un appareil commun pour le BPCS et le SIS. Le terme "suffisamment bas" dans la note de 11.2.10 de l'IEC 61511-1:2016 signifie que le taux de défaillances dangereuses des équipements partagés, combiné à la probabilité de défaillance des autres couches de protection (autre que la SIF), satisfait aux critères de risque de l'entreprise.

A.11.2.11 Dans le cas des éléments terminaux qui, suite à la perte d'alimentation, ne conduisent pas à l'état de sécurité (systèmes "activer pour déclencher", par exemple), il convient d'attirer l'attention sur la mise à disposition de moyens manuels locaux pour obtenir l'état de sécurité.

A.11.2.12 Aucune autre ligne directrice n'est fournie.

A.11.2.13 Le manuel de sécurité a pour objet de documenter toutes les informations nécessaires relatives à la façon dont un appareil, un sous-système SIS ou un système peut être appliqué en toute sécurité.

NOTE 1 Le cas échéant, le manuel de sécurité, destiné à couvrir les informations du fabricant et de l'utilisateur final, peut être sectionné (entre matériel, logiciel et programme d'application, par exemple).

NOTE 2 Pour les éléments conformes à l'IEC 61508, l'entrée du fabricant est le manuel de sécurité selon les exigences de l'IEC 61508-2:2010, Annexe D.

Il convient que les manuels de sécurité incluent, sans s'y limiter, les informations suivantes:

a) Une description abrégée de l'élément et de sa topologie (schémas), y compris du matériel et du logiciel;

NOTE 3 Une réduction ou augmentation de la tolérance aux défauts du matériel conformément à l'IEC 61511-1:2016 11.4.4 peut être justifiée dans le manuel de sécurité.

b) L'identification de la révision et des contraintes liées au programme d'application;

NOTE 4 L'Article 12 de l'IEC 61511-1:2016 peut être passé en revue pour plus de détails sur les informations pertinentes relatives à la programmation d'application.

c) Identification de révisions matérielles et micrologicielles;

d) Description opérationnelle, y compris la définition de l'état de sécurité et des opérations de sécurité intrinsèque;

NOTE 5 Différents modes de fonctionnement peuvent être pris en compte, comme le démarrage, le fonctionnement normal, le fonctionnement dégradé et le mode de sollicitation.

e) La liste de toutes les hypothèses relatives au fonctionnement, à la maintenance et aux essais;

NOTE 6 Les hypothèses peuvent inclure les conditions d'utilisation, la maintenance préventive, la manière de procéder à des essais périodiques et le suivi des erreurs de diagnostic.

f) Une liste de toutes les limitations et restrictions relatives aux fonctions de sécurité de l'élément;

NOTE 7 Les limitations et restrictions concernent, sans s'y limiter, les paramètres de configuration, l'environnement et le processus.

g) Les modes de défaillance et les taux de défaillances correspondants du/des appareil(s);

NOTE 8 Les taux de défaillances peuvent provenir du fabricant ou de l'expérience pratique.

h) D'autres paramètres nécessaires pour les analyses de fiabilité (la durée de vie utile, les durées de réparation et, le cas échéant, les taux de défaillances de cause commune, par exemple);

i) La/les réponse(s) (ou comportement) aux anomalies détectées et aux avertissements;

j) Les instructions sur le fonctionnement et la maintenance du fabricant et, le cas échéant, les recommandations pour les intervalles d'essais périodiques;

k) Les mesures prises pour éviter et contrôler les défaillances systématiques, y compris les défaillances logicielles et, le cas échéant, les défaillances de cause commune;

l) Des informations sur la manière dont chaque mode de défaillance peut être révélé par un essai fonctionnel normal et par des diagnostics, y compris l'intervalle d'essai de diagnostic.

m) Il convient que le manuel de sécurité inclue les restrictions d'utilisation de l'appareil, avec des détails relatifs à sa configuration, ses interfaces, son installation, ses diagnostics, la durée moyenne de réparation, la réponse aux défaillances, l'intervalle d'essai et les contraintes de langage du programme d'application.

A.11.2.14 Aucune autre ligne directrice n'est fournie.

A.11.3 Lignes directrices pour les "Exigences relatives au comportement du système lors de la détection d'une anomalie"

A.11.3.1 Aucune autre ligne directrice n'est fournie.

A.11.3.2 Aucune autre ligne directrice n'est fournie.

A.11.4 Lignes directrices pour la "Tolérance aux défauts du matériel"

A.11.4.1 L'approche traditionnelle de la conception d'un système de sécurité consiste à s'assurer qu'aucune première défaillance n'aurait comme conséquence la perte de la fonction prévue. Les architectures de système telles que 1oo2 ou 2oo3 ont une tolérance aux anomalies de type 1, parce qu'elles peuvent fonctionner sur sollicitation, même en présence d'une défaillance dangereuse. Ces systèmes sont utilisés comme approche normalisée pour les systèmes de sécurité, afin de s'assurer qu'ils étaient suffisamment robustes pour pouvoir résister à des défaillances aléatoires du matériel. Les architectures tolérantes aux pannes assurent également une protection dans la plage de défaillances systématiques qui ne se produisent pas en même temps (surtout au niveau matériel).

L'IEC 61511-1:2016 admet que l'industrie de transformation a besoin de plusieurs niveaux de performances des systèmes de sécurité. A cet égard, elle a adopté le concept de niveaux d'intégrité de sécurité avec des performances croissantes, en fonction de la réduction du risque exigée pour l'événement dangereux considéré. Compte tenu des différents niveaux de performances, il n'est plus pertinent de prévoir la tolérance aux anomalies de tous les niveaux d'intégrité de sécurité. En choisissant l'architecture à utiliser pour un niveau spécifié d'intégrité, il est cependant important de s'assurer qu'elle est suffisamment robuste pour les défaillances aléatoires du matériel et les défaillances systématiques. Pour assurer la robustesse vis-à-vis des défaillances aléatoires du matériel, la présente norme demande qu'une analyse de fiabilité soit effectuée.

Les exigences de 11.4.1 of IEC 61511-1:2016 sont ciblées pour s'assurer que les architectures présentent la tolérance aux anomalies nécessaire, pour les défaillances aléatoires du matériel et certaines défaillances systématiques. En décidant de l'étendue de la tolérance aux anomalies nécessaire, il convient de prendre en compte un certain nombre de facteurs, indiqués ci-après:

a) la complexité des appareils utilisés au sein du sous-système SIS ou du SIS;

b) il sera moins probable qu'un appareil souffre de défaillances systématiques pendant le fonctionnement, si la nature de ses défaillances est comprise et prise en compte lors de la sélection de l'appareil, lors de l'installation et de la configuration de l'appareil, mais aussi lors de la définition de ses pratiques de fonctionnement et de maintenance;

c) les taux de défaillances issus de l'expérience de terrain;

d) l'exigence du niveau d'intégrité de sécurité pour l'application impliquée;

e) dans quelle mesure les défaillances conduisent à un état de sécurité ou peuvent être détectées par des diagnostics, de manière à ce qu'une action spécifiée puisse être prise;

f) les actions parasites dues à des défaillances en sécurité qui augmentent généralement quand la tolérance aux anomalies augmente et qui peuvent, à leur tour, créer un nouveau danger ou être une cause supplémentaire de danger existant ou peuvent devenir inacceptables par rapport à la fréquence de défaillance parasite cible;

g) les défaillances de cause commune et les défaillances systématiques qui peuvent dramatiquement réduire les avantages attendus de la tolérance aux anomalies;

h) la tolérance aux anomalies réellement atteinte qui peut être réduite à néant quand la restauration des défaillances dangereuses prend trop de temps (par exemple, un 2oo3 dont les défaillances ne sont pas corrigées en moins de 0,8 MTTF est pire qu'une architecture 1oo1);

i) la faisabilité de la redondance qui peut ne pas être pratique pour toutes les fonctions;

j) les différentes SIF dans lesquelles le SIS (ou ses sous-systèmes) intervient.

NOTE 1 Il peut être exigé que les sous-systèmes SIS fonctionnent dans le cadre d'une faible sollicitation ou d'une sollicitation élevée, en fonction du mode de fonctionnement. Une SIF peut être spécifiée pour fermer une vanne en réponse à des écarts de processus spécifiés. En cas de réarmement manuel ou automatique, le SIS peut maintenir la vanne à l'état de sécurité jusqu'à ce qu'il soit invité à faire autrement. Les exigences de tolérance aux défauts du matériel pour le fonctionnement du SIS en réponse à un événement dangereux peuvent être déterminées selon le mode à faible sollicitation, son fonctionnement en cours d'arrêt pouvant l'être selon le mode à sollicitation élevée.

NOTE 2 La tolérance minimale aux défauts du matériel a été définie pour limiter les éventuelles imperfections de la conception de la SIF, qui peuvent résulter du nombre d'hypothèses formulées lors de cette conception, ainsi que de l'incertitude quant au taux de défaillances des appareils utilisés dans diverses applications du processus.

A.11.4.2 Une bonne compréhension du concept de sous-système SIS (voir l'IEC 61511-1:2016 , 3.2.78) est nécessaire pour appliquer les exigences de tolérance aux défauts du matériel.

Les exigences de tolérance aux défauts du matériel s'appliquent à l'ensemble du SIS ou aux sous-systèmes SIS exigés pour exécuter une SIF, pas à des appareils individuels au sein d'un sous-système. Par exemple, dans le cas d'un sous-système SIS de capteurs comprenant un certain nombre de capteurs redondants, l'exigence de tolérance aux anomalies s'applique au sous-système SIS de capteurs dans son ensemble et non pas aux capteurs individuels.

A.11.4.3 L'IEC 61508 considérait les facteurs décrits en 11.4.1 ci-dessus et spécifiait l'étendue de la tolérance aux anomalies exigée dans l'IEC 61508-2:2010 par l'utilisation de deux itinéraires différents appelés 1_H et 2_H. En préparant cette norme sectorielle pour le secteur des industries de transformation, il a été considéré que l'itinéraire 2_H lui était le mieux adapté. Par conséquent, les exigences de tolérance aux anomalies de l'IEC 61511-1: — s'appuient sur l'itinéraire 2_H de l'IEC 61508-2:2010. L'itinéraire 1_H de l'IEC 61508-2:2010 pourrait être appliqué en alternative. Il convient de noter les conceptions de sous-systèmes SIS peuvent exiger plus de redondance d'appareil que ce qui est indiqué dans l'IEC 61511-1:2016 Tableau 6, afin de satisfaire aux exigences de disponibilité du processus (cible de fréquence de défaillance parasite, par exemple).

Il convient qu'une évaluation de l'itinéraire 1_H prenne en compte l'environnement d'exploitation prévu pour assurer la conformité à l'IEC 61511. Pour les appareils de terrain, l'environnement d'exploitation a souvent un impact significatif sur le taux de défaillances démontré, ce qui peut également avoir un effet sur la distribution des défaillances en sécurité et dangereuses.

A.11.4.4 La tolérance aux anomalies peut être assurée par des appareils redondants non identiques (en cas de mise en œuvre d'une redondance diversifiée, par exemple). La tolérance aux défauts du matériel d'un SIS est en fait donnée par la combinaison la plus courte de défaillances indépendantes de l'appareil qui conduisent à une défaillance dangereuse de ce SIS. Si le SIS a été divisé en sous-systèmes SIS indépendants, sa tolérance aux défauts du matériel est égale à la valeur minimale de la tolérance aux défauts du matériel de ses sous-systèmes SIS.

Les exigences de tolérance aux défauts du matériel peuvent être assouplies quand le SIS est réparé en ligne. Il convient toutefois que les paramètres clés relatifs à un assouplissement aient d'abord été évalués (par exemple, MTTR ou durée d'essai par rapport à la probabilité d'une sollicitation lors de la réparation ou des essais). Cela doit être inclus dans le calcul des mesures de probabilité (PFD_{avg}, PFH) relatives à la revendication de SIL.

En fonction de l'architecture sélectionnée, la réduction de la tolérance aux défauts du matériel peut être à l'origine d'un risque accru d'événements dangereux. Il convient d'évaluer le risque de poursuite de l'exploitation avec une défaillance connue, afin de déterminer le besoin de prendre des mesures compensatoires.

Certaines premières défaillances/anomalies peuvent être exclues si elles présentent clairement une très faible probabilité compte tenu des propriétés inhérentes à la conception et à la construction (voir 3.2 de l'IEC 61511-1:2016). En d'autres termes, il convient que la contribution au niveau objectif de défaillances de la somme des défaillances dangereuses des appareils en série, dont l'exclusion des anomalies est revendiquée, ne dépasse pas 1 %. Il convient que toute autre exclusion des anomalies/des défaillances soit justifiée et documentée. Il ne serait ensuite pas normalement considéré comme nécessaire de contraindre (sur la base de la tolérance aux défauts du matériel) l'intégrité de sécurité d'une SIF avec ces seules défaillances/anomalies.

NOTE 1 Dans le cas des raccordements à l'installation, il est courant de partir du principe que les données de l'appareil de terrain incluent le raccordement à l'installation de l'appareil de terrain jusqu'à l'extrémité, le raccordement à l'installation présentant un taux de défaillances dangereuses non détectées beaucoup plus faible que l'appareil de terrain. La tolérance aux défauts du matériel est en général fournie pour le câblage uniquement quand la tolérance aux défauts du matériel est nécessaire pour l'appareil de terrain. Avec d'autres formes de communication de signal, il peut être nécessaire de déterminer la tolérance aux défauts du matériel pour les moyens de transmission du signal séparément à cause d'un taux de défaillances dangereuses non détectées plus élevé dans l'environnement d'exploitation. Pour ces formes de communication, les moyens de transmission du signal peuvent exiger une tolérance aux défauts du matériel plus importante qu'exigée pour l'appareil de terrain.

NOTE 2 Les appareils du système exécutant des fonctions uniques qui ne sont souvent pas exigées pour que le SIS fonctionne (interfaces opérateurs, stations d'ingénierie, systèmes de gestion de la maintenance et enregistreurs de données, par exemple) et qui sont peu susceptibles d'avoir un impact sur la capacité du SIS à fonctionner comme exigé ne sont en général pas considérés dans l'analyse.

Si certaines anomalies peuvent être exclues (conformément aux critères notés ci-dessus), le HFT minimal peut être réduit (voir 11.4.6 de l'IEC 61511-1:2016).

A.11.4.5 Le Tableau 6 de l'IEC 61511-1:2016 définit la tolérance minimale aux anomalies pour les SIS ou les sous-systèmes des SIS. L'exigence de tolérance aux anomalies dépend du SIL exigé de la SIF en cours de mise en œuvre par le SIS. En établissant la tolérance aux défauts du matériel, il est acceptable de prendre pour hypothèse que le SIS ou le sous-système SIS a été correctement choisi pour l'application et est installé de manière adéquate, mis en service et maintenu de telle sorte qu'une défaillance de jeunesse et qu'une défaillance de fin de vie puissent être exclues de l'évaluation. Les facteurs humains peuvent être exclus lors de la détermination de la tolérance aux défauts du matériel.

A.11.4.6 La tolérance aux anomalies est la solution préférentielle pour s'assurer qu'une architecture robuste est atteinte. Si l'IEC 61511-1:2016 , 11.4.6 s'applique, la justification a pour objet de démontrer que l'architecture alternative proposée avec une tolérance réduite aux défauts du matériel offre une solution équivalente, voire meilleure (à l'aide, par exemple, d'autres moyens vérifiables comme la certification) Il convient de prouver ce qui suit:

a) la conformité aux exigences en matière de tolérance aux défauts du matériel, spécifiées en 11.4.5 de l'IEC 61511-1:2016 , peut générer d'autres défaillances, ce qui conduirait à une baisse de la sécurité globale; et

b) si la tolérance aux défauts du matériel devient nulle, les modes de défaillances identifiés dans le SIS qui exécute la SIF peuvent être exclus, car le/les taux de défaillances dangereuses du/des mode(s) de défaillances identifié(s) sont très faibles par rapport au niveau objectif de défaillances pour la SIF à l'étude.

NOTE 1 Exemples de mise en œuvre de tolérance réduite aux défauts du matériel: dispositions de sauvegarde (redondance analytique, remplacement de la sortie d'un capteur en échec par les résultats de calculs physiques d'autres sorties de capteurs, par exemple), l'utilisation d'éléments plus fiables de la même technologie (si disponibles), le remplacement par une technologie plus fiable, la diminution de l'impact d'une défaillance de cause commune à l'aide d'autres technologies, l'augmentation des marges de conception, l'application de contraintes aux conditions environnementales (pour les composants électroniques, par exemple), la diminution de l'incertitude de fiabilité par regroupement de plus d'informations de situation ou de jugements d'experts, etc.

NOTE 2 La tolérance aux défauts du matériel est uniquement efficace lorsqu'il existe une forte probabilité de détection et de réparation de la défaillance d'une partie avant la défaillance des autres parties redondantes. S'il s'agit de systèmes distants ou placés dans des endroits hostiles (des SIS sous-marins, par exemple) et où la maintenance est difficile (voire complètement impossible), les avantages de la tolérance aux défauts du matériel sont réduits et, dans ces situations, la conception du SIS peut être résistante à toute défaillance, c'est-à-dire qu'elle repose sur la fiabilité intrinsèque des composants plutôt que sur la tolérance aux défauts du matériel.

NOTE 3 La sécurité globale du processus peut être réduite si un autre démarreur de moteur à pleine tension (c'est-à-dire un commutateur à fusible combiné et un contacteur avec transformateur de commande et relais de pilote, assurant également la protection contre les surcharges et les courts-circuits utilisée pour la connexion et la déconnexion à un moteur triphasé réversible ou non) est installé pour des raisons de tolérance aux anomalies. Cela est dû à l'augmentation du nombre de composants lorsque plusieurs démarreurs de moteur sont utilisés au lieu d'un seul, ce qui augmente:

- les déclenchements parasites;
- la complexité de la conception (coordination de la protection contre la surcharge et le court-circuit, par exemple) et les difficultés à appréhender totalement le comportement et les modes de défaillance des démarreurs de moteur;
- la maintenance, l'inspection et les essais finals;
- l'exposition à une tension élevée;
- les défaillances de phase à phase dues à un manque de synchronisation (en général suite à une erreur de câblage) entre plusieurs combinaisons de démarreurs de moteur à pleine tension;
- l'exposition à des arcs électriques;
- les redémarrages exigés.

La justification supplémentaire quant à l'utilisation d'un seul démarreur de moteur à pleine tension de combinaison industrielle à la place de la redondance s'appuie sur les considérations suivantes:

- les modes de défaillance de tous les composants sont bien définis;
- le comportement du démarreur de moteur dans les états d'anomalie peut être déterminé;
- les démarreurs manuels industriels ou les démarreurs de moteur à pleine tension de combinaison industrielle ne s'appuient pas sur des logiciels pour exécuter leur fonction spécifiée;
- les données de défaillances fiables sont suffisantes pour montrer que les taux de défaillances revendiqués pour les défaillances dangereuses détectées et non détectées permettent une quantification des défaillances aléatoires du matériel;

- la faible valeur MTTFdu des démarreurs de moteur à pleine tension de combinaison industrielle;
- l'utilisation de procédures quantitatives pour vérifier que l'utilisation d'un seul démarreur de moteur à pleine tension de combinaison industrielle est justifiée.

A.11.4.7 Aucune autre ligne directrice n'est fournie.

A.11.4.8 Aucune autre ligne directrice n'est fournie.

A.11.4.9 Aucune autre ligne directrice n'est fournie.

A.11.5 Lignes directrices relatives aux "Exigences relatives au choix des appareils"

A.11.5.1 Objectifs

Aucune autre ligne directrice n'est fournie.

A.11.5.2 Lignes directrices relatives aux "Exigences générales"

Des considérations de migration de technologies non programmables vers des technologies PE sont données à l'Annexe C.

A.11.5.2.1 Certaines considérations sont à prendre en compte pour choisir les appareils et les sous-systèmes à utiliser dans un SIS. La première option concerne la conformité des appareils à l'IEC 61508-2:2010 (exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité) et à l'IEC 61508-3:2010 (exigences logicielles). La deuxième option est relative à l'utilisation d'appareils et de sous-systèmes SIS reconnus comme étant fiables du fait d'une utilisation intensive dans des conditions de service similaires et dans un environnement semblable pendant sa durée de vie utile. La durée de vie utile est la période de temps pendant laquelle le taux de défaillances d'un appareil est constant de façon étendue. Le calcul probabiliste du PFD_{avg} global du SIS (il convient qu'il satisfasse à l'exigence du SIL pour chaque SIF mise en œuvre par le SIS) est basé sur ces taux de défaillances. Après la fin de la durée de vie utile, les taux de défaillances peuvent augmenter graduellement, par exemple à cause du vieillissement.

Quelle que soit l'option choisie, il doit être démontré que l'appareil ou le sous-système SIS:

a) est suffisamment fiable pour atteindre la PFD_{avg} cible globale ou le taux cible de défaillances dangereuses de la SIF;

b) satisfait à l'exigence de contrainte architecturale;

c) présente une probabilité suffisamment faible de défaillances systématiques;

d) en cas d'appareils électriques, qu'ils ont un taux de défaillances approprié ou sont basés sur une utilisation préalable.

L'exigence du point c) peut être satisfaite par la conformité à l'IEC 61508-2:2010 et à l'IEC 61508-3:2010 ou en fonction des exigences d'utilisation préalables de l'IEC 61511-1:2016 , 11.5.3.

Une approche pratique pour le choix des appareils utilisés dans les applications de sécurité consiste à utiliser une combinaison de preuves de conformité à l'IEC 61508-2:2010 et à l'IEC 61508-3:2010 et d'une expérience opérationnelle. Cette approche garantit que les appareils sélectionnés sont conçus, fabriqués et gérés pour les applications de sécurité et qu'ils fonctionnent bien pour l'application prévue (par exemple, les défaillances induites par l'application sont prises en compte).

Les procédures de démonstration de la conformité d'un appareil à l'IEC 61508-2:2010 et à l'IEC 61508-3:2010 n'incluent pas la prise en compte des modes de défaillance dangereuse potentielle des interfaces de processus, de l'installation, des alimentations électriques ou des interfaces de communication. Elles peuvent ne pas inclure la limite d'appareil complète et

sont parfois limitées à la portion E/E/PE de l'appareil. Les défaillances associées aux interfaces de processus sont très prédominantes dans les capteurs, y compris les lignes de processus branchées, les lignes gelées, l'infiltration de la corrosion et des gaz, ainsi que dans les vannes, y compris la détérioration des joints, les blocages, les dépôts et la corrosion (y compris l'accumulation de tige). C'est la raison pour laquelle il convient d'évaluer les appareils développés conformément à l'IEC 61508-2:2010 et à IEC 61508-3:2010 afin de garantir leur fonctionnement selon leurs applications prévues. Cela peut inclure le regroupement d'informations d'utilisation préalable ou l'essai simulé d'échantillons statistiques.

Lors de la sélection des appareils, il convient également que l'utilisateur considère la façon de les protéger contre une défaillance systématique. S'agissant d'un appareil développé conformément à l'IEC 61508-2:2010 et à l'IEC 61508-3:2010, il existe un grand nombre de techniques et de mesures qu'il convient que le fabricant mette en œuvre au cours du développement de l'appareil afin de réduire les éventuelles défaillances systématiques. D'un autre côté, l'historique d'utilisation préalable basé sur une expérience significative documentée avec un produit donné dans une application donnée peut être utilisé pour démontrer qu'il existe des défaillances systématiques dangereuses suffisamment faibles sur l'application prévue et donc une protection adéquate contre elles.

A.11.5.2.2 Aucune autre ligne directrice n'est fournie.

A.11.5.3 Lignes directrices relatives aux "Exigences relatives au choix des appareils basés sur l'utilisation préalable"

A.11.5.3.1 De nombreux utilisateurs disposent d'appareils dont l'utilisation est approuvée pour leurs installations. Les capteurs et les vannes qui ont eu un historique de performances non satisfaisantes ont été éliminés comme des appareils approuvés.

Il convient que l'évaluation de ces appareils inclue la prise en compte de leur version et qu'elle s'appuie sur une surveillance documentée des performances sur le terrain. De plus, il convient que le fabricant dispose d'un système de modification incorporant l'évaluation de l'impact des défaillances rapportées et des modifications introduites.

L'ISA TR84.00.04:2015 et la recommandation NAMUR NE130 (appareils "à utilisation préalable" pour les SIS) donnent des lignes directrices sur la façon de qualifier les appareils de terrain, de les garder sous le contrôle de la gestion des changements et d'observer et de documenter leurs performances. Les résultats peuvent être collectés dans un formulaire d'approbation d'appareil.

Si un tel formulaire n'existe pas, il convient que les utilisateurs et les concepteurs conduisent une évaluation sur les capteurs et les vannes pour s'assurer qu'ils sont satisfaisants et que l'appareil fonctionnera comme cela est souhaité. Cela peut exiger des discussions avec d'autres utilisateurs ou concepteurs pour voir ce qu'ils utilisent pour des applications similaires.

A.11.5.3.2 Pour des appareils plus complexes, il convient de noter qu'il peut devenir plus difficile de démontrer la pertinence de l'expérience acquise dans une application. Par exemple, une expérience acquise par l'utilisation d'un PLC dans une application impliquant l'emploi d'un langage à contacts simple peut ne pas être appropriée à une utilisation de l'équipement pour des calculs ou des séquences complexes.

En général, les aspects concernés relatifs au profil d'exploitation des appareils de terrain sont différents de ceux d'un solveur logique.

Pour les appareils de terrain, les points suivants contribuent au profil d'exploitation:

- la fonctionnalité (par exemple, mesurage, action);
- la plage de fonctionnement;

- les propriétés/caractéristiques du processus (par exemple, propriétés des produits chimiques, de la température, de la pression); et
- la connexion au processus.

Pour les solveurs logiques, les points suivants contribuent au profil d'exploitation:

- la version et l'architecture du matériel;
- la version et la configuration du logiciel intégré;
- PA;
- la configuration des E/S;
- le temps de réponse; et
- le taux de sollicitation du processus.

Pour tous les appareils, les points suivants contribuent au profil d'exploitation:

- EMC; et
- les conditions d'environnement.

A.11.5.3.3 Aucune autre ligne directrice n'est fournie.

A.11.5.4 Lignes directrices relatives aux "Exigences relatives au choix des appareils programmables FPL (appareils de terrain, par exemple) basés sur l'utilisation préalable"

A.11.5.4.1 Aucune autre ligne directrice n'est fournie.

A.11.4.4.2 Aucune autre ligne directrice n'est fournie.

A.11.5.4.3 Aucune autre ligne directrice n'est fournie.

A.11.5.4.4 Ce paragraphe précise les exigences supplémentaires lors de la tentative de qualification d'un appareil programmable FPL à une capacité SIL 3.

A.11.5.5 Lignes directrices relatives aux "Exigences relatives au choix des appareils programmables LVL (solveurs logiques, par exemple) basés sur l'utilisation préalable"

A.11.5.5.1 Aucune autre ligne directrice n'est fournie.

A.11.5.5.2 Aucune autre ligne directrice n'est fournie.

A.11.5.5.3 Aucune autre ligne directrice n'est fournie.

A.11.5.5.4 Aucune autre ligne directrice n'est fournie.

A.11.5.5.5 Aucune autre ligne directrice n'est fournie.

A.11.5.5.6 Aucune autre ligne directrice n'est fournie.

A.11.5.6 Lignes directrices relatives aux "Exigences relatives au choix des appareils programmables FVL (solveurs logiques, par exemple)"

Aucune autre ligne directrice n'est fournie.

A.11.6 Appareils de terrain

A.11.6.1 Aucune autre ligne directrice n'est fournie.

A.11.6.2 Aucune autre ligne directrice n'est fournie.

A.11.6.3 Aucune autre ligne directrice n'est fournie.

A.11.7 Interfaces

A.11.7.1 Lignes directrices relatives aux "Généralités"

Les interfaces d'utilisateur relatives à un SIS sont des interfaces opérateur et des interfaces de maintenance/d'ingénierie. Les informations ou les données qui sont transmises entre le SIS et les affichages opérateur peuvent être relatives au SIS ou être informatives.

Si une action de l'opérateur fait partie de la SIF, il convient de considérer tout ce qui est nécessaire pour effectuer cette action comme faisant partie de la SIF. Cela inclurait, par exemple, une alarme indiquant que l'opérateur doit arrêter le processus. Dans cet exemple, il convient que l'interrupteur d'arrêt (les moyens de mettre en œuvre l'action d'arrêt) soit considéré comme faisant partie de la SIF.

La transmission des données, qui ne fait pas partie de la SIF (par exemple, l'affichage de la valeur réelle d'un capteur de la SIF, si la fonction de déclenchement est réalisée au sein de la SIF) peut être affichée dans le BPCS, s'il peut être mis en évidence que les SIF ne sont pas compromises (par exemple, accès à lecture seule dans le BPCS).

A.11.7.2 Lignes directrices relatives aux "Exigences relatives à l'interface opérateur"

Les interfaces opérateur utilisées pour transmettre les informations entre l'opérateur et le SIS peuvent inclure:

– des écrans;
– des panneaux contenant des lampes/voyants, des boutons-poussoirs et des interrupteurs/commutateurs;
– des appareils d'avertissement (visuels et sonores);
– des imprimantes (il convient que ce ne soit pas la seule méthode de communication);
– toute combinaison de ces derniers.

a) afficheurs vidéo

Les afficheurs vidéo du BPCS peuvent partager les fonctions du SIS et du BPCS à condition que les données affichées soient seulement pour information. Les informations critiques de sécurité sont en plus affichées par l'intermédiaire du SIS (par exemple, si l'opérateur fait partie de la fonction de sécurité).

Si une action de l'opérateur est nécessaire pendant des conditions d'urgence, il convient que la mise à jour et les taux de rafraîchissement de l'écran de l'opérateur soient conformes à la SRS.

Il convient que les afficheurs vidéo relatifs au SIS soient clairement identifiés en tant que tels, évitant toute ambiguïté ou possibilité de confusion pour l'opérateur, en cas de situation d'urgence.

L'interface opérateur du BPCS peut être utilisée pour offrir une journalisation automatique des événements des SIF et des fonctions d'alarme du BPCS.

Les points à consigner pourraient être les suivants:

– les événements du SIS (tels que des occurrences de déclenchement et de prédéclenchement);
– toutes les fois que l'accès au SIS est obtenu pour des changements de programme;

– les diagnostics (par exemple, divergences, etc.).

Il est important que l'opérateur soit alerté lors de la dérivation d'une partie quelconque du SIS, par l'intermédiaire d'une alarme et/ou d'une procédure d'exploitation. Par exemple, la dérivation de l'élément terminal dans un SIS (par exemple, robinet de sectionnement) pourrait être détectée par l'intermédiaire d'interrupteurs de fin de course sur la vanne de dérivation qui activent une alarme sur le tableau de contrôle ou en installant des blocages ou des verrouillages mécaniques sur la vanne de dérivation qui sont gérés par les procédures d'exploitation. Il est généralement suggéré de maintenir ces alarmes de dérivation distinctes du BPCS.

b) panneaux

Il convient que les panneaux soient placés en des endroits permettant un accès facile aux opérateurs. Il convient de considérer l'emplacement des panneaux par rapport aux zones affectées par des dangers potentiels.

Il convient que les panneaux soient agencés de manière à s'assurer que la disposition des boutons-poussoirs, des lampes/voyants, des instruments de mesurage et de toutes les autres informations ne soit pas une source de confusion pour l'opérateur. Les interrupteurs d'arrêt pour les différents équipements ou unités de processus ou qui semblent identiques et qui sont regroupés, peuvent avoir comme conséquence l'arrêt intempestif d'un équipement par un opérateur sous contrainte d'une situation d'urgence. Il convient que les interrupteurs d'arrêt soient physiquement séparés et que leur fonction soit identifiée par une étiquette. Il convient de donner des moyens pour soumettre à l'essai toutes les lampes/voyants.

c) imprimantes et journalisation

Il convient que les imprimantes connectées au SIS ne compromettent pas la SIF, si une imprimante présente une défaillance, est arrêtée, est débranchée, manque de papier ou se comporte anormalement.

Les imprimantes sont utiles pour produire des documents préliminaires relatifs aux informations de séquence d'événements (SOE), aux diagnostics et autres événements et alarmes, avec l'indication de l'heure et de la date et l'identification par un numéro repère. Il convient que des utilitaires de formatage de comptes rendus soient fournis.

Si la fonction d'impression comporte une mémoire tampon (les informations sont stockées, puis imprimées sur sollicitation ou en fonction d'un scénario synchronisé), il convient alors que la mémoire tampon soit dimensionnée de sorte que les informations ne soient pas perdues et que sous aucun prétexte, la fonctionnalité du SIS ne soit compromise du fait d'une insuffisance d'espace mémoire tampon.

Il convient que l'opérateur obtienne assez d'informations sur un affichage pour donner suite rapidement aux informations critiques. La cohérence de l'affichage est importante et il convient que les méthodes, les conventions d'alarme et les appareils d'affichage utilisés soient cohérents avec ceux des afficheurs du BPCS.

L'agencement de l'affichage est également important. Il convient d'éviter les agencements qui présentent une grande quantité d'informations sur un afficheur, car ils peuvent conduire à de mauvaises interprétations des données de la part des opérateurs, qui pourraient entreprendre des actions incorrectes. Il convient d'utiliser des couleurs, des indicateurs clignotants et un espacement judicieux des données pour guider l'opérateur vers les informations importantes et réduire toute possibilité de confusion. Il convient que les messages soient clairs, concis et non ambigus.

Il convient que l'affichage soit conçu de telle manière que les données puissent être identifiées par un daltonien. Par exemple, des conditions matérialisées par les couleurs rouge ou vert pourraient également être traduites par des graphismes pleins ou vides.

A.11.7.2.1 Aucune autre ligne directrice n'est fournie.

A.11.7.2.2 Aucune autre ligne directrice n'est fournie.

A.11.7.2.3 Aucune autre ligne directrice n'est fournie.

A.11.7.2.4 Aucune autre ligne directrice n'est fournie.

A.11.7.2.5 Aucune autre ligne directrice n'est fournie.

A.11.7.2.6 Aucune autre ligne directrice n'est fournie.

A.11.7.2.7 Aucune autre ligne directrice n'est fournie.

A.11.7.3 Lignes directrices relatives aux "Exigences relatives à l'interface de maintenance/d'ingénierie"

A.11.7.3.1 Aucune autre ligne directrice n'est fournie.

A.11.7.3.2 Aucune autre ligne directrice n'est fournie.

A.11.7.3.3 Les interfaces de maintenance/d'ingénierie sont des moyens de programmation, d'essais et de maintenance du SIS. Les interfaces sont des appareils qui sont utilisés pour des fonctions telles que:

a) la configuration du matériel du système;
b) le développement du programme d'application, la documentation et le téléchargement vers le solveur logique du SIS;
c) l'accès au programme d'application pour les changements, les essais et la surveillance;
d) la visualisation des ressources système du SIS et informations de diagnostic;
e) le changement des niveaux de sécurité du SIS et l'accès aux variables du programme d'application.

Il convient que les interfaces de maintenance/d'ingénierie aient les capacités d'afficher l'état d'exploitation et de diagnostic de tous les appareils du SIS (par exemple, les modules d'entrée/sortie, les processeurs), comprenant les communications entre ces derniers.

Il convient que la maintenance/l'ingénierie offre des moyens de copier les programmes d'application sur des supports de stockage de secours.

Il convient qu'un ordinateur individuel connecté à un SIS pour les besoins de la maintenance/ ingénierie, ne compromette pas des fonctions de sécurité si l'ordinateur individuel présente une défaillance, est arrêté ou encore s'il est déconnecté.

A.11.7.3.4 Aucune autre ligne directrice n'est fournie.

A.11.7.4 Lignes directrices relatives aux "Exigences relatives à l'interface de communication"

A.11.7.4.1 Les deux interfaces peuvent se ressembler tant que l'interface de maintenance/d'ingénierie ne peut pas être utilisée pour manipuler le processus. Il convient que l'interface de maintenance/d'ingénierie ne soit pas utilisée comme interface opérateur.

A.11.7.4.2 Aucune autre ligne directrice n'est fournie.

A.11.7.4.3 Aucune autre ligne directrice n'est fournie.

A.11.7.4.4 Aucune autre ligne directrice n'est fournie.

A.11.8 Lignes directrices relatives aux "Exigences relatives à la maintenance ou à la conception des essais"

A.11.8.1 Il convient que la conception du SIS prenne en compte la manière dont le système va être maintenu et soumis à l'essai. Si le SIS doit être soumis à l'essai pendant que le processus est en fonctionnement, il convient que la conception n'exige pas la déconnexion de fils, l'application de connexions cavaliers ou le forçage de registres du logiciel (par exemple, des entrées, des sorties), car l'utilisation de ces techniques peut compromettre l'intégrité du SIS. Il convient que la conception du système satisfasse aux exigences techniques et procédurales du SIS pour les essais, afin de réaliser, sans risque, les essais complets du système de capteurs, des solveurs logiques et des éléments terminaux.

Il est important de définir comment un SIS va être maintenu pendant que le processus est en fonctionnement. Par exemple, s'il convient de travailler sur un transmetteur ou sur une vanne, il convient de considérer la façon dont le service de maintenance travaillera sur ces instruments, sans provoquer de déclenchement intempestif, tout en conservant la sécurité du processus.

Il convient de noter qu'il convient que toute limite sur la période d'essai des éléments terminaux soit prise en compte dans le calcul de la PFD_{avg} de la SIF.

A.11.8.2 Aucune autre ligne directrice n'est fournie.

A.11.8.3 Des dérivations peuvent réduire le niveau de sécurité dans un SIS. Cette réduction de sécurité peut être contournée par:

- l'utilisation de mots de passe et/ou commutateurs à verrouillage par clé. Certaines conceptions peuvent incorporer des coffrets fermant à clé (ou verrouillés) contenant les dérivations appropriées;
- l'identification claire des dérivations de tuyauterie peut être réalisée par blocage des positions de vanne ou en installant des marquages de sécurité indiquant l'importance de la position appropriée;
- des installations ou des procédures claires (par exemple, commutateur de suppression de la dérivation maîtresse) pour la commande de l'application et de la suppression de la dérivation;
- l'utilisation de dérivation avec une fonction de limitation de durée qui supprimera automatiquement la dérivation – une telle fonctionnalité réduit le risque qu'une dérivation reste active à l'issue des essais ou de la maintenance.

Par exemple, pour une configuration de capteur 1oo2, certains utilisateurs souhaitent dériver les deux capteurs en même temps, mais d'autres souhaitent avoir une dérivation séparée pour chaque capteur. Si les deux capteurs sont dérivés, il sera nécessaire de mettre en place des mesures pour s'assurer que le risque reste tolérable. L'une ou l'autre option peut être possible, mais il convient d'étudier les deux possibilités très tôt dans le processus de conception.

De même, certaines opérations du processus n'acceptent pas que la position de la vanne soit modifiée pendant que le processus est en fonctionnement ou l'installation d'une dérivation contournant la vanne peut être impraticable. Dans ces cas, il convient que la conception tienne compte des essais du SIS, autant qu'il est possible, c'est-à-dire, au moins par l'intermédiaire de l'électrovanne. Dans ce dernier cas, un certain type de dérivation autour du solénoïde peut être inclus dans la conception, avec les commandes d'alarme ou procédurales habituelles pour cette dérivation.

A.11.8.4 Des temporisateurs peuvent être fournis dans le SIS, afin de limiter la durée de dérivation (par un réarmement automatique et/ou l'envoi d'alarmes à l'opérateur, par exemple). Une logique peut être fournie dans le SIS pour réinitialiser automatiquement une neutralisation ou limitation (par manque de pression au démarrage d'une pompe, par exemple).

A.11.8.5 Aucune autre ligne directrice.

A.11.8.6 Il convient de ne pas utiliser le forçage des entrées et des sorties dans le SIS du PE dans le cadre du programme d'application. Par exemple, le forçage non commandé des entrées et des sorties via la modification en ligne de la mémoire dans le solveur logique à l'aide d'un outil de programmation pendant que le programme est en fonctionnement est fréquemment utilisé lors du développement du programme, afin d'explorer les modifications proposées du programme d'application. Il convient toutefois de ne pas utiliser cette pratique en ligne, car elle masquera le statut d'entrée "réel" des variables de l'installation et/ou donnera des sorties fausses aux appareils de l'installation. Quel que soit l'événement, le solveur logique ne commandera pas les installations de la façon prévue. De telles petites modifications au programme d'application peuvent en outre être aisément être ignorées et rester dans le programme alors qu'elles ne sont plus exigées.

A.11.9 Lignes directrices relatives à la "Quantification de défaillance aléatoire"

A.11.9.1 Il convient que les utilisateurs et les concepteurs consultent l'IEC 61511-3:–, Annexe J, l'IEC 61508-6:2010, Annexe B, l'ISO 12489, à l'ISA TR84.00.02:2002, l'IEC 61508-3:2010, Annexe B, l'IEC 61025 (Arbres de pannes), l'IEC 61078 (Diagrammes de fiabilité), l'IEC 61165 (Diagrammes de Markov), l'IEC 62551 (Réseaux de Petri) et l'IEC 62502 (Arbres d'événements) pour obtenir des lignes directrices relatives aux techniques disponibles pour s'assurer que la conception du SIS satisfait aux performances relatives aux défaillances aléatoires du matériel.

Dans les intervalles d'essais périodiques, la probabilité d'une défaillance dangereuse en mode sollicitation, PFD(t), augmente de façon continue alors que le temps passe. Par conséquent, une fois la valeur moyenne passée, elle restera en permanence au-dessus jusqu'à la fin de l'intervalle d'essai périodique. Dans certains cas, elle peut même dépasser la limite de SIL supérieure qui correspond à cette valeur moyenne et rester en permanence au-dessus. Quand une intégrité de sécurité élevée est exigée, les valeurs moyennes seules peuvent donc donner une fausse impression de sécurité; il convient de vérifier par exemple que le risque qui correspond aux valeurs les plus élevées est cohérent avec les critères de risque de l'organisation de l'utilisateur.

Une SIF qui agit sur un fonctionnement en mode sollicitation (par exemple, fermeture d'une vanne pour éviter une surpression) est souvent immédiatement suivie d'une autre SIF qui implique les mêmes composants, mais qui agit en mode continu (par exemple, pour empêcher l'ouverture de la vanne tant que la surpression est présente en amont de la vanne). Pour la SIF qui fonctionne en mode sollicitation, il convient donc de considérer la fréquence de danger associée à la défaillance du SIS qui ne maintient pas le processus à l'état de sécurité.

A.11.9.2 Les taux de défaillances estimés peuvent être déterminés par une analyse des modes de défaillance quantifiée de la conception, en utilisant les données de défaillance à partir d'une source industrielle reconnue ou à partir de l'expérience d'une utilisation préalable dans le même environnement que celui de l'application prévue. A des fins de prudence, la limite de confiance supérieure de 70 % des données d'entrée peut être utilisée dans les calculs.

Il doit être noté que le taux de défaillances non détectées global des éléments tolérants aux anomalies dépend du temps et augmente pendant les intervalles d'essai périodique. Les éléments tolérants aux anomalies peuvent avoir des taux de défaillances dépendants du temps.

EXEMPLE Un élément fait de deux composants similaires A et B avec le même taux de défaillances non détectées λ présente un taux de défaillances non détectées global A qui augmente de 0 à λ quand la durée diminue.

Lors de l'évaluation des effets des défaillances aléatoires du matériel d'un SIS (ou d'un sous-système SIS), une tolérance nulle aux défauts du matériel, qui met en œuvre une SIF

exploitée en mode à sollicitation élevée ou en mode continu, il convient de ne créditer les diagnostics que si:

- la somme de l'intervalle d'essai du diagnostic et du temps nécessaire pour exécuter l'action spécifiée pour atteindre ou maintenir un état de sécurité est inférieure au temps de sécurité du processus; ou
- en mode à sollicitation élevée, le rapport de la fréquence d'essai du diagnostic à la fréquence de sollicitation est égal ou supérieur à 100.

La procédure d'essai périodique et l'analyse de fiabilité des installations d'essai périodique incluent, par exemple:

- les durées des essais périodiques;
- l'état du processus (en fonctionnement ou arrêté) pendant les essais périodiques;
- l'état de l'appareil soumis à l'essai pendant les essais périodiques (en ligne ou hors ligne); si l'appareil soumis à l'essai est hors ligne (c'est-à-dire, indisponible) pendant les essais périodiques, cela peut contribuer de façon importante à sa PFD_{avg};
- la couverture de l'essai périodique quand les essais périodiques ne sont pas efficaces à 100 %. Cela implique l'identification des défaillances qui, de façon inhérente, ne peuvent jamais être détectées par les essais périodiques;
- la défaillance qui peut être causée par les essais périodiques eux-mêmes (par exemple, défaillance due au changement d'état nécessaire pour l'essai);
- le possible décalage des essais périodiques pour des appareils redondants similaires afin de décorréler les essais périodiques;
- la possibilité que l'essai périodique renvoie une valeur incorrecte sur l'état de santé du SIS:
  - essai périodique affecté par une anomalie associée à l'essai périodique lui-même;
  - l'erreur humaine pendant les essais périodiques (par exemple, absence de détection d'une véritable défaillance, omission d'un essai, appareil soumis à un essai périodique ou réparé qui reste hors ligne à l'issue de l'essai périodique ou de la réparation, etc.).

Si l'intervalle d'essai périodique n'est pas explicitement modélisé pour le calcul probabiliste, le MTTR des défaillances dangereuses individuelles détectées peut être calculé comme la moitié de l'intervalle d'essai périodique plus le MRT de la défaillance considérée.

La plupart des techniques données en A.11.9.1 exigent une certaine quantification de la couverture du diagnostic du SIS. Les diagnostics sont des essais exécutés automatiquement pour détecter des anomalies dans le SIS, pouvant donner lieu à des défaillances en sécurité ou des défaillances dangereuses.

Une technique de diagnostic particulière ne peut pas, habituellement, détecter toutes les anomalies possibles. L'efficacité des diagnostics utilisés peut être estimée pour l'ensemble des anomalies concernées (voir l'Annexe C de l'IEC 61508-2:2010 et l'Annexe C de l'IEC 61508-6:2010 pour obtenir des exemples de calcul de la couverture du diagnostic).

L'amélioration de la couverture du diagnostic du SIS peut aider à satisfaire aux exigences du SIL. Dans ce cas, il convient qu'à la fois la couverture du diagnostic et la période entre les essais de diagnostic (l'intervalle des essais de diagnostic) soient prises en compte pour calculer la probabilité de la défaillance (mode sollicitation) ou la fréquence de la défaillance (mode continu) du SIS. Pour d'autres lignes directrices, voir l'IEC 61508-2:2010, Annexe C ou l'ISA TR84.00.02:2015.

Dans les situations où le SIS est la seule couche de protection et où il est utilisé pour une fonction de sécurité fonctionnant dans le mode de fonctionnement continu, il convient que l'intervalle des essais de diagnostic soit tel que les anomalies dans le SIS soient détectées à temps pour assurer l'intégrité du SIS et permettre d'entreprendre une action pour garantir un

état de sécurité dans le cas d'une défaillance se produisant dans le processus ou dans le système de commande de processus de base.

Pour réaliser cela, il convient que la somme de l'intervalle des essais de diagnostic et du temps de réaction pour atteindre un état de sécurité soit inférieure au "temps de sécurité du processus". Conformément à 3.2.52.1 de l'IEC 61511-1:2016 , le temps de sécurité du processus est défini comme étant la période de temps entre une défaillance se produisant dans le processus ou dans le BPCS (avec risque de donner lieu à un événement dangereux) et l'occurrence de l'événement dangereux si la SIF n'est pas exécutée.

En règle générale, les défaillances critiques et potentiellement critiques des appareils communs (comme des défaillances d'UC/RAM/ROM) neutralisent presque totalement le traitement des données et ont donc plus d'impact qu'une défaillance d'un point de sortie unique. Les modes de défaillance qui présentent une probabilité de défaillance élevée doivent être détectés avec plus de certitude. De plus, il convient de tenir compte de la détectabilité des modes de défaillance.

Pour chaque diagnostic mis en œuvre, il convient que l'intervalle des essais et que l'action résultant de la détection de l'anomalie satisfassent à la SRS.

Dans le cas où ces appareils de diagnostic ne seraient pas intégrés dans les équipements mis à disposition par le constructeur, des appareils de diagnostic configurés par un organisme externe peuvent être mis en œuvre sur le système ou au niveau de l'application afin de satisfaire au SIL pour la SIF.

Les appareils de diagnostic peuvent ne pas être capables de détecter des erreurs systématiques (comme des bogues logiciels). Cependant, des mesures conservatoires appropriées pour détecter des anomalies systématiques éventuelles peuvent être mises en œuvre.

Les appareils de diagnostic peuvent être réalisés en utilisant diverses méthodes ou une combinaison de méthodes, incluant les éléments figurant ci-dessous:

a) Capteurs

1) Des alarmes de diagnostic pourraient être utilisées pour détecter un capteur qui délivre une indication complètement au-delà ou en deçà de la plage attendue. L'utilisation d'une alarme "hors plage" peut être une manière de réaliser cela. Par exemple, dans une application de déclenchement sur températures élevées, avec les capteurs de température redondants, une alarme "signal faible, hors plage" pourrait être ajoutée pour diagnostiquer une défaillance de capteur ou une perte de signal de capteur.
2) Si des capteurs redondants sont utilisés, la comparaison des valeurs analogiques permet de détecter les anomalies qui peuvent se produire pendant l'exploitation normale. Si trois capteurs sont utilisés, la valeur médiane des trois lectures peut être utilisée (choix de la valeur médiane – voir la note ci-dessous). Des écarts significatifs entre les lectures peuvent être créés par:
   - le raccordement ou le gel au niveau des lignes de sortie d'impulsion;
   - la réduction de la pression d'alimentation de purge;
   - un revêtement relatif à un procédé de gaine thermométrique;
   - des problèmes de mise à la terre ou d'alimentation en énergie;
   - la non-réponse d'un transmetteur de capteur ayant une valeur de sortie qui reste fixe.

   NOTE 1 Le choix de la valeur médiane est plus avantageux que la comparaison à la moyenne, parce que la moyenne est biaisée par l'appareil qui ne fonctionne pas correctement. Toutefois, le choix de la valeur médiane ne fonctionne pas si deux transmetteurs donnent des lectures fausses; les défaillances de cause commune peuvent donc être considérées.
3) Si "2)" est appliqué ou si une comparaison est faite entre des capteurs analogues dans le SIS et des lectures de paramètres de processus comparables par d'autres capteurs

dans les systèmes tels que le BPCS, l'éventuelle amélioration de la couverture du diagnostic dépendra d'applications spécifiques et doit être analysée, évaluée et documentée. Si une couverture du diagnostic supérieure à 90 % est revendiquée, il convient d'analyser et de documenter les sources de défaillance de cause commune (CCF, Common Cause Failures) entre des capteurs qui collaborent.

NOTE 2 A titre de comparaison, une divergence peut générer au moins une alarme. Ce seuil d'alarme de divergence peut être défini conformément à un écart documenté de la variable de processus associée. Une telle comparaison détecte la défaillance des capteurs SIS et des capteurs non-SIS. Les fausses alarmes et les déclenchements parasites générés par les défaillances des capteurs non-SIS peuvent ensuite être analysés avant la mise en œuvre de ce type de solution.

NOTE 3 L'amélioration de la couverture du diagnostic fournie par ce type de comparaison peut être utilisée pour augmenter l'intervalle d'essais périodiques.

4) Des délais peuvent être prévus pour prévenir les alarmes intempestives dues aux variations de la réponse du capteur du fait des changements de processus provoqués par l'emplacement du capteur ou par sa technologie. Par exemple, certains capteurs de débit redondants peuvent comporter un délai de 1 s à 2 s. Un certain nombre de progiciels proposés par des constructeurs sont disponibles pour surveiller les lectures des capteurs redondants et calculer l'écart-type, afin d'initier les alarmes de diagnostics.

5) Une autre méthode de diagnostics relative au capteur est la comparaison de variables liées (par exemple, les totalisateurs de débit en fonction d'un changement de niveau de réservoir ou relation entre pression et température).

b) Eléments terminaux

1) La comparaison des informations en retour de l'élément terminal (tels que des interrupteurs de fin de course ou des transmetteurs de position) par rapport à l'état requis, peut être effectuée pour vérifier que les actions prévues ont été entreprises. Il convient que des délais suffisants soient utilisés pour filtrer l'alarme relative aux vannes en cours de transition (par exemple, de complètement ouverte à complètement fermée). Cette comparaison des informations en retour de l'élément terminal par rapport à l'état requis ne peut être considérée comme étant un diagnostic que si la vanne change périodiquement à l'état de sécurité, dans le cadre de l'exploitation normale (par exemple, fonctionnement en lots).

2) Certaines vannes, certains actionneurs, solénoïdes, et/ou positionneurs peuvent comporter des capacités de diagnostics.

c) Solveurs logiques

Les solveurs logiques électroniques programmables (PE) qui sont configurés pour la sécurité ou conformes à l'IEC 61508 incluent généralement des diagnostics qui détectent différentes anomalies. Les types et la couverture du diagnostic seront généralement décrits dans le manuel de sécurité.

d) Appareils de diagnostic configurés extérieurement

Des exemples de ces appareils comprennent les chiens de garde et les appareils de surveillance d'extrémité de ligne.

Il convient également de tenir compte du degré de confiance dans les données de fiabilité utilisées pour effectuer les calculs de mesure cible. L'utilisation des limites supérieures de confiance à 70 % des paramètres de fiabilité d'entrée garantit l'exécution de calculs prudents (voir 11.9.4 de l'IEC 61511-1:2016).

A.11.9.3 Aucune autre ligne directrice n'est fournie.

A.11.9.4 Les valeurs de données de fiabilité utilisées lors de la quantification des effets des défaillances aléatoires du matériel ne sont toujours connues qu'avec des incertitudes numériques. L'évaluation de l'impact de ces incertitudes sur les mesures cibles est utile pour consolider les revendications de SIL.

L'incertitude (voir Note 1) d'un paramètre de fiabilité donné (le taux de défaillances, par exemple) peut être évaluée par:

a) des analyses statistiques,

b) l'exercice d'un jugement expert et, le cas échéant,

c) l'exécution d'essais spécifiques.

En règle générale, les incertitudes numériques diminuent lorsque les informations de situation disponibles augmentent.

Un paramètre de fiabilité n'est donc pas une valeur déterministe parfaitement connue, mais une variable aléatoire avec une distribution plus ou moins éparpillée autour de sa valeur moyenne (voir la Figure A.5).

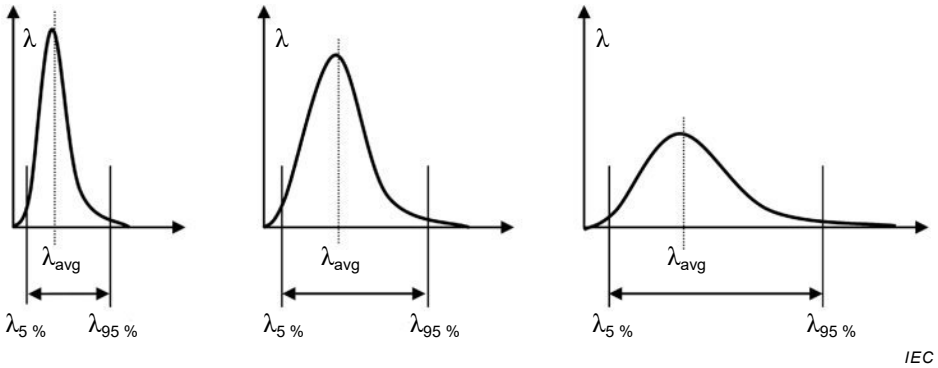


Figure A.5 – Représentation des incertitudes d'un paramètre de fiabilité

Plus la distribution est fine, moins le paramètre est incertain. L'incertitude augmente de gauche à droite dans la Figure A.5.

A la limite, si le paramètre était parfaitement connu, la courbe serait une simple ligne droite verticale (c'est-à-dire, une distribution Dirac).

Comme le montre la Figure A.5, l'incertitude du paramètre de fiabilité λ peut être évaluée par son intervalle de confiance à, par exemple, 90 %: la valeur moyenne réelle de λ présente une probabilité de 90 % d'appartenir à l'intervalle [$\lambda_{5\ \%}$, $\lambda_{95\ \%}$] où λ présente une probabilité de 5 % d'être supérieur à $\lambda_{5\ \%}$ et une probabilité de 5 % d'être plus défavorable que $\lambda_{95\ \%}$.

Sur une base purement statistique, la moyenne d'un paramètre de fiabilité peut être estimée à l'aide de "l'estimation de probabilité maximale" et les limites de confiance [$\lambda_{5\ \%}$, $\lambda_{95\ \%}$] être calculées à l'aide de la fonction χ^2 (Chi carré) qui est indiquée dans des tableaux dans les livres statistiques.

Un échantillon de *n* défaillances observées sur un temps T d'observation cumulée fournit une moyenne égale à n/T et un intervalle de confiance à 90 % égal à $[\frac{1}{2T}\chi^2_{0,95,2n}, \frac{1}{2T}\chi^2_{0,05,2(n+1)}]$.

La largeur de cet intervalle diminue, c'est-à-dire que la précision s'améliore quand le temps d'observation cumulée et/ou quand le nombre de défaillances observées augmente (de droite à gauche à la Figure A.5).

L'approche bayésienne peut également être utilisée pour prendre en charge les observations statistiques, le jugement expert et les résultats de l'essai spécifique. Cela peut être utilisé pour s'adapter aux fonctions de distribution probabiliste pour utilisation approfondie dans la simulation de Monte-Carlo.

Si l'intervalle de confiance est important (c'est-à-dire, en cas d'informations de situation rares), il convient de mettre en œuvre dès que possible un processus d'ensemble de données de fiabilité. En outre, il convient de mettre régulièrement à jour les prévisions probabilistes des mesures cibles probabilistes à l'aide des données de fiabilité collectées.

NOTE 1 La norme IEC 61511 contient des calculs probabilistes qui nécessitent l'exécution de données de fiabilité précises. Elle ne peut pas être correctement mise en œuvre sans une collecte des données de fiabilité des utilisateurs. Quand un manque de données de fiabilité est identifié, il s'agit d'une opportunité pour lancer une collecte de données de fiabilité spécifiques pour compenser ce manque. Si cela n'est pas utile pour le SIS présent, cela le sera pour le prochain.

La première approche pour prendre en charge l'incertitude décrite ci-dessus consiste à utiliser des données de fiabilité d'entrée pessimistes. Cela garantit que, malgré le manque de précision, l'évaluation de la mesure cible (PFD_{avg} ou PFH) n'est pas optimiste. Pour cela, des limites de confiance supérieures plus élevées que les valeurs moyennes conventionnelles peuvent être utilisées pour les paramètres de fiabilité d'entrée. L'utilisation de limites supérieures de 70 % ($\lambda_{70\ \%} > \lambda_{avg}$, par exemple) est généralement considérée pour assurer un niveau de confiance raisonnable. Cela est présenté à la Figure A.6, qui montre que le conservatisme des données d'entrées décroît lorsque la précision augmente (la différence $\lambda_{70\ \%} - \lambda_{avg}$ diminue).

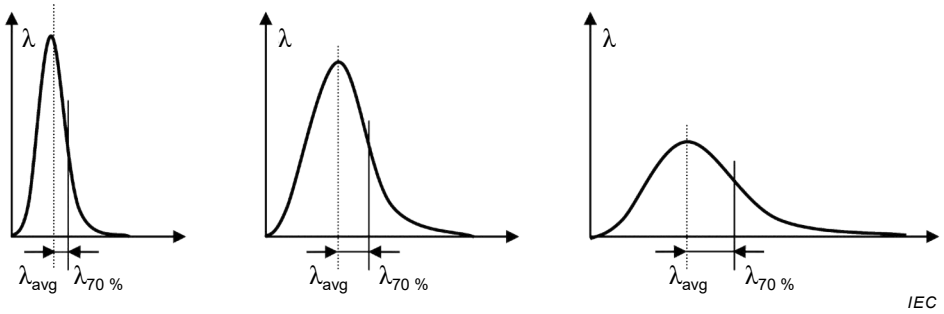


Figure A.6 – Représentation de la limite supérieure de confiance à 70 %

NOTE 2 A partir d'un échantillon de n défaillances observées sur un temps T d'observation cumulée, la limite supérieure de confiance peut être calculée à l'aide de la fonction χ^2: Par exemple, $\lambda_{70\ \%}$ peut être évalué par $\lambda_{0,7} = \frac{1}{2T}\chi^2_{0,3,2(n+1)}$ et il y a 70 % de chances que la valeur réelle soit inférieure (c'est-à-dire meilleure) que celle-ci. Cette limite supérieure de confiance existe même quand aucune défaillance n'a été observée. Elle est toujours pessimiste comparée à λ_{avg}, mais elle l'est de moins en moins quand T et/ou n augmente (voir Figure A.6).

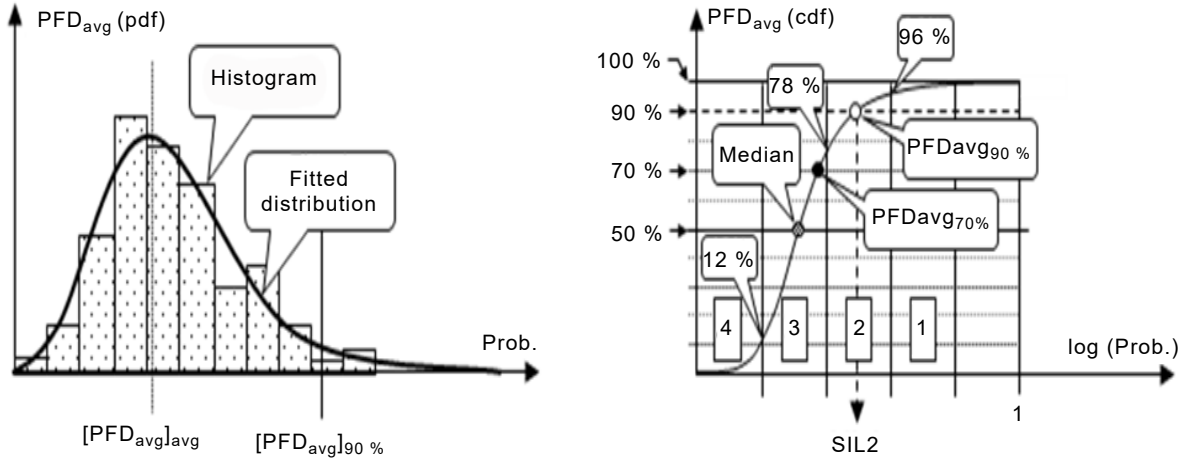
NOTE 3 Les calculs effectués avec la limite supérieure de confiance à 70 % des paramètres d'entrée ne donnent pas la limite supérieure de confiance à 70 % du résultat global (PFD_{avg}, par exemple). Les calculs ainsi effectués ne font que garantir que le résultat est prudent.

L'approche précédente implique qu'un seul calcul de la cible probabiliste (c'est-à-dire, PFD_{avg}), mais le niveau de conservatisme n'est pas connu. Une autre approche peut donc être utilisée si ce niveau de conservatisme doit être connu. Elle consiste à utiliser l'ensemble des distributions des paramètres de fiabilité d'entrée plutôt que des valeurs uniques comme $\lambda_{70\ \%}$. La simulation dite de "Monte-Carlo" peut être utilisée pour cela:

a) l'utilisation de nombres aléatoires pour simuler les distributions probabilistes des valeurs des paramètres de fiabilité d'entrée; et

b) la réalisation d'un certain nombre de calculs (par exemple, 100) de la cible probabiliste avec différents jeux de nombres aléatoires.

Cela fournit un échantillon statistique (c'est-à-dire, un histogramme) du résultat cible (par exemple, PFD_{avg}) qui peut être traité pour obtenir la distribution probabiliste correspondante et les niveaux de confiance et moyens correspondants (voir Figure A.7).



Anglais	Français
PFD_{avg} (pdf)	PFD_{avg} (pdf)
Histogram	Histogramme
Fitted distribution	Distribution ajusté
Prob.	Probabilité

Figure A.7 – Distribution probabiliste type des résultats cibles de la simulation de Monte-Carlo

La Figure A.7 présente la fonction de densité probabiliste (pdf, probabilistic density function) et la fonction de distribution cumulée (cdf, cumulative distribution function) correspondante qui peuvent être obtenues d'une simulation de Monte-Carlo. Elle montre la distribution de PFD_{avg} autour de sa valeur moyenne $[PFD_{avg}]_{avg}$.

NOTE 4 PFD_{avg} est en elle-même une variable aléatoire compte tenu des lois probabilistes sous-jacentes utilisées pour procéder aux calculs. Le calcul ci-dessus ne fournit la distribution qu'intrinsèquement à cause des incertitudes des paramètres de fiabilité d'entrée.

$[PFD_{avg}]_{avg.}$ peut être utilisé à la place du PFD_{avg} classique, mais son conservatisme ne peut pas être démontré. Il est probable qu'il soit proche de sa valeur médiane (c'est-à-dire, 50 % de chances que la valeur réelle soit meilleure que (PFD_{avg}) 50 % et 50 % que la valeur réelle soit plus défavorable).

La courbe cdf de la Figure A.7 montre que PFD_{avg} a 12 % de chances d'être dans la plage de SIL 4 (88 % de chances d'être dans la plage de SIL 3 ou plus défavorable), 78 % de chances d'être dans la plage de SIL 3 ou plus favorable (22 % de chances d'être dans la plage de SIL 2 ou plus défavorable), 96 % de chances d'être dans la plage de SIL 2 ou plus favorable (4 % de chances d'être dans la plage de SIL 1 ou plus défavorable), etc.

A des fins de conservatisme, un niveau de confiance de 90 % peut être choisi. $[PFD_{avg}]_{90\ \%}$ étant dans les limites de SIL 2, cela conduit à SIL 2 pour cet exemple. Il est à noter qu'avec un niveau de confiance de 70 %, le même exemple donne SIL 3.

A.11.9.5 Aucune autre ligne directrice n'est fournie.

A.12 Développement du programme d'application du SIS

A.12.1 Objectif

Voir l'Article B.1 et l'Article F.20 pour un/des exemple(s) de définition du développement d'un programme d'application pour une ou plusieurs SIF dans un SIS.

A.12.2 Lignes directrices relatives aux "Exigences générales"

A.12.2.1 L'Article 12 de l'IEC 61511-1:2016 concerne le développement et la modification de programmes d'application faisant l'objet d'exigences jusqu'à SIL 3. L'expérience montre qu'il existe peu de différence dans les méthodes de développement SIL 1, SIL 2 ou SIL 3 lors de l'utilisation de LVL dans un solveur logique conforme à l'IEC 61511-1: — en fonction du manuel de sécurité correspondant.

Il peut y avoir des différences entre SIL 1, SIL 2 et SIL 3 pour les techniques d'essai et de vérification pour des SIL différents. Voir A.7.2.2.

A.12.2.2 Par exemple, il convient que le programmeur de l'application passe en revue les informations dans la description logique (Article F.15 et Article F.17, par exemple) et les compare aux instructions séquentielles dans le cadre du processus de détection des erreurs et pour s'assurer qu'il a bien compris l'exigence prévue.

A.12.2.3 La présente norme se limite aux exigences relatives aux programmes d'application développés à l'aide du LVL. "Le développement de programme d'application" est interprété comme la conception et la mise en œuvre de la logique d'application de sécurité à l'aide d'un PE sélectionné conformément à l'IEC 61511-1:2016 , 11.5.

A.12.2.4 La présente norme porte également sur l'application des appareils qui utilisent les langages de programme figé (FPL), comme par exemple le contrôle de l'entrée des paramètres dans les capteurs intelligents (voir Annexe C et le Tableau F.13 par exemple).

A.12.2.5 Il convient d'utiliser des zones séparées du programme d'application pour la non-sécurité et la SIF.

Une manière de démontrer que l'indépendance est adéquate pourrait être de satisfaire à tous les points suivants:

a) les SIF dans le programme d'application sont clairement identifiées comme étant un code d'application de SIF;

b) les éléments non-SIF dans le programme d'application sont clairement séparés;

c) toutes les variables utilisées dans la mise en œuvre de la SIF sont identifiées;

d) tout le programme d'application mettant en œuvre des fonctions instrumentées non liées à la sécurité est identifié en tant que code de fonction instrumentée non lié à la sécurité;

e) tout le programme d'application utilisant des variables non liées à la sécurité et des variables SIF satisfait aux conditions suivantes:

f) le programme d'application non lié à la sécurité (y compris l'ensemble des fonctions et des blocs fonctionnels) n'écrit dans aucune variable SIF utilisée dans le programme d'application de sécurité; et

g) le programme d'application de sécurité ne dépend d'aucune variable non liée à la sécurité dans la mise en œuvre des SIF;

h) l'ensemble du programme d'application de sécurité (y compris les variables et les données) est protégé contre tout changement du programme d'application non lié à la sécurité; et

i) si les programmes d'application de sécurité et ceux non liés à la sécurité partagent les mêmes ressources (l'UC, les ressources du système d'exploitation, la mémoire, les bus,

par exemple), la SIF (le temps de réponse, par exemple) du programme d'application de sécurité n'est alors jamais compromise.

A.12.2.6 Voir les lignes directrices de A.11.2.8. Si le programme d'application n'inclut pas de réinitialisation manuelle, il convient que la SRS le précise.

Ce paragraphe traite du danger qui peut être créé si l'alimentation du SIS est coupée et si la restauration de l'alimentation n'arrive pas à maintenir le processus à l'état de sécurité. Voir également A.11.2.8 et 12.2.5 de l'IEC 61511-1:2016 . En cas d'activation pour déclenchement, voir également l'IEC 61511-1:2016 , 11.6.2.

A.12.2.7 Aucune autre ligne directrice n'est fournie.

A.12.2.8 Aide à réduire la complexité du programme d'application et garantit que l'ensemble des entrées et des sorties est adressé à chaque analyse. Voir aussi l'ISA TR84.00.09. Il aide également à garantir que les exigences en matière de temps de réponse sont satisfaites (voir l'IEC 61511-1:2016 , 10.3.2).

A.12.2.9 Garantit que le bon programme d'application est utilisé. Il convient de considérer le stockage et la récupération sécurisés, ainsi que la durée pendant laquelle il convient de stocker les anciennes versions, en fonction des exigences opérationnelles et des régulations. Il convient également de veiller à conserver les matériels et les logiciels intégrés nécessaires à l'exécution d'anciennes versions du programme d'application. Avant la mise en œuvre d'une modification dans le programme d'application, il convient de vérifier que le programme d'application en fonctionnement dans la machine est identique à l'exemplaire d'origine. Avant de restaurer les données utilisateur, il convient de vérifier que la version des données utilisateur est la bonne. Voir 5.2.7.

A.12.2.10 Aucune autre ligne directrice n'est fournie.

A.12.3 Lignes directrices relatives à la "Conception du programme d'application"

A.12.3.1 Les modes de fonctionnement peuvent inclure des fonctions d'exploitation manuelles, semi-automatiques, automatiques, de démarrage, par lot, d'essai et de maintenance. Voir l'Article F.14 et l'Article F.27.

A.12.3.2 Pour des exemples d'entrées de la conception du programme d'application, voir l'Article F.13. Pour un exemple de SRS pour le SIS, voir l'Etape F.3. Un exemple de méthodes et d'outils utilisés pour le développement de la conception du programme d'application est donné à l'Article F.20 et à l'étape F.3.

Il peut être nécessaire que le programmeur de l'application et que les concepteurs du SIS discutent des entrées de la conception du programme d'application.

A.12.3.3 Pour faciliter la FSA, il convient que le programme d'application soit traçable jusqu'à la spécification des exigences de sécurité du SIS. Par exemple, il convient de le structurer de telle façon qu'il montre comment les SIF sont mises en œuvre; il convient en outre que les identifiants reflètent l'installation pratique – à l'aide de noms de balise d'entrée/sortie "du monde réel". Il convient également d'annoter le programme d'application pour refléter les fonctions de processus. Voir aussi 5.2.6 de l'IEC 61511-1:2016 et les exemples de la Figure F.11. Il convient que la conception du programme d'application décrive l'appareil et les sous-systèmes SIS du programme d'application, leur interconnexion et la manière d'obtenir les attributs exigés, en particulier l'intégrité de sécurité. Des exemples d'appareils de programme d'application incluent les fonctions d'application qui sont répliquées dans tout le programme (des séquences de commande de pompe, par exemple), l'échange d'informations avec l'E/S de l'installation et les modules de communication, les fonctions au niveau du programme d'application qui interagissent avec les appareils programmables électroniques sous-jacents (l'utilisation de plusieurs SIS pour obtenir les fonctions

redondantes et/ou le comportement en cas de détection d'une erreur et/ou les séquences de démarrage/d'arrêt, par exemple).

L'exécution d'une FSA du programme d'application facilitera l'identification précoce des erreurs, mais permettra également de vérifier que le programme d'application est robuste face aux défaillances. La FSA d'un programme d'application peut inclure:

a) la confirmation que le programme d'application respecte les contraintes du manuel de sécurité, les normes de codage spécifiques de l'application et les pratiques d'une programmation sûre;

b) l'analyse de défaillance du comportement du programme d'application, qui implique d'identifier les fonctions exécutées par le programme d'application, leurs éventuels écarts fonctionnels (dans un HAZOP chimique – trop grand/petit, trop tôt/tard, contraire/non présent/aucun, par exemple), d'évaluer les effets de la défaillance sur chaque fonction d'application et d'identifier les atténuations qui protègent contre une défaillance fonctionnelle.

NOTE De nombreuses fonctions du programme d'application sont des SIF, et l'analyse de défaillance peut être réalisée dans le cadre de l'analyse de défaillance du système. Toutefois, des fonctions supplémentaires peuvent avoir été identifiées dans le programme d'application ou peuvent l'être pendant l'analyse de défaillance fonctionnelle elle-même, afin d'assurer la protection contre une défaillance de la SIF (commande des pompes, vote sur les entrées de processus telles que le feu et le gaz ou la température et la pression, action à entreprendre en cas de défaillance, par exemple).

A.12.3.4 Des exemples de techniques de conception de programme d'application sont donnés ci-dessous:

a) Voir la Figure F.11, feuille 4, ligne 1;

b) Voir des exemples de programme d'application à l'Article F.20 (Tableaux F.8 à F.14 inclus). Il convient que la structure de programme d'application soit cohérente avec la structure du processus. Par exemple, dans une usine de produits chimiques, il convient de regrouper les programmes d'applications de chaque unité de processus. Dans chaque unité de processus, une séparation est prévue entre l'équipement, de manière à faciliter la compréhension et la maintenance;

c) Il convient de définir le bon ordre d'exécution des réseaux et de la logique au sein de chaque programme, ainsi que la séquence d'exécution et les taux d'exécution souhaités de tous les programmes d'application. Il convient de confirmer que les taux d'exécution des programmes d'application sont cohérents avec les temps de réponse de processus exigés de la SRS du programme d'application;

d) Des exemples de description des modules de bibliothèque normalisés peuvent être trouvés à la Figure F.11, feuille 1;

e) Des exemples de description des modules de bibliothèque spécifiques peuvent être trouvés en B.4.1; il convient de développer et de concevoir de façon personnalisée les blocs de fonctions et les fonctions; des blocs de fonctions conçus de façon personnalisée sont souhaitables, car des opérations répétitives peuvent être programmées, soumises à l'essai et utilisées de façon répétée; il convient que les modules d'E/S et les zones de données de variable de mémoire soient configurés;

f) En règle générale, l'allocation de mémoire est automatique lors de la programmation d'application dans les PLC. L'allocation de mémoire est assurée par partitionnement de différentes parties du programme d'application (alarmes, entrées, sorties, logique de sécurité, logique non liée à la sécurité, espaces vides pour croissance future, par exemple) dans leurs contacts individuels (voir la Figure F.11 pour un exemple). Si le partitionnement doit être manuel, il convient que la gestion de mémoire fasse l'objet d'une attention particulière, par:

   – la distribution de variables équivalentes dans des pages dédiées afin de ne pas mélanger les constantes et les variables, les entrées et les sorties, les variables physiques et les variables intermédiaires;

   – la séparation des types de variables afin de ne pas mélanger les entiers et les binaires;

- le fait d'éviter le multiplexage de types de variables simples dans des types de variables plus complexes, par exemple par l'imbrication de plusieurs variables binaires dans des entiers ou dans des octets, en suivant la règle d'une adresse de mémoire par variable;

g) Un exemple de variable globale d'application pourrait être une alarme de sécurité (une alarme de température élevée, par exemple) modifiée en fonction des éléments qui composent le lot faisant l'objet du processus. Un autre exemple pourrait être la limite d'alarme d'un gaz hautement combustible utilisé dans les systèmes de protection contre l'incendie et les gaz (20 % de la limite inférieure d'explosion, par exemple). Un exemple de protection de l'intégrité pourrait être la fonctionnalité du solveur logique sous-jacent qui peut contraindre la variable globale à être uniquement remplacée par une instruction du programme d'application. D'autres considérations relatives à l'utilisation des variables globales peuvent être consultées en G.3.4.3, G.3.4.4, G.7.2.4, G.7.3.1 et G.7.3.2;

h) Il est souhaitable de séparer les fonctions de sécurité et non sécuritaires dans des programmes distincts, de sorte que l'accent puisse être mis sur les programmes de sécurité et qu'il peut être rapidement démontré que les fonctions non-sécurité n'interfèrent pas avec les fonctions de sécurité; la Figure B.13 donne un exemple d'analyse d'indépendance SIF ou non-SIF; il convient que le SRS spécifie quelle SIF et quelles autres fonctions seront incluses dans un programme donné; il est également souhaitable de limiter la taille des programmes de sécurité à quelques fonctions, afin que le niveau d'intégrité le plus élevé puisse ne pas être appliqué aux fonctions de sécurité essentielles;

i) Les feuilles 1 et 2 de la Figure F.11 donnent des exemples de description d'entrée et de sortie; il convient de développer les noms de balise d'E/S et les variables de mémoire;

j) Les Figures B.6 et B.12 donnent des exemples de spécification de l'IHM SIS;

k) Il convient de définir les variables de communication des systèmes périphériques du SIS; si les variables sont des variables de mémoire, elles devront être assignées aux bonnes zones de données afin que le sous-système de communication du SIS puisse y accéder; il convient que les variables qui peuvent être modifiées par d'autres systèmes externes au SIS soient définies avec précautions et de les placer en priorité dans une zone de lecture/écriture spéciale de la mémoire; la Figure B.13 représente un exemple d'échanges de données entre le SIS et le BPCS;

l) Les diagnostics concernant le capteur et l'élément terminal, ainsi que la philosophie des essais périodiques, sont à définir et dépendront de la redondance du capteur et de l'élément terminal; la philosophie nécessite d'être soigneusement définie et il convient qu'elle comprenne un appareil d'alarme approprié pendant la période d'essai; la Figure F.11 feuille 3 lignes A1 à A6, feuille 4 lignes 4, 6, 8 et 10, feuille 5 lignes 17 à 20 donnent des exemples de mise en œuvre des diagnostics;

m) Il est nécessaire d'aborder avec précaution le traitement et l'enregistrement des alarmes, de même que leur impact sur la réduction du risque. De plus, il est nécessaire d'identifier l'approche de la maintenance prioritaire. Certains utilisateurs exigeront des commutateurs câblés via des points d'entrée numériques pour lancer la maintenance prioritaire, alors que d'autres utiliseront une entrée de données contrôlées au SIS depuis une station d'affichage. Dans tous les cas, des procédures sécurisées doivent éviter toute dérivation/neutralisation indésirable. Voir la Figure F.11, feuille 3, pour des exemples types de diagramme d'alarme. Voir l'Article F.14 et le Tableau F.13 pour la hiérarchisation d'alarme. Voir la Figure F.11, feuille 2, lignes DI1, DI2 et DI3 pour des exemples types d'interfaces opérateur;

n) Des exemples de validation de capteur et de vérification de l'intégrité des données de l'application incluent:

   - les vérifications de données d'E/S hors plage (un transmetteur hors plage, par exemple);
   - la validation des données de communications d'application (un chien de garde externe, des algorithmes de contrôle de redondance cyclique (CRC) externes, par exemple); et
   - la comparaison des valeurs des capteurs et l'alarme d'écart;

o) Les vérifications de configuration du système peuvent être effectuées via des essais structurels (voir 12.5.3 b pour une description détaillée des essais structurels); des

précautions supplémentaires doivent être prises pour vérifier que les noms de balise, etc., sont uniques y compris entre les contrôleurs;

p) Un exemple de contrôle de la complexité est donné en B.3.2.2.1, dans lequel la complexité d'un programme d'application est limitée à l'aide d'une organisation hiérarchique de trois couches de modules (voir également la Figure B.9);

q) La Figure F.11, feuille 3, lignes D01, D02 et D03, feuille 4, lignes 1 et 2 et feuille 5, lignes 12 et 16 à 20 montrent un exemple de gestion des anomalies d'E/S du SIS et des sous-systèmes du SIS;

r) Un exemple d'essai en ligne avec neutralisation automatique serait un essai de course partielle de la sortie physique – voir aussi A.16.3.1.2 et A.16.3.1.3;

s) La Figure B.6 donne un exemple de commutateurs d'interface à maintenance pour les essais hors ligne;

t) Il convient de modifier le SIS hors ligne, la sécurité du processus de modification dépendant généralement des éléments suivants:

   – le blocage de la modification en ligne du programme d'application dans le solveur logique. Cela se produit en principe suite à la neutralisation de la modification du code du solveur logique par des mots de passe et des commutateurs matériels;

   – le blocage de l'accès au lien de téléchargement du programme d'application;

   – les caractéristiques intrinsèques du bureau du programme d'application et de ses fonctionnalités de sécurité imbriquées, y compris le contrôle de la syntaxe, les vérifications de cohérence, la traçabilité et le contrôle de version;

u) Les spécifications des exigences de sécurité du programme d'application sont en général contenues dans un document ou dans un ensemble de documents organisés de manière hiérarchique, afin d'affiner progressivement les exigences en partant de la SRS jusqu'aux spécifications de mise en œuvre les plus détaillées (le mapping de la mémoire, par exemple). La documentation du programme d'application fournie par le solveur logique n'est pas une SRS adéquate pour le SIS.

A.12.3.5 Des considérations pour une conception de programme d'application appropriée comprennent:

a) Voir l'Article F.17 et l'Article F.27.

b) Il convient que le programme d'application mis en œuvre réalise toutes les fonctionnalités décrites dans ses spécifications des exigences de sécurité. En outre, il convient que tous les autres comportements non spécifiés soient identifiés, et qu'ils ne compromettent pas l'intégrité de sécurité.

c) Voir A.12.6 et l'Annexe G pour des lignes directrices afin d'éviter toute ambiguïté. Il convient de mettre en œuvre le programme d'application de manière à aider les opérateurs et les mainteneurs à comprendre et interagir avec le SIS (si exigé). Par exemple, la présentation des alarmes, les temps de réponse exigés, les charges de travail de l'opérateur, etc. Il convient que les fonctions supportent les activités de maintenance, y compris l'utilisation de dérivations.

d) Voir A.12.6 pour des lignes directrices sur l'absence d'erreurs de conception.

A.12.4 Lignes directrices relatives à la "Mise en œuvre du programme d'application"

A.12.4.1 Dans la mesure du possible, il convient que le programme d'application s'appuie sur des modules logiciels éprouvés, qui peuvent inclure des fonctions de bibliothèque utilisateur et des règles bien définies de liaison des modules de programme d'application (voir B.4.3.3.1, B.4.3.3.2.1 et B.4.3.4.1 et la Figure B.9). La Figure F.11, feuille 1, donne un exemple d'une partie d'un programme d'application qui utilise des blocs fonctionnels de bibliothèque proposés par le fournisseur et dont la sécurité a été évaluée.

A.12.4.2 Voir les références suivantes pour présenter la manière dont chaque exigence de la Partie 1 peut être mise en œuvre.

NOTE L'Annexe F est un exemple basé sur la deuxième édition de l'IEC 61508 et de l'IEC 61511.

a) l'origine du programme d'application – bas de la Figure F.11 – bloc de titre;

b) une description de l'objet du programme d'application; Article F.1, Article F.2, Article F.3, Article F.4, ainsi que F.5.1 et F.5.2;

c) aucune autre ligne directrice n'est fournie;

d) aucune autre ligne directrice n'est fournie;

e) la traçabilité jusqu'à la SRS du programme d'application – Tableau F.12;

f) l'identification de chaque SIF et de son SIL – Tableau F.11;

g) l'identification et la description des symboles utilisés, notamment les conventions logiques, les fonctions de bibliothèques normalisées, les fonctions de bibliothèques d'applications – Figure F.11, feuille 1;

h) pour l'identification des signaux d'entrée et de sortie du solveur logique du SIS, voir le Tableau F.9 et le Tableau F.10;

i) lorsque le SIS global utilise des communications, une description du flux d'informations de communication – voir la Figure F.12;

j) une description de la structure du programme, y compris une description de l'ordre du traitement logique des données par rapport aux sous-systèmes d'entrée/de sortie SIS – voir l'Article B.1 – ainsi que les limitations types imposées par les durées d'analyse;

k) si la spécification SIF l'exige, les moyens permettant de s'assurer de l'exactitude des données de terrain et des données envoyées via une liaison de communication – voir la Figure F.11, feuille 5, ligne 17, ligne 18, ligne 19, ligne 20; et

l) pour l'identification de la version et un historique des changements, voir le bas de chaque feuille à la Figure F.4, à la Figure F.5, à la Figure F.6, à la Figure F.7, à la Figure F.8, à la Figure F.9, à la Figure F.10 et à la Figure F.11.

A.12.4.3 Il convient que la réutilisation des fonctions de bibliothèque du programme d'application démontre le bon fonctionnement dans une application similaire, y compris des preuves que les mêmes fonctions de bibliothèque ont démontré un bon fonctionnement dans des conditions d'utilisation similaires. Un exemple de fonction de bibliothèque du programme d'application déjà développée et utilisée dans de nombreuses installations de processus est un module de programme d'application qui exécute les fonctions de démarrage, d'arrêt et de verrouillage présentes dans une fonction de commande de moteur à 3 fils momentanée.

A.12.4.4 Pour construire un programme d'application robuste et fiable, il convient de bien réfléchir à sa structure. Cela pourrait inclure la façon dont la redondance au niveau de l'application est ajoutée à la conception sous-jacente du solveur logique, la façon dont les fonctions sont partagées entre plusieurs E/S (par exemple, la façon dont la commande des vannes est structurée) et l'ordre de traitement des variables d'entrée et de sortie.

A.12.5 Lignes directrices relatives aux "Exigences relatives à la vérification du programme d'application (revue et essai)"

A.12.5.1 Aucune autre ligne directrice n'est fournie.

A.12.5.2 Dans ce contexte, la compétence signifie que la personne a une expérience et une formation techniques professionnelles (une licence, une maîtrise ou un diplôme équivalent, par exemple), qu'elle maîtrise le langage de programmation, la conception et les outils de mise en œuvre utilisés, et qu'elle est forte d'une expérience en matière de programmation d'applications. Il convient en outre que cette personne ait des connaissances sur la sécurité fonctionnelle, en particulier dans le serveur des industries de transformation. Il convient qu'elle puisse reconnaître la logique non sûre inhérente (par exemple, portes OR ou inversions des applications d'état de sécurité Désactiver ou des portes AND des applications d'état de sécurité Activer). Voir Article F.28.

A.12.5.3 Pendant les essais, il convient d'exercer tous les secteurs du programme d'application afin de s'assurer du bon fonctionnement et de garantir qu'un secteur de l'application n'a pas d'impact négatif sur une autre partie du programme. Il convient de vérifier

les données dans toute la plage admise pour garantir que le système fonctionnera correctement dans la plage. Il convient également d'effectuer des vérifications hors plage afin de garantir que les données hors plage sont détectées et que l'action adéquate est prise. Il convient également de procéder à des essais pour confirmer que le programme d'application n'exécute pas des fonctions imprévues susceptibles de compromettre ses exigences de sécurité.

Il convient que la revue du programme d'application inclue des techniques telles que des examens, un contrôle collectif et une analyse formelle. Il convient de lui associer une simulation et des essais, pour donner l'assurance que le programme d'application satisfait à sa spécification connexe.

L'essai peut être de type "boîte noire" (essai effectué sans connaître la structure interne du programme d'application, comme un essai fonctionnel, par exemple) ou de type "boîte blanche" (essai effectué en connaissant la structure interne du programme d'application). Dans les deux cas, il est important de démontrer les résultats d'essai par rapport aux exigences, mais, dans le cas d'un essai de type "boîte blanche", un comportement "inattendu" peut être plus facile à identifier.

Au départ, les essais de programme d'application peuvent avoir lieu sur un simulateur, puis sur le matériel du solveur logique en s'appuyant sur les spécifications produites au stade de la conception et de la spécification des exigences. Le but des phases d'essai initiales (simulation et essais par rapport aux spécifications de conception) est:

a) de démontrer que les modules du programme d'application assurent les fonctionnalités nécessaires et qu'ils ne sont pas en mesure d'adopter un comportement interdit;

b) de soumettre le programme d'application à une large plage de conditions et de séquences pour démontrer qu'il résiste à un comportement imprévu;

c) les essais structurels couvrent trois phases critiques du développement et des essais du programme d'application (unité, intégration et niveaux d'essai du système).

Les essais structurels du programme d'application sont censés mettre à l'épreuve les décisions prises par le programme d'application avec les cas d'essai, en fonction de la structure et de la logique de la conception. Les essais structurels complets mettent en pratique les structures de données du programme d'application (les tables de configuration, les types, les sous-programmes, les fonctions, par exemple), sa logique de contrôle et procédurale aux niveaux d'essai décrits ci-dessous.

Il convient de réaliser les essais structurels aux niveaux d'essai de l'unité, de l'intégration et du système. Comme utilisée ici, une "unité" est l'appareil de code compilable séparément le plus petit – ou son équivalent (une procédure, un sous-programme, une classe, une méthode ou une table de base de données, par exemple). Les essais structurels garantissent que les déclarations et décisions du programme d'application sont totalement mises en application par l'exécution du code. Par exemple, ils confirment que les éléments de boucle du programme d'application se comportent comme prévu à leurs limites de données. Pour un programme d'application configurable, l'intégrité des données dans les tables de configuration est évaluée pour connaître leur impact sur le comportement du programme. Au niveau de l'unité, les essais structurels incluent également l'identification du "code mort", du code auquel aucun chemin de code ne peut accéder pour exécution.

Il convient que les essais structurels d'intégration soient effectués après tous les essais de vérification des unités concernées et avant les essais structurels au niveau du système. La vérification du programme d'application confirme que la sortie de chaque phase du développement du programme d'application respecte (c'est-à-dire qu'elle est cohérente avec) les entrées correspondantes. Les essais de performances confirment que le produit du programme d'application terminal, qui fonctionne dans son environnement et son matériel prévus, est cohérent avec le produit prévu tel que défini dans les spécifications du produit et les exigences du programme d'application.

- Essais structurels au niveau de l'unité

L'unité est compilée et reliée à un pilote et à des éléments de remplacement temporairement utilisés, si nécessaire. Le pilote est un remplacement d'unité réelle qui finira par appeler l'unité à l'essai; si le pilote transmet des données à l'unité à l'essai, il est configuré pour transmettre des valeurs variables de cas d'essai, par exemple la valeur maximale, minimale, nominale et "d'essai de contrainte". Les éléments de remplacement temporairement utilisés sont des remplacements d'unités appelées par l'unité à l'essai. Comme pour le pilote, si les éléments de remplacement temporairement utilisés renvoient des données à l'unité à l'essai, ils envoient également des valeurs de données "d'essai de contrainte" et nominales, selon le cas. Les interfaces des pilotes et des éléments de remplacement temporairement utilisés, y compris leurs noms, sont les mêmes que les interfaces des véritables unités, ce qui permet au jeu d'unités d'être relié sans avoir à modifier l'unité à l'essai.

Les essais structurels au niveau de l'unité peuvent être effectués sur le véritable matériel cible, sur un émulateur ou sur un simulateur du véritable matériel ou, si la situation l'exige, sur un processeur totalement différent. Le dernier cas peut se produire, par exemple, si le véritable matériel n'a aucune disposition pour déterminer les résultats des essais d'une unité, mais si le code est écrit dans un langage d'ordre supérieur. Le programme d'application d'ordre supérieur peut donc être compilé et relié pour s'exécuter sur un autre solveur logique qui prend en charge la lecture des résultats de l'essai dans le cas où le solveur logique cible ne pourrait pas prendre en charge les essais.

Les essais structurels (aussi appelés essais de boîte blanche) sont effectués avec l'élément à l'essai, dans ce cas l'unité, affiché en interne à des fins de détermination de la façon dont il convient que l'élément se comporte – par exemple, pour déterminer les possibles branches de code. Un essai structurel au niveau de l'unité a pour principal objet de vérifier que le programme d'application est conforme à la conception, y compris la logique, l'exactitude des algorithmes et la précision (par rapport à un programme d'application parallèle ou à des calculs à la main), mais également à l'exactitude des unités d'ingénierie des données. Cela exige, pour chaque unité, de procéder à des essais adaptatifs complets, à des essais de programme d'application complets (y compris la vérification de l'absence de code mort) et à des essais de contrainte (pour détecter, par exemple, les conditions de dépassement positif et négatif, mais aussi les valeurs de données de contrôle de boucle nominales et maximales). La conception détaillée est utilisée pour développer les critères d'acceptation.

- Environnement pour les essais structurels au niveau de l'intégration et au niveau du système

  Il est préférable de configurer les essais structurels d'intégration et de système à l'aide du véritable matériel et de l'environnement, dans la mesure du possible. Il y a plusieurs raisons à cela, mais les deux plus importantes sont (a) que le programme d'application peut faire l'objet de certaines subtilités, tant bonnes que mauvaises, qui n'apparaîtront qu'au moment du fonctionnement sur le véritable matériel et (b) qu'il convient que le SIS final, y compris le programme d'application et le matériel prévu, soit validé en fonctionnement sur ce matériel, et il convient que les essais structurels poussent le programme d'application en ce sens. Il y a toutefois aussi suffisamment de bonnes raisons d'effectuer des essais structurels de façon partielle ou complète dans un environnement simulé. Lorsque l'établissement de capacités de simulation est considéré, les deux configurations les plus communes sont d'émuler le solveur logique et de simuler l'environnement ou de simuler le solveur logique et l'environnement. Les principaux avantages d'utiliser une simulation de l'environnement et, dans certains cas, du solveur logique incluent:

  – la capacité à configurer des valeurs d'entrée absolument connues, de sorte que les résultats puissent être prédéterminés pour établir les critères d'acceptation de chaque essai;

  – un simulateur facilite l'établissement d'entrées supérieures, inférieures et exactement égales aux limites des valeurs de données critiques;

  – il est facile de configurer des entrées illégales pour soumettre à l'essai toutes les conditions d'erreurs et de défaillances;

  – les résultats de chaque essai peuvent être facilement consultés.

- Essais structurels au niveau de l'intégration

  Les essais structurels d'intégration combinent des unités cohérentes d'un point de vue fonctionnel de parties de programme d'application vérifiées (avec des parties de programme d'application soumises à des essais structurels au niveau de l'unité) par compilation et/ou assemblage et liaison de ces parties, en même temps que les pilotes et les éléments de remplacement temporairement utilisés nécessaires. La structure est alors chargée dans l'environnement réel ou simulé pour exécution. Cela permet à la personne en charge de l'essai de se concentrer sur le progiciel fonctionnel afin de confirmer son exploitation correcte, y compris les interfaces internes et externes. Une fois l'essai de chaque progiciel fonctionnel terminé, le progiciel fonctionnel suivant peut être soumis à l'essai séparément ou être ajouté (c'est-à-dire, relié) à un progiciel déjà soumis à l'essai. Il convient que les essais de régression (c'est-à-dire, fonctionnement d'un sous-ensemble sélectionné de cas d'essai qui se sont déjà exécutés avec succès) soient effectués sur les progiciels déjà soumis à l'essai afin de confirmer qu'ils ne sont pas affectés de façon défavorable par le nouveau progiciel fonctionnel.

- Approche incrémentale

  L'approche incrémentale des essais structurels au niveau de l'intégration est la meilleure dont disposent les développeurs de programme d'application (par opposition aux tiers et aux personnes en charge des essais de validation, voir ci-dessous), particulièrement si le programme d'application est volumineux ou complexe. Dans cette approche, de petites portions choisies et cohérentes d'un point de vue fonctionnel du programme d'application sont compilées, reliées et soumises à l'essai. Cette approche est utilisée quelle que soit la méthode de développement du cycle de vie du programme d'application, y compris les trois méthodes suivantes. Dans la méthode en cascade, toutes les exigences sont développées, puis la conception est terminée avant que les "fils" sélectionnés soient codés et soumis à des essais structurels. Dans la méthode à spirale, un appareil essentiel du système de programme d'application est présenté, puis les exigences, la conception et le code sont développés. L'essai structurel de l'appareil est réalisé avant de passer à la description et au développement de l'appareil essentiel suivant. Enfin, dans la méthode de développement incrémental du programme d'application, l'ensemble des spécifications et des exigences peut être développé, mais la conception et la mise en œuvre sont développées fonction par fonction.

  Dans tous les cas, si le système d'exploitation a été uniquement développé pour le système à l'essai, il convient que ce système d'exploitation soit d'abord soumis à un essai structurel. Il convient que cette portion du code lui-même soit divisée en progiciels fonctionnellement cohérents si elle est grande et/ou complexe; dans le cas contraire, elle peut être structurellement soumise à l'essai en tant qu'entité. La seconde portion du programme d'application à soumettre à l'essai est en principe la section d'entrée/de sortie unique. S'il y a plusieurs appareils d'entrée/sortie, ils peuvent être soumis à des essais structurels séparés. Il est toutefois souvent préférable de sélectionner un fil qui inclut la capacité à faire entrer les données et à voir la sortie qui en résulte pour chaque essai structurel. La troisième étape consiste à sélectionner et à soumettre à un essai structurel une portion structurellement cohérente de l'application et des utilitaires nécessaires pour prendre en charge cette application. Ensuite, sélectionner la prochaine portion cohérente d'un point de vue fonctionnel du programme d'application et les utilitaires d'application associés pour le prochain essai structurel, et ainsi de suite. Il convient que toutes les fonctions précédemment soumises à l'essai soient soumises à des essais de régression, suivant les cas.

Pendant la revue, il convient de vérifier le format des données dans le programme d'application, quant à:

- l'exhaustivité (par exemple, toutes les fonctions de sécurité ont été mises en œuvre et tous les états de chaque fonction de sécurité ont été considérés);
- la cohérence intrinsèque (la même cohérence a été utilisée dans tout le programme, ce qui garantit la clarté et le caractère explicite de la logique de sécurité, ainsi que sa séparation visuelle de la logique non-SIF comme la création de rapports de statut, etc.);
- la protection contre les modifications non autorisées (il convient, par exemple, d'appliquer deux niveaux de protection, l'un au niveau de la station de programmation d'application

pour garantir que le code source de l'application n'est pas modifié sans autorisation appropriée, et l'autre pour garantir qu'un programme d'application ne peut pas être téléchargé dans le SIS sans autorisation appropriée);

- la cohérence avec les exigences fonctionnelles (garantir que chaque exigence fonctionnelle a été correctement interprétée, par exemple);
- la cohérence avec les structures de données (garantir que les structures de données sont lisibles et que le même format est utilisé dans tout le programme d'application, par exemple);
- la compatibilité avec le logiciel intégré de base (par exemple, séquence d'exécution, durée d'exécution, etc.);
- les valeurs de données correctes (les types de données corrects – entier, virgule flottante, booléen, etc. – ont été utilisés, par exemple);
- le fonctionnement dans un périmètre de sécurité connu (vérification de plage au sein même de l'application, pour s'assurer que les valeurs restent dans la plage prévue et qu'elles sont soumises à l'essai, par exemple);
- avoir la capacité de faire des modifications sûres.

Il convient également de vérifier le programme d'application pour s'assurer que les paramètres modifiables sont protégés contre:

- des valeurs initiales non valides ou non définies (garantir que toutes les valeurs modifiables qui peuvent être saisies ont une valeur par défaut, afin de s'assurer que le programme d'application reste dans la plage si aucune valeur n'est saisie par l'utilisateur, par exemple);
- des valeurs erronées (par exemple, fournir une alarme ou arrêter si une valeur passe en dehors de la plage soumise à l'essai ou attendue par le processus);
- des changements non autorisés (garantir que des changements non autorisés ne peuvent pas être apportés par un utilisateur ou qu'une valeur ne peut pas être modifiée suite à une anomalie dans un autre système, par exemple);
- corruption de données. la corruption des données (par exemple, assurer que les données ne peuvent pas être corrompues par un autre système ou une autre tâche non liée à la sécurité).

Il convient de vérifier les communications, les interfaces de processus et le programme d'application associé afin de détecter une défaillance et d'assurer la protection contre la validation de données de corruption de message, sauf si cela a été traité via un appareil conforme à l'IEC 61508.

Il convient que le temps de réponse de l'application soit vérifié pour toutes les fonctions de sécurité afin de garantir que l'itinéraire des données dans l'application est tel que le temps de sécurité du processus peut être satisfait. Par exemple, l'agencement logique peut signifier qu'il convient que le programme d'application passe par plusieurs cycles avant que la fonction de sécurité ne soit résolue.

A.12.5.4 Aucune autre ligne directrice n'est fournie.

A.12.5.5 Dès le début des essais formels, il convient que tous les changements apportés aux fonctions du programme d'application et aux données de configuration soient mis en œuvre de manière stricte, selon une procédure de modification définie.

A.12.5.6 Aucune autre ligne directrice n'est fournie.

A.12.6 Lignes directrices relatives aux "Exigences relatives à la méthodologie et aux outils du programme d'application"

A.12.6.1 Voir l'IEC 61508-3:2010, Annexe D et l'ISA TR84.00.09 pour d'autres lignes directrices. Voir également l'Annexe G pour des considérations supplémentaires. Il convient que le programmeur ne fasse pas d'hypothèse, en dehors de celles définies par le manuel de sécurité, par exemple, ne pas utiliser les capacités d'un compilateur qui ne seraient pas mentionnées dans le manuel de sécurité. Dans le meilleur des cas, le compilateur aurait été configuré pour imposer ces restrictions.

Pour certains systèmes PE, la plage complète de fonctions de configuration peut inclure des fonctions de commande générale qui dépendent d'algorithmes dont il est difficile de prouver qu'ils répondent toujours de façon prévisible – par exemple, des fonctions qui utilisent des algorithmes qui ne s'arrêtent pas de façon fiable (par exemple, récursion) ou qui pourraient provoquer des exceptions dans l'exécution du programme (par exemple, "tan 90 degrés"). Pour ce type de système, le fabricant fournira normalement un "Manuel PE" afin de définir quelles fonctions peuvent être utilisées pour les applications de sécurité. De plus, quand des systèmes PE d'usage général sont utilisés, il peut être nécessaire de limiter la façon dont les outils sont utilisés afin d'éviter des outils dont il est connu qu'ils présentent des erreurs lors de leur fonctionnement (cela peut souvent être observé dans des forums de discussion), mais aussi pour limiter la complexité des fonctions de programmation à celles dont il est démontré qu'elles se comportent de façon fiable. Dans ce cas, il sera nécessaire de compléter le manuel PE qui accompagne le système PE par des procédures supplémentaires, afin de contraindre la manière d'utiliser les outils (pour spécifier les bonnes pratiques de programmation, par exemple), d'identifier les fonctionnalités non sûres (les fonctionnalités de langage non définies, les algorithmes non terminés, par exemple), d'identifier les vérifications pour détecter les erreurs de configuration, et de spécifier les procédures de documentation du programme d'application destinées à assurer le caractère prévisible du programme d'application. Si l'architecture du SIS n'est pas définie dans le manuel PE, il convient que les procédures incluent également la façon dont la tolérance aux anomalies sera gérée, par exemple par redondance et diversité. Il convient de savoir s'il convient de définir d'autres contraintes de programme d'application (les chiens de garde, la vérification des données, etc.).

Les instructions et les exemples pour permettre à un groupe de programmeurs de produire des programmes de format et de style similaires peuvent également être proposés comme faisant partie du manuel de sécurité ou comme un document spécifique à l'application. Il convient que ces instructions incluent les détails des algorithmes spécifiques ou des fonctions qui ne doivent pas être utilisés dans les programmes, ces algorithmes ou ces fonctions pouvant avoir comme conséquence un comportement imprévu qui pourrait avoir un impact sur la sécurité.

Des sections types du manuel de sécurité du PE sont:

a) les niveaux d'intégrité de sécurité auxquels l'appareil ou le système est adapté;

b) le comportement prévu de chaque fonction de bibliothèque (c'est-à-dire pour garantir une sémantique et une syntaxe bien définies du langage de programmation utilisé);

c) les règles et les contraintes visant à limiter l'utilisation des fonctionnalités "pas sûres" du langage de l'application et du jeu d'outils;

d) les exigences relatives aux outils et aux langages de programmation et leurs limitations;

e) l'utilisation des chiens de garde imbriqués;

f) des lignes directrices pour le programmeur sur la façon d'utiliser les outils de programmation pour vérifier la bonne utilisation des variables de données. Les autres fonctionnalités à traiter peuvent comprendre le mapping mémoire, des vérifications sur des drapeaux d'état et des vérifications de validité sur des valeurs d'entrée.

A.12.6.2 Il convient d'identifier l'ensemble des méthodes et des techniques utilisées pour développer le programme d'application, et de justifier leur choix.

Un jeu d'outils type qui prend en charge la programmation d'application est donné à l'Article E.1.

Il convient de choisir les méthodes et techniques de manière à réduire le risque d'introduction d'erreurs dans le programme d'application pendant le développement. Les éléments suivants peuvent alors être pris en considération:

- une syntaxe et une sémantique bien définies;
- l'adéquation à l'application;
- la compréhension par le personnel impliqué dans le développement, la maintenance et l'utilisation du système;
- la garantie des propriétés importantes pour la SIF (par exemple, le cas le plus défavorable des temps d'exécution);
- les preuves/justifications d'une utilisation satisfaisante dans des applications similaires;
- les règles et les contraintes visant à limiter l'utilisation des fonctionnalités "pas sûres" de la méthode – pour d'autres lignes directrices, voir les Articles E.2 et E.3;
- un ordre d'exécution et une mise à jour déterministes des éléments de données.

Les méthodes et les techniques de suppression des erreurs incluent une revue, un essai de simulation, une analyse et une preuve analytique – voir aussi 12.5 de l'IEC 61511-1:2016 .

Pour s'assurer que les erreurs restant dans le programme d'application ne donneront pas lieu à des résultats inacceptables, les points suivants pourraient être pris en compte:

- les techniques de vérification et de gestion des exceptions "en ligne";
- l'utilisation de bases de données constructeur externes et de comptes rendus d'erreurs globaux;
- la surveillance des comptes rendus de défaillance du SIS et des problèmes de processus et de leur impact sur le SIS;
- la redondance des fonctionnalités importantes du SIS par enregistrement dans d'autres systèmes;
- l'utilisation d'une copie du programme d'application du SIS pendant la phase de formation.

Les méthodes et les outils pour gérer les modifications incluent le contrôle de configuration et de version, les bases de données de gestion des exigences, la mise à jour des documents conformes à l'exécution, le contrôle des documents et la gestion des changements, la traçabilité et le suivi des responsabilités pour les changements, les suites d'essais automatiques.

Il convient que les outils soient choisis pour mettre en œuvre des méthodes et des techniques destinées à réduire l'erreur humaine dans leur application pratique. Les éléments suivants peuvent alors être pris en considération:

- la connaissance des outils par les membres concernés de l'équipe de développement;
- les preuves/justifications d'une utilisation satisfaisante des outils dans des applications similaires;
- les règles et les contraintes visant à limiter l'utilisation des fonctionnalités "pas sûres" des outils;
- la liste documentée de la version précise de tous les outils et du SIS;
- la compatibilité entre les différents outils et avec le SIS;
- la capacité à générer la documentation du programme d'application;
- le caractère prévisible du comportement du sous-système SIS;

- la compatibilité de l'architecture tolérante aux anomalies entre la conception du programme d'application et le matériel.

Il convient que le langage et que l'environnement de développement d'application PE soient conformes à l'IEC 61508-3:2010, Tableau A.3.

Quand il est décidé d'utiliser des outils qui n'ont pas été fournis dans le cadre du système PE, il convient de prendre en considération la façon dont les attributs suivants peuvent être atteints:

- simplicité de la disposition du programme d'application;
- mise à disposition des commentaires intégrés dans le programme d'application pour expliquer ses fonctions et son comportement prévu;
- la manière dont la couverture des essais peut être optimisée et démontrée;
- la garantie des propriétés importantes pour la SIF (par exemple, le cas le plus défavorable des temps d'exécution);
- l'aide de commentaires appropriés et en langage naturel;
- la compartimentation pour refléter l'application;
- les similitudes avec d'autres programmes d'application connexes.

D'autres méthodes, techniques et outils qui pourraient être considérés comprennent des mesurages (par exemple, couverture d'essai) et l'utilisation de différents outils pour améliorer la vérification d'une ou de plusieurs fonctions (par exemple, outils dos à dos);

Il convient de considérer la disponibilité des outils (pas nécessairement ceux utilisés pendant le développement initial du système) destinés à assurer les services appropriés pendant toute la vie du SIS.

Pour plus de détails sur les caractéristiques de l'environnement de programmation et des outils, voir l'Annexe E.

A.13 Essai de réception en usine (ERU)

A.13.1 Objectifs

L'essai de réception en usine (comprenant souvent un essai d'intégration de programme d'application) a pour objet de montrer que le SIS peut mettre en œuvre toutes les SIF exigées dans le temps de réponse exigé, satisfaire aux autres exigences fonctionnelles de la SRS et ne pas présenter de comportements indésirables prévisibles.

A.13.2 Lignes directrices relatives aux "Recommandations"

A.13.2.1 Un essai de réception en usine (ERU) peut être recommandé pour les solveurs logiques mettant en œuvre des SIF dont la logique d'application est assez complexe ou comportant des dispositions de redondance (1oo2, 1oo2D, 2oo3, etc.).

A.13.2.2 Le point le plus important de l'essai de réception en usine est d'avoir une procédure d'essai bien définie, bien écrite et bien structurée, qui définit la manière de soumettre à l'essai la logique d'application et les éléments à rechercher après chaque étape.

Il convient que le personnel qui exploitera le processus assiste aux ERU, car il donnera une formation préalable sur l'exploitation du SIS. Fréquemment, il peut également proposer de bonnes suggestions ou des perfectionnements intéressants à la procédure d'essai, qui n'ont pas été prévus pendant la conception.

A.13.2.3 Aucune autre ligne directrice n'est fournie.

A.13.2.4 Aucune autre ligne directrice n'est fournie.

A.13.2.5 Lors de l'ERU, il convient de soumettre les interfaces à l'essai (les communications entre le BPCS et le SIS, par exemple).

A.13.2.6 Aucune autre ligne directrice n'est fournie.

A.13.2.7 Aucune autre ligne directrice n'est fournie.

A.14 Installation et mise en service du SIS

A.14.1 Objectifs

A.14.2 Lignes directrices relatives aux "Exigences"

A.14.2.1 Aucune autre ligne directrice n'est fournie.

A.14.2.2 Il convient d'installer le SIS conformément au plan de conception et d'installation. Il convient de passer correctement en revue, avec l'équipe de projet, tous les écarts par rapport à la conception, pour s'assurer que toutes les exigences de conception sont toujours satisfaites. Après avoir correctement installé le SIS, il convient de le mettre en service entièrement et de lancer les activités de validation.

A.14.2.3 Même si l'IEC 61511-1:2016 a abordé la mise en service en une seule phase, il est reconnu que l'application, l'expérience de l'équipe de projet et les nécessités du projet peuvent exiger de procéder à la mise en service en plusieurs phases. La configuration de l'instrument inclut des paramètres qui garantissent son exécution conformément à la SRS ou au manuel de sécurité (amortissement, linéarisation, etc.).

A.14.2.4 Il convient de produire une documentation qui montre la conformité aux configurations exigées (c'est-à-dire les exigences selon la SRS ou le manuel de sécurité).

A.14.2.5 Aucune autre ligne directrice n'est fournie.

A.15 Validation de sécurité du SIS

A.15.1 Objectif

La validation de sécurité du SIS a pour objet de prouver que le SIS satisfait aux exigences indiquées dans la SRS. Il convient que les activités de validation soient achevées avant de mettre le SIS en l'exploitation.

A.15.2 Lignes directrices relatives aux "Exigences"

A.15.2.1 Aucune autre ligne directrice n'est fournie.

A.15.2.2 Il convient d'inclure le plan de validation du programme d'application dans le plan de validation global du SIS ou d'un sous-système SIS.

A.15.2.3 Aucune autre ligne directrice n'est fournie.

A.15.2.4 Si le SIS a déjà été soumis à un essai de réception en usine (ERU), cela peut être pris en compte lors de la validation. Il convient que l'équipe de validation passe les résultats de l'ERU en revue pour s'assurer que tout le programme d'application a été soumis à l'essai avec succès et que tous les problèmes détectés lors de l'ERU ont été corrigés.

Il sera très important de s'assurer qu'il n'y a eu aucun dommage d'expédition/de stockage/de gestion, que tous les capteurs et éléments terminaux sont correctement connectés au solveur logique, que les SIF fonctionnent correctement et que l'interface opérateur fournit les informations nécessaires.

A.15.2.5 Aucune autre ligne directrice n'est fournie.

A.15.2.6 L'étape finale des essais, c'est-à-dire la démonstration que le système intégré fonctionne correctement dans son environnement prévu, avec les appareils physiques et interfaces prévus et selon les procédures de fonctionnement définies, ne peut être entièrement réalisée qu'après l'installation et pendant la mise en service de l'ensemble du système.

A.15.2.7 Aucune autre ligne directrice n'est fournie.

A.15.2.8 Il convient de ne pas utiliser le forçage des entrées et des sorties dans le SIS du PE dans le cadre des procédures d'exploitation du programme d'application.

Il convient que le forçage des entrées et des sorties ne soit pas permis sans mettre le SIS hors service, sauf s'il est complété par des procédures et une sécurité d'accès approuvées par l'installation. Il convient que ce forçage fasse l'objet d'une annonce ou d'une alarme, suivant les cas.

Il convient que les déclenchements de la maintenance prioritaire soient annoncés.

A.16 Fonctionnement et maintenance du SIS

A.16.1 Objectifs

Aucune autre ligne directrice n'est fournie.

A.16.2 Lignes directrices relatives aux "Exigences"

A.16.2.1 Il convient d'établir un plan de maintenance du SIS. Il convient que le plan de maintenance décrive tous les modes dégradés potentiels du SIS provoqués par la maintenance ou une défaillance du SIS. Il convient d'identifier les mesures compensatoires associées à ces modes dégradés et de développer des plans de maintenance. Il convient d'enregistrer toutes les actions de maintenance.

A.16.2.2 La défaillance et/ou la dérivation d'une SIF alors que le processus est en exploitation augmente la probabilité d'un état de processus non sûr. Il convient donc de mettre des procédures en place pour:

- une situation de défaillances de diagnostic, particulièrement le modèle des défaillances, les causes pour prendre des mesures de réductions du risque relatives, tout en prévenant les opérateurs;
- l'identification des mesures compensatoires, ce qui permet une poursuite de l'exploitation à un niveau de sécurité tolérable;

  NOTE 1 Un exemple de moyen de soumettre les diagnostics à l'essai consiste à insérer une erreur artificielle.

  NOTE 2 Le mode de défaillance et l'analyse de l'effet sont des outils importants pour l'analyse de risque. Leur utilisation est recommandée.

- une dérivation due à un essai périodique fonctionnel.

Il convient d'appliquer des procédures d'exploitation et des mesures d'atténuation des risques strictes au démarrage et au retrait de la dérivation (par exemple, l'approbation avant l'application de la dérivation, l'avertissement aux opérateurs quand la dérivation est en place,

l'inspection de la boucle avant le retour à l'état d'exploitation). Il convient de fournir une formation adéquate aux opérateurs.

– les méthodes et procédures utilisées pour soumettre les diagnostics à l'essai. Si l'essai d'insertion d'erreur est réalisé, il convient de tenir compte de l'impact négatif pour s'assurer que la SIF et le SIL du système satisfont encore aux exigences de sécurité fonctionnelle après le retour à l'état opérationnel.

Si les diagnostics indiquent une défaillance via l'essai d'insertion d'erreur, il convient d'effectuer une véritable analyse pour déterminer la raison et l'effet de cette défaillance sur la SIF et sur son SIL, mais aussi d'agir:

a) conformément à la procédure de maintenance pour traiter la défaillance aléatoire du matériel (par exemple, maintenir ou changer l'appareil); ou

b) de revenir à la phase de cycle de vie adéquate et de procéder conformément au processus de gestion des changements afin de traiter la défaillance système (par exemple, erreur de conception non détectée).

A.16.2.3 Les points suivants peuvent être spécifiés:

- les causes de sollicitation qui exigent des mesures compensatoires;
- les instructions d'utilisation des mesures compensatoires; et
- de quelle manière les actions compensatoires amèneront le processus à un état de sécurité, le temps de réponse et les conséquences sur la défaillance de la mesure compensatoire;
- il convient d'appliquer des procédures d'exploitation et des mesures d'atténuation des risques strictes au démarrage et au retrait de la dérivation (par exemple, l'approbation avant l'application de la dérivation, l'avertissement aux opérateurs quand la dérivation est en place, l'inspection de la boucle avant le retour à l'état d'exploitation). Il convient de fournir une formation adéquate aux opérateurs.

A.16.2.4 Aucune autre ligne directrice n'est fournie.

A.16.2.5 Aucune autre ligne directrice n'est fournie.

A.16.2.6 Aucune autre ligne directrice n'est fournie.

A.16.2.7 Aucune autre ligne directrice n'est fournie.

A.16.2.8 Aucune autre ligne directrice n'est fournie.

A.16.2.9 Aucune autre ligne directrice n'est fournie.

A.16.2.10 Aucune autre ligne directrice n'est fournie.

A.16.2.11 Il convient que les procédures d'essai périodique pour les capteurs et les éléments terminaux incluent des essais complets de leur interface au gaz/fluide de transformation. Il convient que l'essai effectué par accès à distance n'ait pas d'impact sur les performances de la SIF.

NOTE Un essai en ligne peut être réalisé en cas d'utilisation d'un appareil intelligent local.

A.16.2.12 Aucune autre ligne directrice n'est fournie.

A.16.2.13 Les hypothèses formulées pendant la détermination du SIL peuvent influencer le SIL du système.

Il convient que le gestionnaire des opérations passe en revue et vérifie les hypothèses faites pendant la détermination du SIL, y compris l'occupation, la probabilité de prévention, les procédures pour éviter ou réduire la sollicitation et les procédures à appliquer en cas d'alarme.

Il convient d'effectuer une nouvelle analyse de risque si ces hypothèses diffèrent de la condition réelle.

A.16.3 Essais périodiques et inspection

A.16.3.1 Lignes directrices relatives aux "Essais périodiques"

A.16.3.1.1 Il convient de choisir l'intervalle d'essai périodique de manière à obtenir la probabilité moyenne de défaillance sur sollicitation comme cela est exigé dans la SRS.

A.16.3.1.2 Les essais périodiques du SIS doivent refléter aussi précisément que possible les véritables conditions de fonctionnement. Il convient d'effectuer les essais périodiques avant toute activité de maintenance normale susceptible de modifier les résultats représentatifs de l'essai.

Il est préférable d'effectuer les essais périodiques sur le SIS en tant qu'essais intégraux, c'est-à-dire qu'il convient de soumettre à l'essai l'ensemble de la boucle du SIS. L'essai périodique peut être effectué en tant qu'essai intégré de bout en bout (c'est-à-dire, en boucle complète) ou à l'aide d'une approche segmentée (série d'essais au niveau de l'appareil en superposition, c'est-à-dire, capteurs, solveurs logiques et éléments terminaux). Il convient que les essais périodiques incluent, sans s'y limiter, la vérification des conditions suivantes:

a) les séquences d'exploitation logique, par exemple comme indiqué par les diagrammes de cause à effet;
b) l'exploitation de tous les appareils d'entrée, y compris les capteurs de terrain et les modules d'entrée du SIS;
c) la logique associée à chaque appareil d'entrée;
d) la logique associée aux entrées combinées;
e) les valeurs initiatrices du déclenchement (points définis) de toutes les entrées;
f) les fonctions d'alarme;
g) la vitesse de réponse du SIS si nécessaire;
h) l'exploitation des modules de sortie du SIS et de tous les éléments terminaux;
i) les fonctions de calcul exécutées par le SIS;
j) le planning et la vitesse des appareils de sortie;
k) le fonctionnement des actions manuelles qui amènent le processus à son état de sécurité;
l) le fonctionnement des diagnostics lancés par les utilisateurs;
m) le SIS est opérationnel après un essai, par exemple une réinitialisation d'une limitation ou d'une neutralisation.

Si un essai en boucle du SIS n'est pas possible pour des raisons de sécurité ou opérationnelles, un essai partiel peut être effectué pour les appareils ou les sous-systèmes qui font partie de la boucle du SIS. Certains éléments peuvent être soumis à l'essai dans les conditions d'exploitation de processus en fournissant une neutralisation du signal d'entrée ou un remplacement d'une action de sortie. Les éléments tels que les vannes de processus, qui provoquent des arrêts de processus, peuvent donc être soumis à l'essai pendant les périodes d'arrêt.

Pour les applications pour lesquelles un essai partiel est appliqué, il est impératif que les procédures d'essai soient écrites afin de garantir que tous les éléments de boucle sont inclus:

- les essais de l'élément terminal pendant l'arrêt de l'unité;
- les essais du SIS en excitant les sorties, dans la mesure où cela est possible pendant les essais "en ligne" (par exemple, relais de déclenchement de sortie, solénoïde d'arrêt, ouverture/fermeture partielle d'une vanne);
- il convient que toute limitation de la période d'essai des éléments terminaux soit prise en considération dans le calcul de la PFD_{avg} de la SIF.

Il convient que tous les chemins qui traversent des architectures redondantes soient soumis à des essais périodiques pour démontrer que tous les canaux fonctionnent correctement, pas seulement les canaux suffisants pour lancer la sortie. Cela exige souvent que des dispositions spéciales soient prises pour faciliter l'essai.

Il convient d'effectuer un essai en boucle de SIS à des intervalles prédéterminés.

Il convient que les parties non couvertes par un essai soient démontrées par d'autres moyens; par exemple, si des défaillances dangereuses ne peuvent pas être détectées par l'essai périodique, il convient que cet élément soit révisé à des intervalles prédéterminés.

Pour les vannes, un essai de course partielle peut être traité comme un essai fonctionnel qui couvre une fraction des défaillances possibles, et non comme un auto-essai avec couverture du diagnostic. Il convient que la fraction détectée soit correctement documentée via une analyse FMEDA (Failure Modes, Effects, and Diagnostic Analysis, Analyse des modes de défaillance, de leurs effets et du diagnostic) ou similaire.

A.16.3.1.3 Il convient que la fréquence des essais périodiques soit cohérente avec les recommandations applicables du fabricant et avec les bonnes pratiques techniques et plus fréquemment, s'il est déterminé que cela est nécessaire, par une expérience d'exploitation antérieure.

Un certain nombre de stratégies sont à utiliser pour choisir l'intervalle des essais périodiques pour une SIF.

Par exemple, certains utilisateurs aiment choisir cet intervalle d'essais périodiques aussi long que possible, pour minimiser le coût de maintenance et l'impact potentiel des essais. Dans ce cas, la conception du SIS peut inclure plus de redondance dans les équipements, une couverture du diagnostic élargie et des appareils plus robustes. A la fin de la conception, un calcul peut alors être exécuté pour déterminer l'intervalle maximal d'essai permis pour atteindre les performances du SIL définies pour la SIF. Le point négatif dans cette philosophie de conception est que chaque système d'une installation aura un intervalle d'essai différent et peut exiger un suivi de conformité plus rigoureux. Elle peut également encourager à concevoir les performances orientées vers la partie inférieure de la courbe de performances (par exemple, $PFD_{avg} = 10^{-1}$ pour les systèmes de SIL 1 et $PFD_{avg} = 10^{-2}$ pour des systèmes SIL 2).

Il convient de noter que PFD_{avg} est une probabilité qui dépend du temps et qui augmente à mesure que le temps passe. Ainsi, pour les intervalles d'essai périodique très longs, il peut devenir très gros, même si en moyenne la cible du SIL est atteinte; il peut également devenir un très mauvais indicateur du risque. Cela peut être inacceptable, mais l'étalement des essais, à certains égards, limite l'impact de ce problème.

D'autres utilisateurs peuvent vouloir normaliser sur la base d'un intervalle d'essai défini et soumettre à l'essai tous les systèmes d'une installation avec le même intervalle d'essai. Par exemple, ils peuvent souhaiter soumettre à l'essai chaque SIF annuellement; ainsi, ils conçoivent chaque SIS en conséquence. Lorsqu'elles présélectionnent un intervalle d'essais périodiques avant de commencer la conception, les sociétés de l'utilisateur peuvent alors présélectionner des architectures, des appareils et la couverture du diagnostic qui satisferont au SIL pour la plupart des applications. Avec ces caractéristiques déjà définies dans leurs normes internes, elles réduisent les coûts des études de conception, pour la plupart des

applications. Dans ce cas, il convient qu'un calcul soit effectué sur le SIS pour s'assurer que les performances de SIL exigées seront satisfaites avec l'intervalle d'essais périodiques présélectionné.

De plus, les arrêts dus à la sollicitation réelle sur le SIS pendant l'exploitation peuvent être crédités en tant qu'essais périodiques (partiels ou complets) dans des conditions données, par exemple:

- l'arrêt documente les informations équivalentes telles qu'elles ont été enregistrées dans l'essai périodique correspondant;
- l'arrêt couvre toutes les parties du SIS; dans le cas contraire, il convient de soumettre à l'essai séparément les appareils ou les sous-systèmes SIS qui ne sont pas activés;
- l'arrêt se produit dans un temps maximal prédéterminé avant le prochain essai périodique planifié, qui peut ensuite être annulé.

Si ces conditions sont remplies, le prochain essai périodique planifié peut être ignoré.

Dans le choix d'un intervalle d'essais périodiques, il convient de considérer le taux de sollicitation, pour les systèmes en mode sollicitation, le taux de défaillances de chaque appareil soumis à l'essai, ainsi que les exigences de performances du système global.

A.16.3.1.4 Aucune autre ligne directrice n'est fournie.

A.16.3.1.5 Aucune autre ligne directrice n'est fournie.

A.16.3.1.6 Aucune autre ligne directrice n'est fournie.

A.16.3.1.7 Aucune autre ligne directrice n'est fournie.

A.16.3.2 Lignes directrices relatives à "L'inspection"

Comme indiqué dans l'IEC 61511-1:2016 , l'inspection du SIS est différente des essais périodiques. Alors qu'un des essais périodiques assure que le SIS fonctionnera correctement, un examen visuel doit valider l'intégrité mécanique de l'installation.

Généralement, l'inspection est faite en même temps que l'essai périodique, mais elle peut être faite plus fréquemment si cela est souhaité.

NOTE 1 L'inspection peut détecter des défaillances naissantes, que les essais périodiques ne trouvent pas.

NOTE 2 Un système, un sous-système ou un composant du SIS en mauvais état est susceptible de présenter un taux de défaillances (λ) plus élevé que l'hypothèse retenue dans le PFD_{avg} et dans les calculs de risque résiduel. Les mauvaises conditions de ces éléments peuvent être résolues.

A.16.3.3 Lignes directrices relatives à la "Documentation des essais périodiques et de l'inspection"

Il est important de documenter les résultats des essais périodiques et de l'inspection pour consigner/archiver ce qui a été trouvé. Il n'y a pas d'exigence spécifique concernant la durée de conservation de ces résultats qu'il convient d'observer; une durée suffisante est toutefois généralement retenue, de manière à tenir compte du réexamen des résultats précédents, pour voir s'il y a un historique de défaillance d'appareil.

Par exemple, si un capteur ne réussit pas à passer un essai périodique, il est de bonne pratique de passer en revue les résultats des essais périodiques précédents, pour voir si ce capteur n'avait pas réussi à passer un essai périodique semblable lors des séries d'essais antérieures. Si l'historique indique des défaillances répétées, il convient d'envisager une reconception du SIS en utilisant un type de capteur différent.

A.17 Modification du SIS

A.17.1 Objectif

La modification s'applique principalement aux changements se produisant lors de la phase d'exploitation du SIS.

A.17.2 Lignes directrices relatives aux "Exigences"

A.17.2.1 Chaque changement apporté au SIS (sous-système ou composants) est une modification, sauf si un remplacement en nature a lieu. Ces modifications peuvent inclure des problèmes relatifs:

- au nouvel intervalle d'essai périodique ou aux procédures;
- aux composants avec différentes caractéristiques, par exemple, au remplacement de composants obsolètes;
- aux changements de point défini;
- aux changements de conditions d'exploitation;
- aux changements de procédures d'exploitation;
- aux changements de micrologiciel ou de logiciel de l'application;
- à la correction des défaillances systématiques;
- à un taux de défaillances plus important que voulu;
- à un taux de sollicitation en hausse.

A.17.2.2 Aucune autre ligne directrice n'est fournie.

A.17.2.3 Dans la mesure du possible, il convient d'éviter de modifier en ligne un programme d'application du SIS. Si des modifications "en ligne" sont exigées, il convient de documenter la procédure complète et de l'approuver, en accord avec la planification de sécurité.

A.17.2.4 Aucune autre ligne directrice n'est fournie.

A.17.2.5 Aucune autre ligne directrice n'est fournie.

A.17.2.6 Aucune autre ligne directrice n'est fournie.

A.17.2.7 Aucune autre ligne directrice n'est fournie.

A.17.2.8 Aucune autre ligne directrice n'est fournie.

A.18 Déclassement du SIS

A.18.1 Objectifs

Aucune autre ligne directrice n'est fournie.

A.18.2 Lignes directrices relatives aux "Exigences"

A.18.2.1 Aucune autre ligne directrice n'est fournie.

A.18.2.2 Aucune autre ligne directrice n'est fournie.

A.18.2.3 Aucune autre ligne directrice n'est fournie.

A.18.2.4 Aucune autre ligne directrice n'est fournie.

A.18.2.5 Aucune autre ligne directrice n'est fournie.

A.19 Exigences relatives aux informations et à la documentation

A.19.1 Objectifs

Pour des exemples de structure de documentation, voir l'IEC 61508-1:2010, Annexe A. Pour plus de détails, voir l'IEC 61506. La documentation peut être disponible sous différentes formes (papier, film ou support de données à présenter à l'écran). Une variété de différents exemples de documentation est fournie dans les annexes à des fins de représentation uniquement.

A.19.2 Lignes directrices relatives aux "Exigences"

A.19.2.1 La liste des informations et de la documentation pouvant être utilisée pour mettre en œuvre un SIS comprend:

a) les résultats de l'analyse de danger et de risque;
b) l'affectation de couche de protection;
c) les hypothèses utilisées lors de la détermination des exigences d'intégrité;
d) les SRS;
e) la logique d'application;
f) la documentation de conception;
g) les informations et/ou la documentation des modifications;
h) les dossiers de vérification et de validation;
i) les procédures de mise en service et de validation du SIS;
j) les procédures d'exploitation du SIS;
k) les procédures de maintenance du SIS;
l) les procédures d'essais périodiques;
m) les résultats des évaluations et des audits.

A.19.2.2 Il convient d'identifier et de documenter les SIS de manière à les distinguer clairement des systèmes non relatifs à la sécurité (le BPCS, par exemple).

A.19.2.3 Aucune autre ligne directrice n'est fournie.

A.19.2.4 Aucune autre ligne directrice n'est fournie.

A.19.2.5 Aucune autre ligne directrice n'est fournie.

A.19.2.6 Aucune autre ligne directrice n'est fournie.

A.19.2.7 Aucune autre ligne directrice n'est fournie.

A.19.2.8 Voir l'Article F.26 pour une liste type des documents fournis avec la conception du SIS.

A.19.2.9 Aucune autre ligne directrice n'est fournie.

Annexe B
(informative)

Exemple de développement de programme d'application de solveur logique de SIS à l'aide d'un diagramme de bloc fonctionnel

B.1 Généralités

L'exemple suivant décrit:

- Une méthode d'organisation des activités liées au développement du programme d'application satisfaisant à l'IEC 61511-1:2016 , 6.3;
- La génération des SRS du programme d'application sur la base de celles satisfaisant à l'IEC 61511-1:2016 ,10.3.2;
- Le développement et la mise en œuvre de deux fonctions d'arrêt dans un programme d'application, satisfaisant à 7.2.2, 11.5.2.3, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6 et 15.2.2 de l'IEC 61511-1:2016 .

B.2 Développement du programme d'application et philosophie de validation

Une méthodologie de développement efficace doit aider les ingénieurs en programme d'application à concevoir des SIF aux performances prévisibles et à l'intégrité de sécurité requise (c'est-à-dire SIL 3).

Les ingénieurs en conception de programme d'application peuvent traditionnellement procéder à un essai complet de la conception du programme d'application uniquement dans la dernière partie de l'effort de conception, quand la véritable architecture matérielle est disponible. Il s'agit d'une méthode très inefficace. En effet, à la découverte d'une erreur à cette étape, ils doivent revenir en arrière à la phase de conception correspondante afin de corriger les erreurs et élaborer une nouvelle version, ce qui entraîne une augmentation considérable du temps et de l'argent investis dans le développement du produit final.

L'approche textuelle traditionnelle de la spécification du programme d'application de sécurité n'est pas assez efficace pour gérer les exigences de sécurité avancées et complexes habituellement présentes dans les spécifications des SIF.

L'outil le plus efficace pour faire face à ces défis est l'ingénierie dirigée par les modèles (IDM). L'IDM est une méthode mathématique et visuelle destinée à résoudre les problèmes liés à la conception de systèmes de sécurité complexes. Elle est actuellement utilisée avec succès dans de nombreuses applications. Elle fournit une approche efficace pour surmonter les difficultés de la phase de développement du cycle de vie de sécurité. Cette approche et cet exemple incluent les étapes suivantes:

- Modélisation de la SRS du programme d'application par:
  - l'identification des éléments du SIS concerné;
  - la description de leur comportement à l'aide d'un langage de modélisation approprié;
- Analyse et synthèse du comportement de la mise en œuvre prévue de la SRS du programme d'application eu égard à leur exécution;
- Démonstration de la conformité de la mise en œuvre du programme d'application avec la SRS afin de documenter le processus de validation et de contribuer à satisfaire à 12.5 et à l'Article 15 de l'IEC 61511-1:2016 .

Cela permet une détection et une correction précoces des erreurs au cours de la conception du programme d'application, lorsque l'impact ponctuel et financier de la modification du

programme d'application est limité. La réutilisation de la conception est facilitée par l'IDM, tant pour la mise à niveau du programme d'application que pour le développement des programmes d'application dérivés aux des capacités étendues. L'IDM offre un environnement de conception commun à tous les développeurs, ce qui facilite la communication générale, l'analyse des données et la vérification du programme d'application entre différents groupes de développement.

La spécification et la simulation par texte ont été utilisées pendant très longtemps, mais elles sont très inefficaces et inadéquates pour traiter avec les caractéristiques avancées et complexes des SIF puisque ces outils sont totalement non graphiques par nature et ne fournissent pas de preuves mathématiques appuyant l'analyse. En raison de la limitation des outils graphiques, les ingénieurs de conception se reposaient fortement sur la programmation basée sur le texte et sur les modèles mathématiques traditionnels. Cela représentait une grande cause d'inquiétude pour garantir l'intégrité de sécurité puisque le développement de modèles dans des programmes basés sur le texte n'est pas seulement difficile et long mais qu'il induit également grandement en erreur. Le débogage du modèle et la correction des erreurs constituaient un processus pénible. Il exige de nombreux cas et séries d'erreurs avant qu'un modèle final d'arbre des défaillances puisse être créé, puisque le modèle fonctionnel subissait des changements invisibles lors du passage du modèle par les différentes étapes de conception. Ces défis sont de nos jours relevés grâce à l'utilisation d'outils de modélisation graphique dédiés pris en charge par les progiciels de développement satisfaisant à 12.6 de l'IEC 61511-1:2016 et couvrant l'ensemble du cycle de vie de sécurité du programme d'application de 6.3.1 de l'IEC 61511-1:2016 . Cela permet de développer un seul référentiel de spécification et de mise en œuvre, ce qui présente l'avantage de pouvoir démontrer les propriétés d'intégrité de sécurité pour un coût très bas comparé aux techniques manuelles. Dans cet exemple, la philosophie générale de développement du programme d'application consiste à suivre des pratiques d'ingénierie dirigée par les modèles.

Les modèles suivants seront réalisés séquentiellement, intégrés de façon incrémentielle et utilisés afin de supporter la conception et la validation:

- Modèles fonctionnels:
  - Modèle d'architecture fonctionnelle matérielle
  - Modèle d'architecture physique matérielle
  - Modèle d'architecture fonctionnelle du programme d'application
  - Modèle d'architecture du programme d'application
- Modèles de propriétés de sécurité:
  - Propriétés de temps
  - Propriétés de l'intégrité de sécurité
- Vérification du modèle.

Ces modèles sont progressivement intégrés afin de démontrer de manière séquentielle la conformité du programme d'application à sa SRS.

Ces modèles sont utilisés pour:

- La conception dans le cadre de la matérialisation de la spécification détaillée de l'intégrité fonctionnelle et de sécurité;
- La production automatique de programme d'application compilé;
- L'essai semi-automatique par vérification du modèle, afin de vérifier si chaque module de programme d'application satisfait à ses spécifications fonctionnelles et de sécurité;
- La validation en fournissant une description détaillée de la couverture et des résultats de l'essai.

B.3 Description de l'application

B.3.1 Généralités

Le présent exemple repose sur une partie d'un SIS pour une installation GNL.

B.3.2 Description du processus

Le processus appuyant cet exemple est une partie d'un terminal gazier (GNL). L'objectif de l'installation est de réceptionner le GNL des navires, de le stocker et de le préparer pour l'injection dans le réseau de distribution de gaz.

B.3.3 Fonctions instrumentées de sécurité

B.3.3.1 Généralités

Le SIS du processus ci-dessus inclut 7 SIL 3 SIF et 64 SIL 2 SIF. L'exemple porte sur une SIF de SIL 3 et une SIF de SIL 2. Les informations données ci-dessous peuvent être considérées comme faisant partie intégrante de la SRS et être utilisées en entrée pour la SRS du programme d'application.

B.3.3.2 SIF 02.01 – Arrêt d'urgence de déchargement GNL

La section du processus concernée par cette fonction est décrite à la Figure B.1.

L'objectif de cette fonction de SIL 2 est d'isoler le navire de l'installation en cas de détection de pression très élevée dans l'un des trois réservoirs de GNL.

La sollicitation sur la fonction se produit lorsqu'une pression très élevée est perçue par un commutateur de pression (les capteurs n'apparaissent pas sur la Figure B.1) dans l'un des trois réservoirs de GNL. La fonction ferme alors 3 vannes (XV1008, XV2008 et XV3008). Si la pression reste très élevée après un certain délai, deux vannes supplémentaires (XV1014 et XV2014) sont fermées. Les vannes doivent rester fermées jusqu'à la réinitialisation, même si le signal indiquant une pression très élevée disparaît.

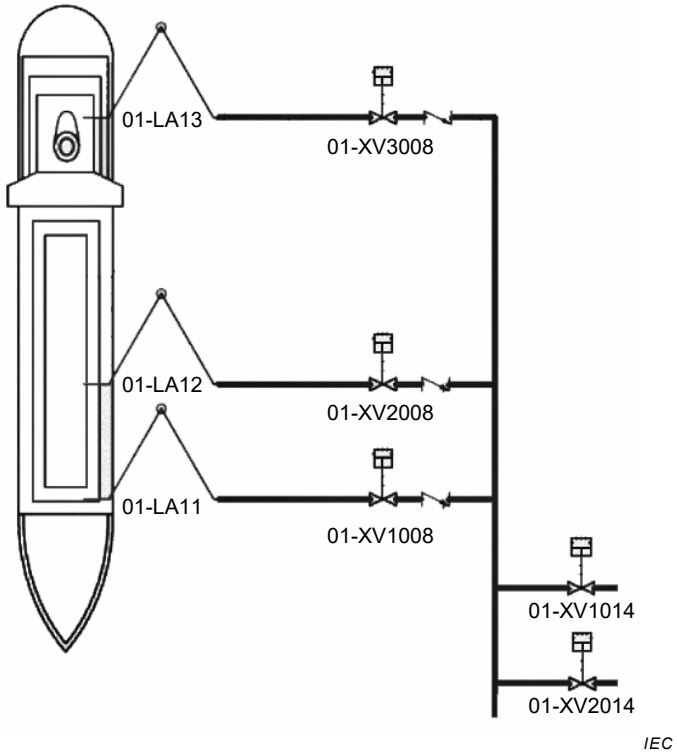


Figure B.1 – Schéma de procédé de la SIF 02.01

B.3.3.3 SIF 06.02 – Fermeture d'urgence de la vanne d'alimentation d'un ORV

La section du processus concernée par cette fonction est décrite à la Figure B.2.

L'objectif de cette fonction de SIL 3 est d'isoler chaque ORV en fermant la vanne d'alimentation XV1001 et la vanne d'isolement XV1013 en cas de détection d'une température très basse (les capteurs n'apparaissent pas sur la Figure B.2) sur le tuyau d'exportation par un thermocontact. Une seule vanne doit être fermée à la fois afin de ne pas piéger le gaz dans le circuit entre les vannes. Les vannes doivent rester fermées jusqu'à la réinitialisation, même si le signal indiquant une température très basse disparaît. La fermeture des deux vannes d'isolation mène à un état dangereux. Eviter cet état dangereux correspond à une assignation de SIL 2.

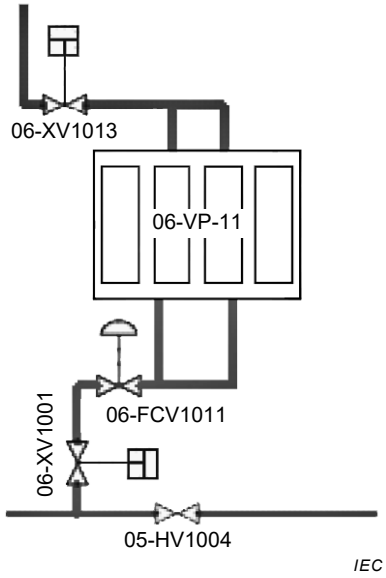


Figure B.2 – Schéma de procédé de la SIF 06.02

B.3.4 Réduction de risque et réaction en chaîne

L'analyse de risque spécifie qu'une sollicitation sur les deux SIF en même temps peut se révéler dangereuse et ne doit pas se produire.

B.4 Exécution du cycle de vie de sécurité du programme d'application

B.4.1 Généralités

L'Article B.4 décrit séquentiellement:

- les entrées nécessaires pour le développement de la SRS du programme d'application extrait de la SRS;
- le développement de la SRS du programme d'application (IEC 61511-1:2016 , 10.3.2);
- la conception de l'architecture du programme d'application (IEC 61511-1:2016 , Article 12);
- la modélisation, la conception et les essais du programme d'application (IEC 61511-1—, 12.3 et 12.4);
- la modélisation et les essais d'intégration du programme d'application (IEC 61511-1—, 12.4 et 12.5);
- la production du programme d'application;
- la contribution à la validation du SIS (IEC 61511-1:2016 , Article 15).

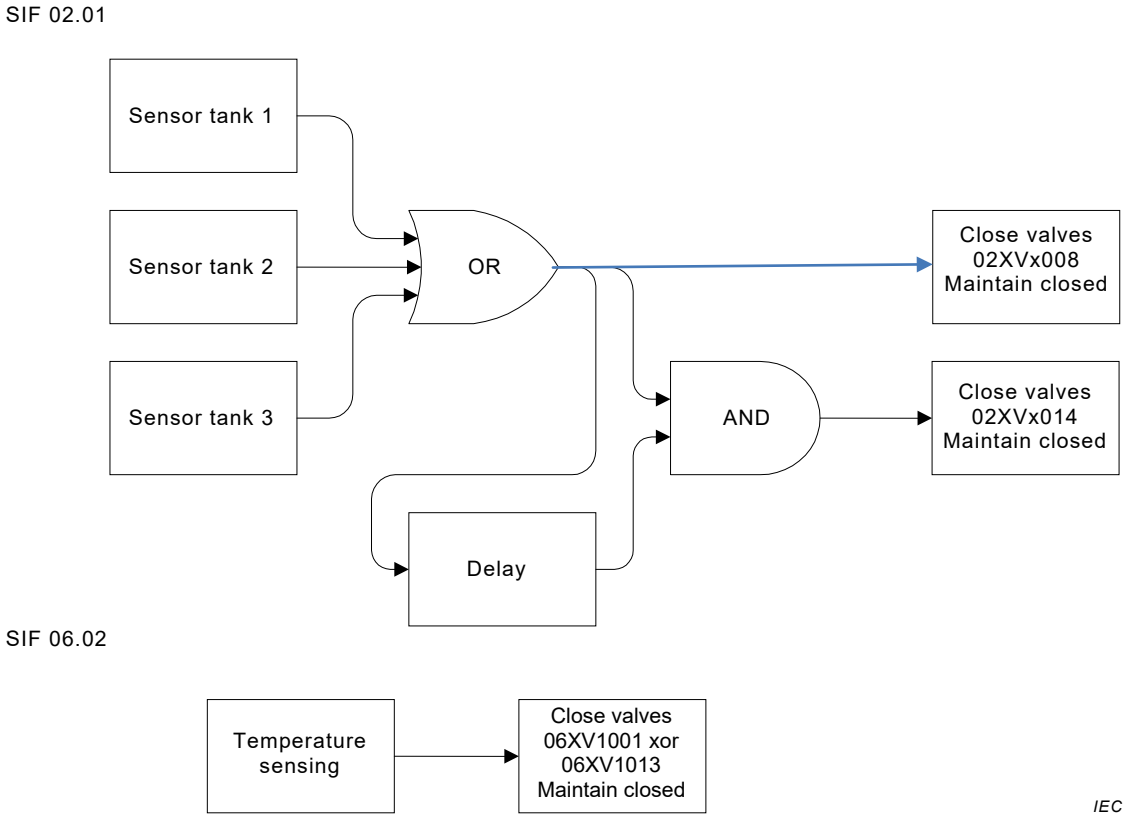
B.4.2 Entrées pour le développement de la SRS du programme d'application

B.4.2.1 Généralités

Les éléments suivants sont les entrées issues des phases précédentes du cycle de vie.

B.4.2.2 Spécification fonctionnelle

La spécification fonctionnelle découlant de l'approfondissement des exigences décrites à la Figure B.1 et à la Figure B.2 est présentée à la Figure B.3 ci-dessous. Ces schémas décrivent le comportement prévu des SIF avant de prendre une décision concernant les futurs matériel et logiciel d'application nécessaires à leur mise en œuvre.



Anglais	Français
Sensor tank	Boîtier de capteur
OR	OU
AND	ET
Delay	Délai
Temperature sensing	Détection de la température
Close valves Maintain closed	Fermer les vannes Maintenir fermé

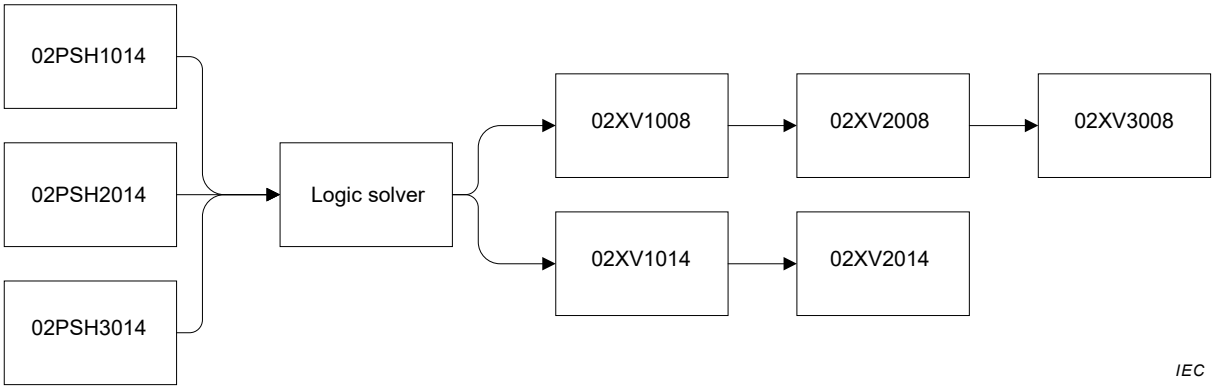
Figure B.3 – Spécification fonctionnelle de la SIF 02.01 et de la SIF 06.02

B.4.2.3 Architecture fonctionnelle matérielle

Les présents diagrammes présentent l'architecture matérielle nécessaire à la mise en œuvre des SIF avant l'application des contraintes de HFT et de toute autre exigence de la SRS.

SIF 02.01

L'architecture fonctionnelle matérielle est représentée à la Figure B.4:

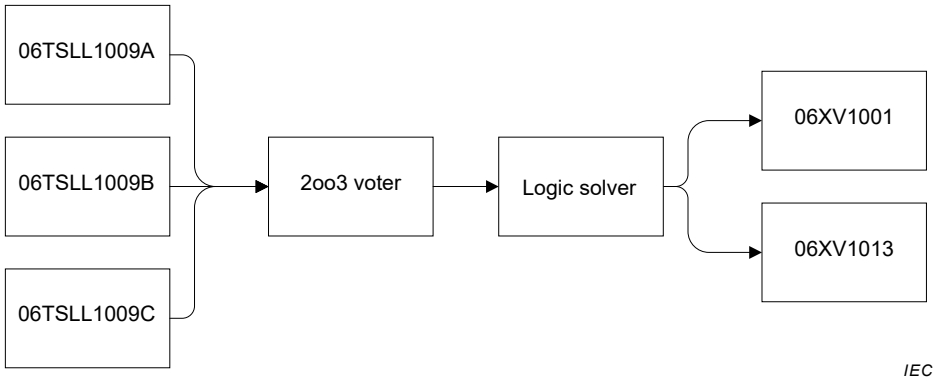


Anglais	Français
Logic solver	Solveur logique

Figure B.4 – Architecture fonctionnelle matérielle de la SIF 02.01

SIF 06.02

L'architecture fonctionnelle matérielle est représentée à la Figure B.5 ci-dessous:

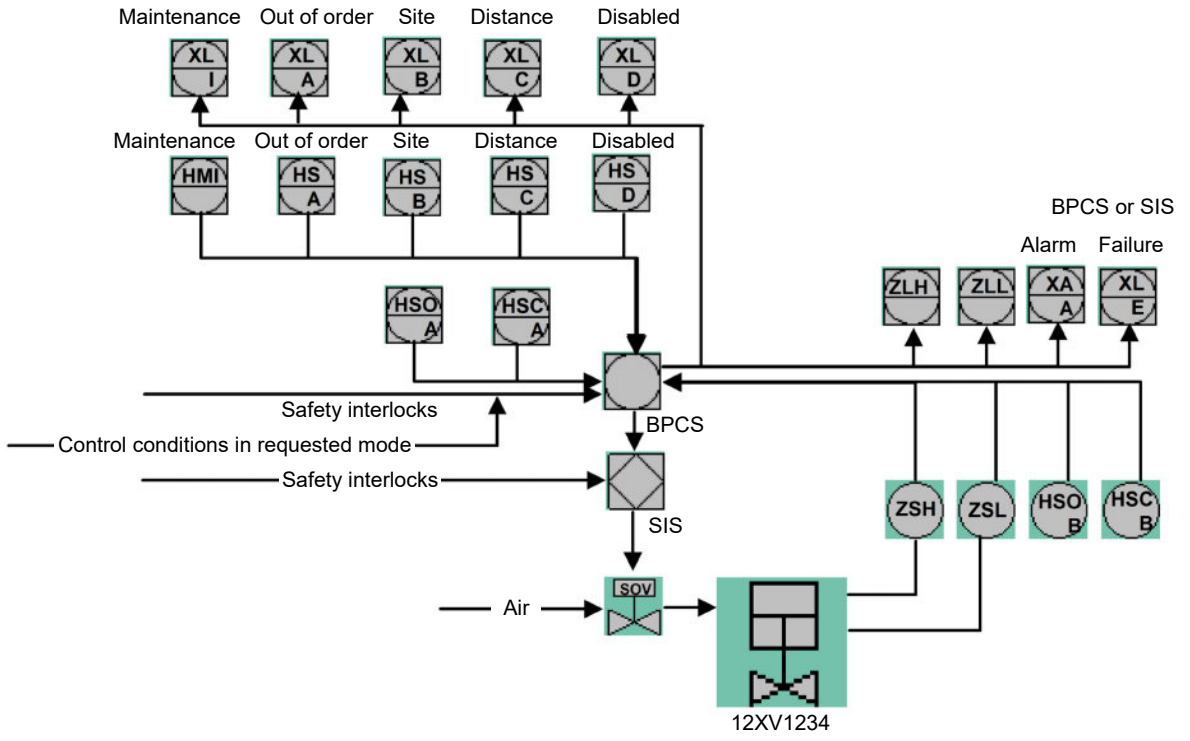


Anglais	Français
2oo3 voter	Appareil de décision 2oo3
Logic solver	Solveur logique

Figure B.5 – Architecture fonctionnelle matérielle de la SIF 06.02

B.4.2.4 Spécification type matérielle pour la SOV/MOV

En général, le schéma de tuyauterie et d'instrumentation décrit l'ensemble des interfaces du matériel et du programme d'application d'un appareil. La Figure B.6 décrit les interfaces du matériel et du programme d'application à mettre en œuvre pour une SOV tant dans le BPCS que dans le SIS.



Anglais	Français
Maintenance	Maintenance
Out of order	En panne
Site	Site
Distance	A distance
Disabled	Désactivé
BPCS or SIS	BPCS ou SIS
Alarm	Alarme
Failure	Défaillance
Safety interlocks	Systèmes de verrouillage
Control conditions in requested mode	Contrôle des conditions en mode requis
BPCS	BPCS
SIS	SIS
Air	Air

Figure B.6 – Spécification matérielle pour une SOV extraite du schéma de tuyauterie et d'instrumentation

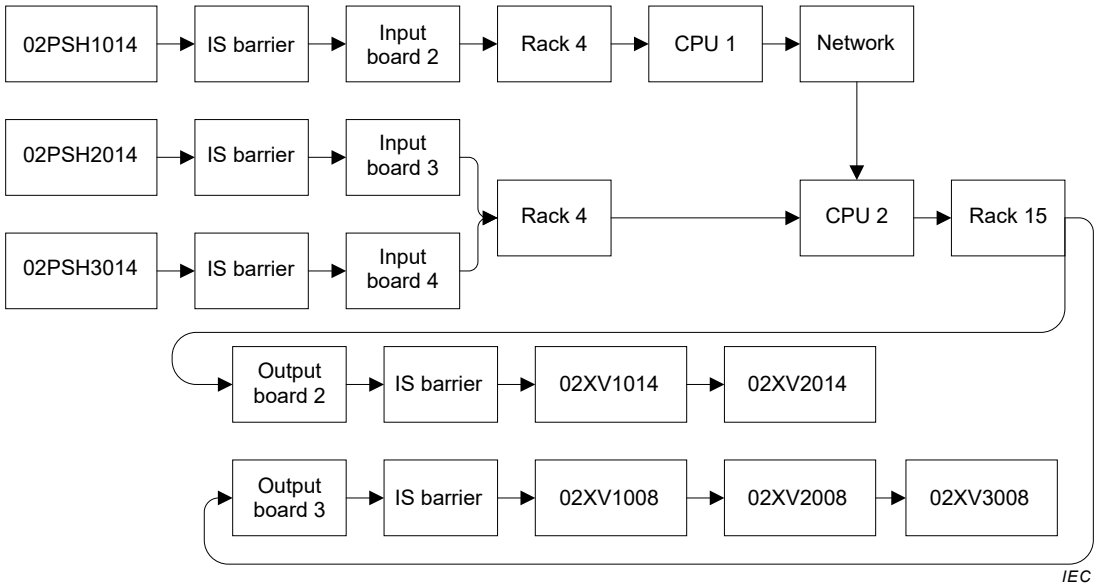
B.4.2.5 Spécification de l'architecture physique matérielle

L'approfondissement des exigences déduites décrites à la Figure B.5 et à la Figure B.6 conduit à la définition du matériel réel à utiliser et à son architecture finale, comme le montrent la Figure B.7 et la Figure B.8.

NOTE 1 La description de l'application des exigences de tolérance aux défauts du matériel, issue des exigences de l'IEC 61511-1:2016 , Article 11, n'est pas présentée ci-dessous.

NOTE 2 Dans le présent exemple, le lien entre le BPCS et le SIS est discret (câblé).

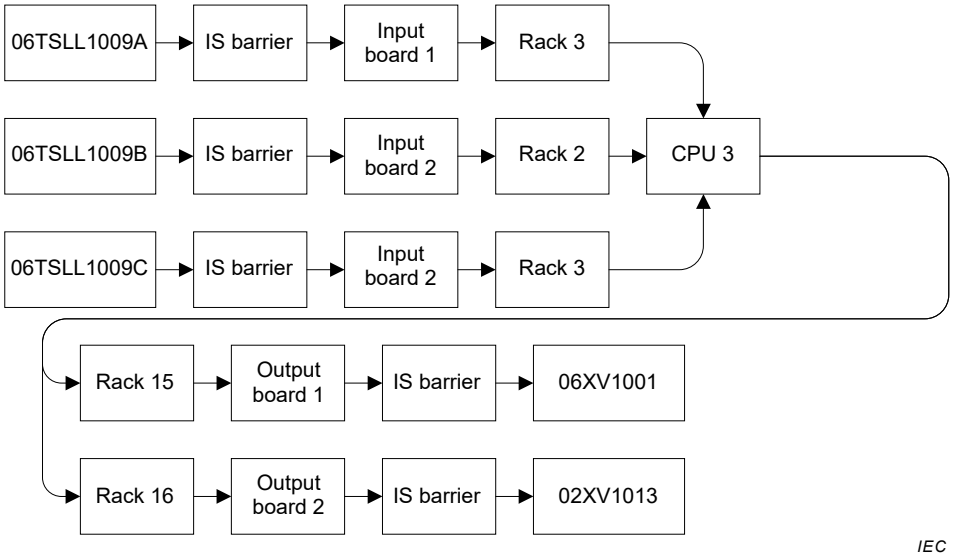
SIF 02.01



Anglais	Français
IS barrier	Barrière SI
Input board	Carte d'entrée
Rack	Baie
CPU	Unité centrale
Network	Réseau
Output board	Carte de sortie

Figure B.7 – Architecture physique matérielle de la SIF 02.01

SIF 06.02



Anglais	Français
IS barrier	Barrière SI
Input board	Carte d'entrée
Rack	Baie

Anglais	Français
CPU	Unité centrale
Network	Réseau
Output board	Carte de sortie

Figure B.8 – Architecture physique matérielle de la SIF 06.02

B.4.3 Conception et développement du programme d'application

B.4.3.1 Généralités

Le Paragraphe B.4 contient des exemples permettant de décrire les étapes suivantes:

- développement de la SRS du programme d'application;
- conception de l'architecture fonctionnelle du programme d'application;
- conception, modélisation et essais fonctionnels du programme d'application;
- modélisation et essais d'intégration du programme d'application.

B.4.3.2 SRS du programme d'application

B.4.3.2.1 Généralités

La SRS du programme d'application peut être organisée comme suit:

- Exigences fonctionnelles correspondant aux comportements prévus:
  - exigences pour les appareils (capteurs et actionneurs);
  - exigences pour les verrouillages de chaque SIF;
  - exigences pour les verrouillages entre les SIF;
- Exigences d'intégrité de sécurité correspondant aux comportements à éviter:
  - au niveau de l'appareil;
  - au niveau de la SIF;
  - à un niveau plus élevé, comme le niveau d'une installation.

B.4.3.2.2 Spécification des exigences fonctionnelles du programme d'application

B.4.3.2.2.1 Exigences fonctionnelles de l'appareil

Les exigences fonctionnelles de l'appareil peuvent être décrites par type d'appareil et organisées selon:

- les modes de fonctionnement génériques de l'appareil; et
- la spécification fonctionnelle de l'appareil.

Le Paragraphe B.4.3.2 donne un exemple pour une SOV.

Modes de fonctionnement d'actionneurs généraux:

Le diagramme d'états pour les modes de fonctionnement d'une électrovanne (SOV, *Solenoid Operated Valve*) est défini ci-dessous au Tableau B.1.

Tableau B.1 – Modes de spécification de fonctionnement

Nom de l'état	Description
Requis	Lorsque les conditions de sécurité génèrent une séquence de sécurité, une commande de la vanne par une logique de niveau supérieur est requise. Cette requête est prioritaire par rapport aux autres modes de fonctionnement. L'appareil est ensuite verrouillé en mode requis. Ses commandes individuelles deviennent indisponibles et la vanne est uniquement commandée par la logique de niveau supérieur. Quand la logique libère les conditions de sécurité, le mode de fonctionnement est forcé sur le mode DISTANCE; l'opérateur est alors libre de changer le mode de fonctionnement.
Distance	La vanne est commandée par l'intermédiaire des commandes d'ouverture et de fermeture de l'interface homme-machine du BPCS. Cela correspond à l'état initial.
Locale	La vanne est commandée par l'intermédiaire de commandes locales d'ouverture et de fermeture par boutons-poussoirs situées à proximité de la vanne.
En panne	Ce mode n'est possible que si la vanne est déjà dans sa position de sécurité. Toutes les commandes de l'opérateur locales comme à distance deviennent indisponibles. La commande par l'intermédiaire des conditions de sécurité reste active.
Maintenance	Ce mode n'est possible que si la vanne est déjà dans sa position de sécurité. La vanne est contrainte de passer à l'état en panne et la totalité des alarmes est neutralisée.

Spécification fonctionnelle d'une SOV:

L'appareil est une électrovanne d'isolation commandée par le SIS et par le BPCS.

Par rapport au danger contre lequel la SIF assure la protection, l'électrovanne dispose par hypothèse d'une position de sécurité unique et non variable. Il s'agit de la position "fermée".

La SOV est un appareil autonome: Elle est équipée de commandes individuelles issues du BPCS et peut, dans des circonstances particulières, être commandée par une logique de niveau supérieur. La logique servant à commander un appareil tel qu'une SOV s'appelle un "type".

Le type pour cette SOV permet de réaliser les actions suivantes:

- commander l'ouverture et la fermeture depuis les postes d'opérateurs du BPCS;
- commander en local l'ouverture et la fermeture sur site grâce au BPCS;
- passer en position de sécurité à l'initiative du SIS ou du BPCS;
- câbler des commandes d'ouverture et de fermeture depuis le SIS;
- sélectionner le mode de fonctionnement depuis les postes d'opérateur du BPCS par un commutateur logiciel;
- réaligner les commandes dans les cas suivants:
  - réaligner des commandes sur les informations des interrupteurs de fin de course lors de l'initialisation;
  - réaligner des commandes sur des appareils de verrouillage logique de niveau supérieur en mode requis;
  - réaligner des commandes sur les commandes sur site en mode sur site;
  - réaligner des commandes sur l'état de sécurité en cas d'action de sécurité;
- traiter l'état de maintenance;
- visualiser l'état de la vanne à partir des informations des deux interrupteurs de fin de course;
- générer une alarme de conflit (lors de l'ouverture ou de la fermeture, détection simultanée des deux interrupteurs de fin de course, de la défaillance de l'interrupteur de fin de course). Pour éviter de générer une alarme de conflit parasite, les informations de

l'interrupteur de fin de course sont différées pour pouvoir transmettre une commande de SIS au BPCS;

- détecter une défaillance du BPCS et du SIS;
- modifier le réglage et les paramètres de réglage.

Paramètres: délai de la détection du conflit.

Accès au niveau de la maintenance uniquement.

B.4.3.2.2.2 Exigences fonctionnelles de la SIF

Les exigences fonctionnelles de chaque fonction de sécurité sont décrites dans la SRS.

B.4.3.2.2.3 Verrouillages entre les exigences fonctionnelles des SIF

Il n'y a aucune exigence fonctionnelle à ce niveau.

B.4.3.2.3 Spécification des exigences d'intégrité de sécurité

B.4.3.2.3.1 Exigences d'intégrité de l'appareil

Les exigences d'intégrité de l'appareil sont les suivantes:

- Aucune combinaison des verrouillages ne doit empêcher les commandes de l'appareil de se mettre en position de sécurité lorsque cela est requis;
- Aucune combinaison des verrouillages ne doit retarder les commandes de la SOV de plus de 100 ms;
- Aucune combinaison des verrouillages ne doit donner lieu à un état indéfini ou instable de la commande de l'appareil physique;
- Toutes les conditions de transition des diagrammes d'état doivent être complètes et exclusives;
- Les actions de chaque condition des machines d'état doivent être définies.

B.4.3.2.3.2 Exigences d'intégrité de la SIF

Les exigences d'intégrité de la SIF sont les suivantes:

- Aucune combinaison des verrouillages ne doit empêcher la fonction de transmettre une requête au type de programme d'application de la SOV lorsque les entrées sont valides;
- Aucune combinaison des verrouillages ne doit retarder une requête à la SOV de plus de 100 ms;
- Aucune combinaison des verrouillages ne doit résulter dans un état non défini ou instable de la commande de l'appareil physique.

B.4.3.2.3.3 Verrouillages entre exigences d'intégrité des SIF

Les exigences d'intégrité de la SIF sont les suivantes:

- Aucune combinaison des verrouillages ou des sollicitations ne doit mener à une sollicitation simultanée sur la SIF 02.01 et la SIF 06.02.

B.4.3.3 conception de l'architecture fonctionnelle du programme d'application

B.4.3.3.1 Conception de l'architecture

L'activité de conception de l'architecture du programme d'application doit garantir que:

- l'architecture obtenue sera conforme à l'IEC 61511-1:2016 , 12.4.4;

- l'architecture obtenue ne dégradera en aucun cas l'intégrité systématique de l'architecture matérielle décrite dans la SRS;

L'architecture du programme d'application s'appuiera sur la structure hiérarchique. Les niveaux et les modules du programme d'application suivants sont pris en considération:

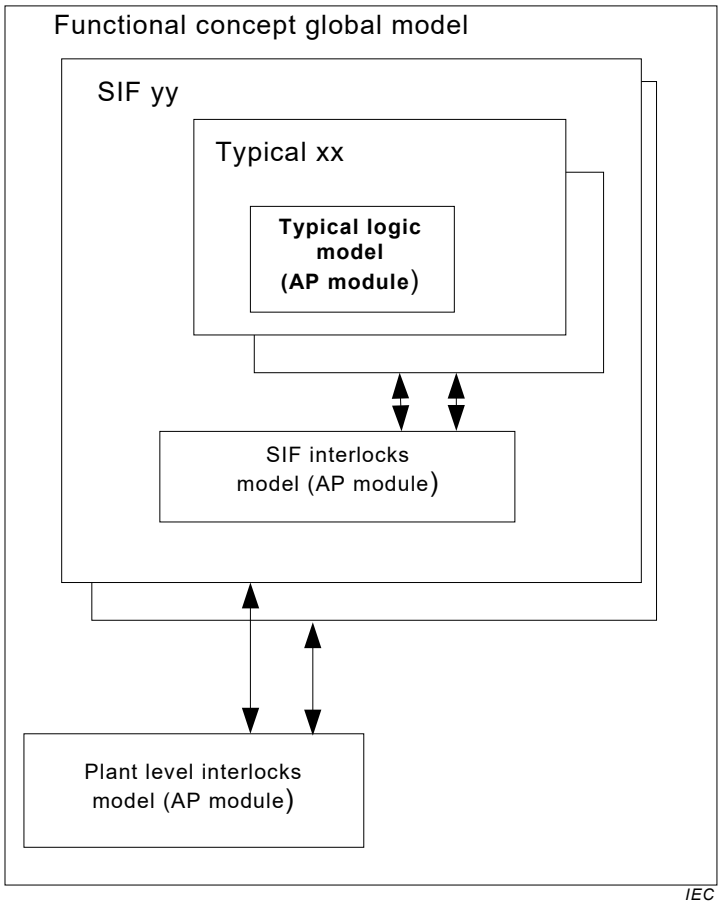
- Les types de programmes d'application pour les appareils: dans cet exemple, les électrovannes et les capteurs de pression et de température seront pris en considération. Ces modules contiennent la logique correspondant à la commande de l'appareil, à l'acquisition et la gestion des entrées, aux fonctions complexes normalisées (le vote, par exemple);
- Logique de la SIF: verrouillage des modules de programme d'application pour réaliser le comportement prévu de chaque SIF;
- Logique de l'installation: verrouillage des SIF.

Ces modules du programme d'application sont décrits au moyen d'un langage graphique de l'environnement du bureau de vérification du modèle de modèles reflétant le comportement prévu des modules du programme d'application à développer. Tous ces modules représentent le programme d'application terminal à produire pour la SIF et peuvent être directement compilés et téléchargés dans les solveurs logiques ciblés.

La liste des modules nécessaires (limités à cet exemple) est la suivante:

- type de SOV;
- vote 2oo3;
- gestion de la communication réseau;
- gestion du capteur;
- logique de la SIF 02.01;
- logique de la SIF 06.02.

Tous les modules sont intégrés ensemble conformément à la structure décrite à la Figure B.9.



Anglais	Français
Functional concept global model	Modèle global du concept fonctionnel
SIF yy	SIF yy
Typical xx	Type xx
Typical logic model (AP module)	Modèle de logique type (module AP)
SIF interlocks model (AP module)	Modèle de verrouillages de la SIF (module AP)
Plant level interlocks model (AP module)	Modèle de verrouillages au niveau de l'installation (module AP)

Figure B.9 – Structure hiérarchique d'intégration de modèle

B.4.3.3.2 Exigences d'intégrité de sécurité déduites de l'architecture

B.4.3.3.2.1 Généralités

Il convient que cette architecture ne remette en aucun cas en question l'intégrité de sécurité systématique de l'architecture matérielle physique définie en B.4.3.3.1.

Ce point n'est pas abordé de manière plus détaillée dans le présent document puisqu'il dépend directement des caractéristiques des solveurs logiques sélectionnés. Mais, au moins, il apparaît que pour la SIF 02.01, il sera nécessaire d'analyser les conséquences de la distribution des modules du programme d'application entre l'UC 1 et l'UC 2 sur l'intégrité systématique de la SIF. Cela requerra d'analyser les combinaisons des modes de défaillances du matériel avec ceux du programme d'application. En règle générale, cette analyse est réalisée à l'aide d'arbres de défaillances qui incluent les défaillances intrinsèques des modules du programme d'application (indépendants du matériel qui les héberge) et dont l'objectif est de déterminer s'il existe un point unique de défaillance qui gêne la HFT.

En outre, la définition de l'architecture du programme d'application permet de définir la SRS de programme d'application déduite qui doit être affectée à chaque module du programme d'application.

B.4.3.3.2.2 Exigences d'intégrité de l'appareil

Exigences dérivées:

- Toutes les conditions de transition des machines d'état doivent être complètes et exclusives;
- Les actions de chaque condition des machines d'état doivent être définies.

B.4.3.3.2.3 Exigences d'intégrité d'une fonction instrumentée de sécurité

Exigences dérivées:

- Aucune combinaison de la valeur dynamique des variables servant d'interface entre les verrouillages d'une SIF et ses modules relatifs ne doit résulter dans un état non défini ou instable d'une SIF.

NOTE Cette exigence ne répète pas celle de B.4.3.3.1. L'exigence de B.4.3.3.1 concerne le comportement statique fonctionnel de la logique. Cette exigence n'a aucun lien avec le comportement dynamique de la logique réparti sur 2 unités centrales et provient de la conception de l'architecture.

B.4.3.3.2.4 Exigences d'intégrité au niveau d'une installation

Aucune exigence dérivée.

B.4.3.4 Conception, modélisation et soumission à l'essai fonctionnelles du programme d'application

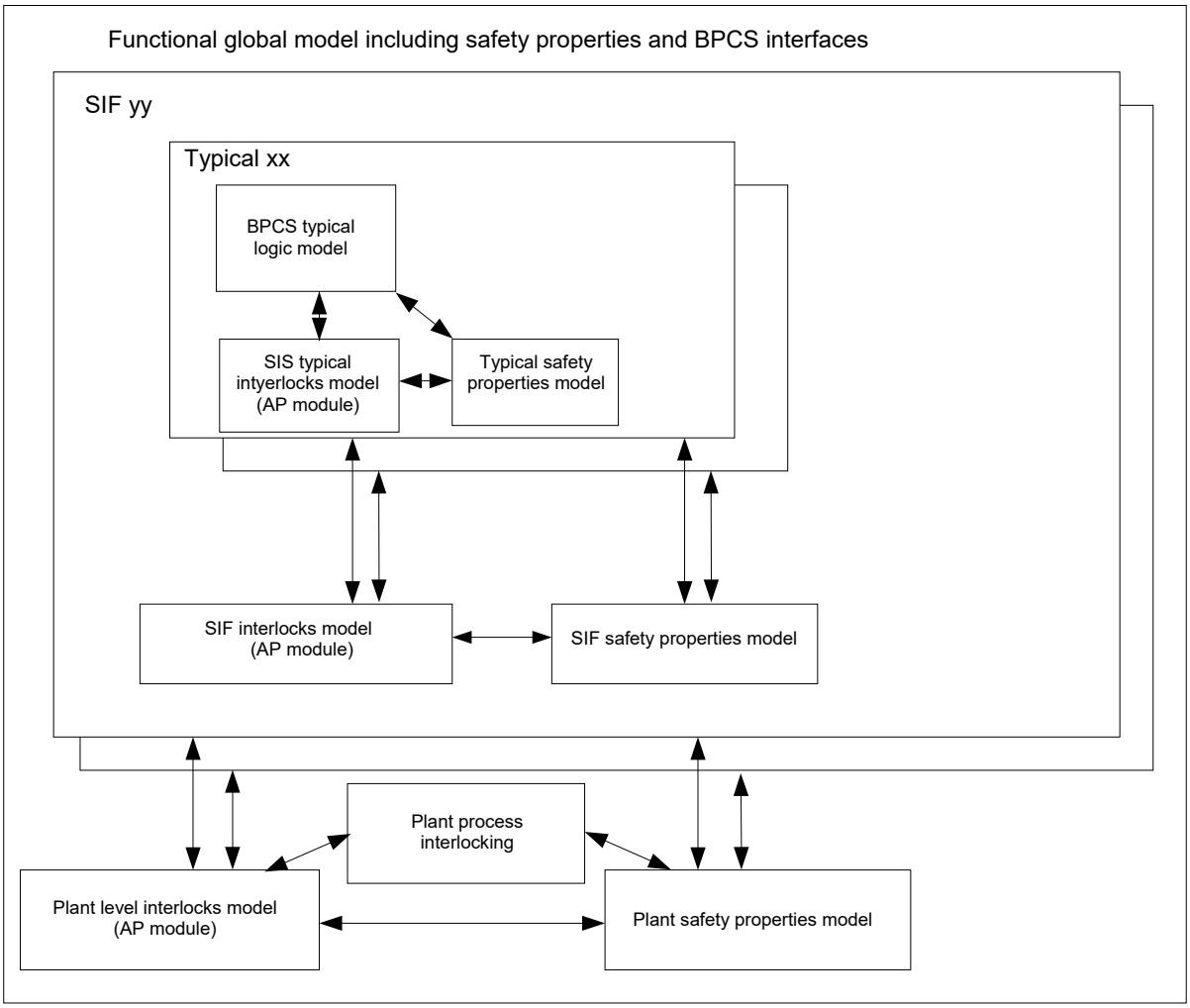
B.4.3.4.1 Conception et essais des modèles fonctionnels des modules du programme d'application

Les modules du programme d'application nécessaires identifiés dans l'architecture du programme d'application sont modélisés dans l'environnement de développement du bureau de vérification du modèle. En parallèle, les modèles sont construits pour décrire les éléments suivants:

- le comportement des appareils physiques;
- le comportement de l'interface homme-machine;
- les propriétés de sécurité exigées des appareils;
- les propriétés de sécurité exigées des SIF;
- les propriétés de sécurité exigées au niveau de l'installation;
- le comportement physique de l'installation (verrouillage par les fluides de processus);
- la partie du BPCS de la logique.

Leur construction est nécessaire pour permettre de prouver l'efficacité des propriétés exigées des SIF modélisées face à leur contexte fonctionnel et physique.

Tous les modules du programme d'application sont intégrés ensemble dans un modèle de vérification fonctionnel conformément à la structure décrite à la Figure B.10.



Anglais	Français
Functional global model including safety properties and BPCS interfaces	Modèle global fonctionnel avec propriétés de sécurité et interfaces BPCS
SIF yy	SIF yy
Typical xx	Type xx
BPCS typical logic model	Modèle de logique type du BPCS
SIS typical interlocks model (AP module)	Modèle de verrouillages type du SIS (module AP)
Typical safety properties model	Modèle des propriétés de sécurité type
SIF interlocks model (AP module)	Modèle de verrouillages de la SIF (module AP)
SIF safety properties model	Modèle des propriétés de sécurité de la SIF
Plant level interlocks model (AP module)	Modèle de verrouillages au niveau de l'installation (module AP)
Plant process interlocking	Verrouillage du processus de l'installation
Plant safety properties model	Modèle des propriétés de sécurité de l'installation

Figure B.10 – Structure hiérarchique d'intégration de modèle comprenant des modèles de propriétés de sécurité et de la logique du BPCS

B.4.3.4.2 Description des modèles

B.4.3.4.2.1 Niveau des types de programmes d'application

Modèle de logique de commande du BPCS de la SOV:

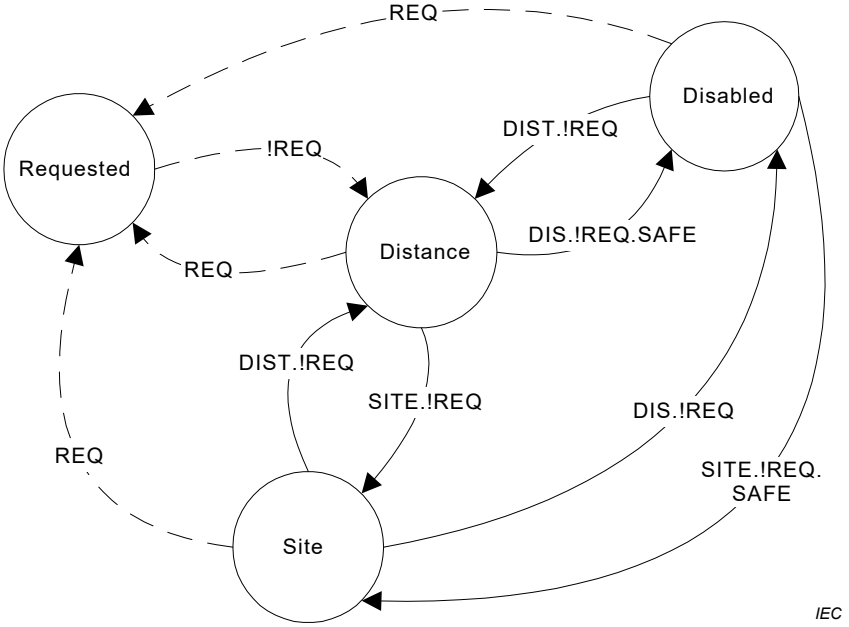
L'approfondissement des modes de fonctionnement des exigences du Tableau B.1 donne une conception détaillée de la logique de commande de la SOV spécifiée par le biais d'un diagramme d'états.

Un exemple de tableau de transition d'état est donné au Tableau B.2.

Tableau B.2 – Tableau de transition d'état

Etats/Etats suivants	Condition de transition	Action
Requis		
Distance	!12HS1234D	
Distance		
Requis	12HS1234D	
Site	12HS1234B ∩ !12HS1234D	
Désactivé	12HS1234A ∩ !12HS1234D ∩ 12ZSL1234	
Site		
Requis	12HS1234D	
Distance	12HS1234C ∩ !12HS1234D	
Désactivé	12HS1234A ∩ !12HS1234D ∩ 12ZSL1234	
Désactivé		
Requis	12HS1234D	
Distance	12HS1234C ∩ !12HS1234D	
Site	12HS1234B ∩ !12HS1234D	

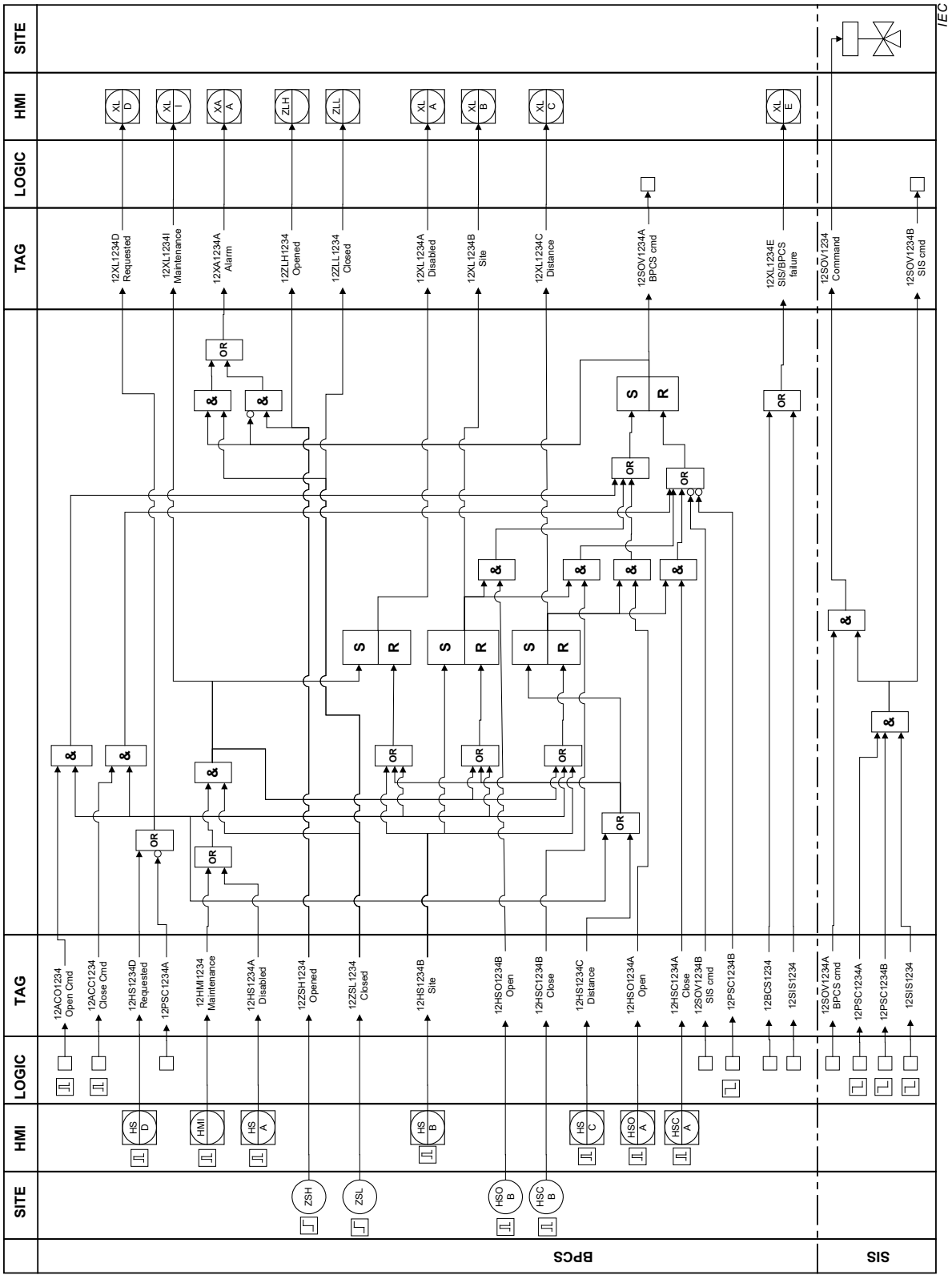
Le Tableau B.2 de transition d'état mène au diagramme de transition d'état représenté à la Figure B.11.



Anglais	Français
Requested	Requis
Disabled	Désactivé
Distance	A distance
Site	Site

Figure B.11 – Diagramme de transition d'état

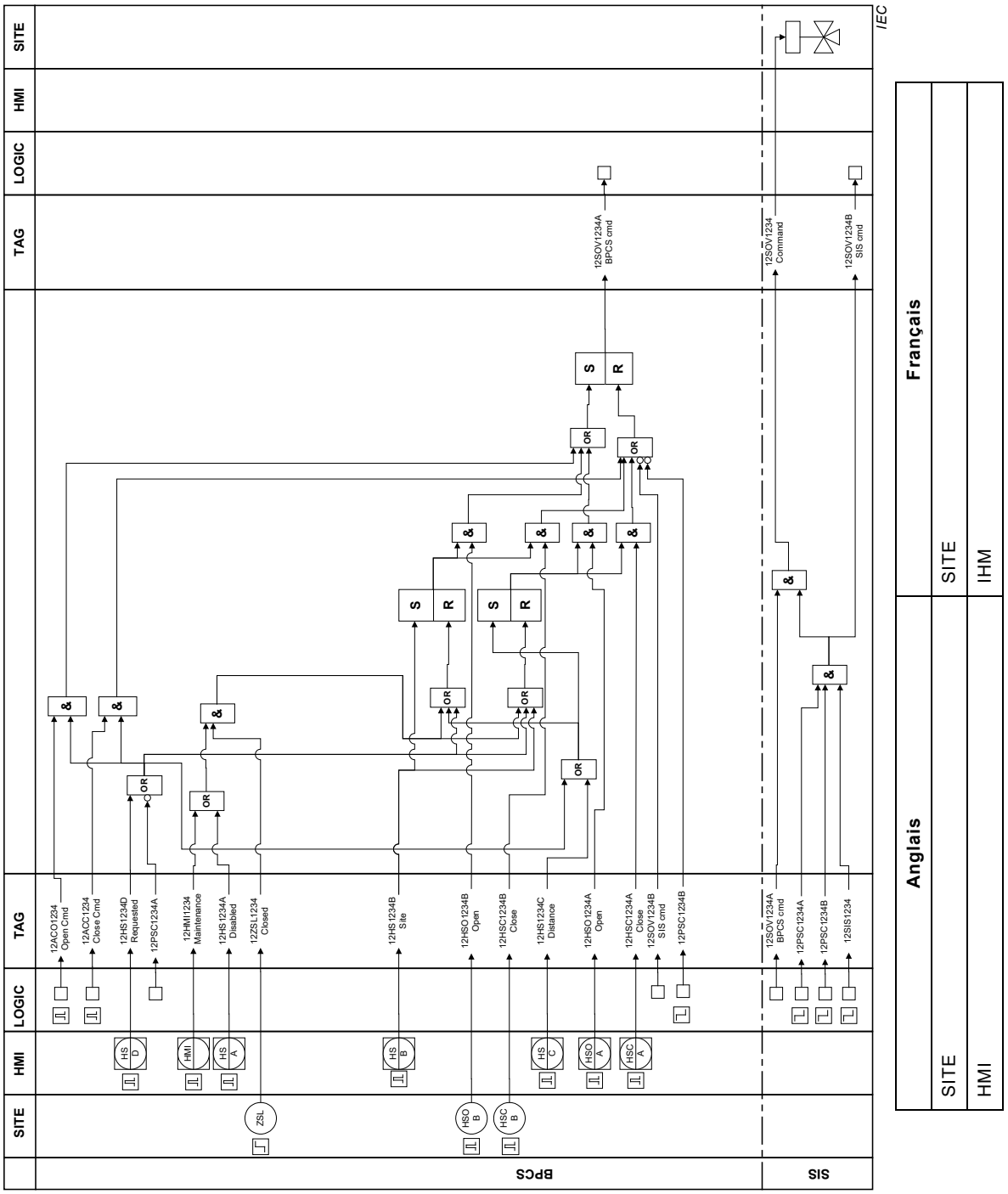
La spécification graphique du comportement de la SOV conformément aux exigences de l'interface de la Figure B.6 et à la Figure B.11 donne la description de blocs fonctionnels de la Figure B.12.


SITE
HMI
LOGIC
TAG
BPCS
SIS
12ACO1234 Open Cmd
12ACC1234 Close Cmd
12HS1234D Requested
12PSC1234A
12HMI1234 Maintenance
12HS1234A Disabled
12ZSH1234 Opened
12ZSL1234 Closed
12HS1234B Site
12HSO1234B Open
12HSC1234B Close
12HS1234C Distance
12HSO1234A Open
12HSC1234A Close
12SOV1234B SIS cmd
12PSC1234B
12BCS1234
12SIS1234
12SOV1234A BPCS cmd
12PSC1234A
12PSC1234B
12SIS1234
12XL1234D Requested
12XL1234I Maintenance
12XA1234A Alarm
12ZLH1234 Opened
12ZLL1234 Closed
12XL1234A Disabled
12XL1234B Site
12XL1234C Distance
12SOV1234A BPCS cmd
12XL1234E SIS/BPCS failure
12SOV1234 Command
12SOV1234B SIS cmd
ZSH
ZSL
HSO B
HSC B
HS D
HMI
HS A
HS B
HS C
HSO A
HSC A
XL D
XL I
XA A
ZLH
ZLL
XL A
XL B
XL C
XL E
&
OR
S
R

Anglais	Français
SITE	SITE
HMI	IHM
LOGIC	LOGIQUE
TAG	BALISE
Open Cmd	Commande ouvrir
Close Cmd	Commande fermer
Requested	Requis
Maintenance	Maintenance
Disabled	Désactivé
Opened	Ouvert
Closed	Fermé
Site	Site
Open	Ouvrir
Close	Fermer
Distance	A distance
SIS cmd	Commande SIS
BPCS cmd	Commande BPCS
Alarm	Alarme
SIS/BPCS failure	Défaillance SIS/BPCS
Command	Commande

Figure B.12 – Diagramme de blocs type de la SOV

Les fonctions et interfaces de l'IHM peuvent ne pas être modélisées, puisqu'elles ne sont que des sorties et n'auront aucun impact sur le comportement de la SOV. La Figure B.12 peut donc être simplifiée dans la représentation de la Figure B.13.

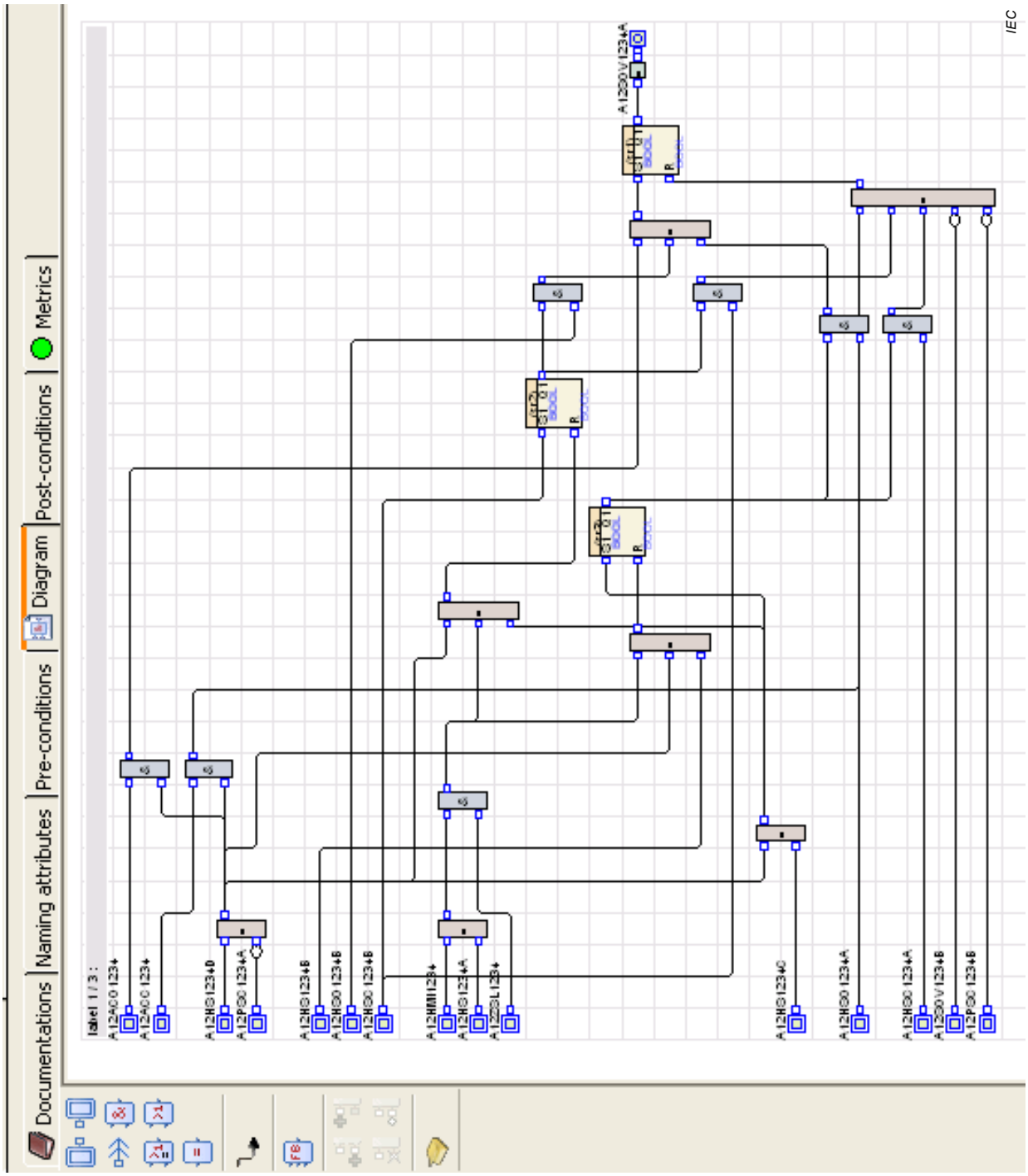


Anglais	Français
SITE	SITE
HMI	IHM

Anglais	Français
LOGIC	LOGIQUE
TAG	BALISE
Open Cmd	Commande ouvrir
Close Cmd	Commande fermer
Requested	Requis
Maintenance	Maintenance
Disabled	Désactivé
Closed	Fermé
Site	Site
Open	Ouvrir
Close	Fermer
Distance	A distance
SIS cmd	Commande SIS
BPCS cmd	Commande BPCS
Command	Commande

Figure B.13 – Diagramme de blocs de modèle type d'une SOV

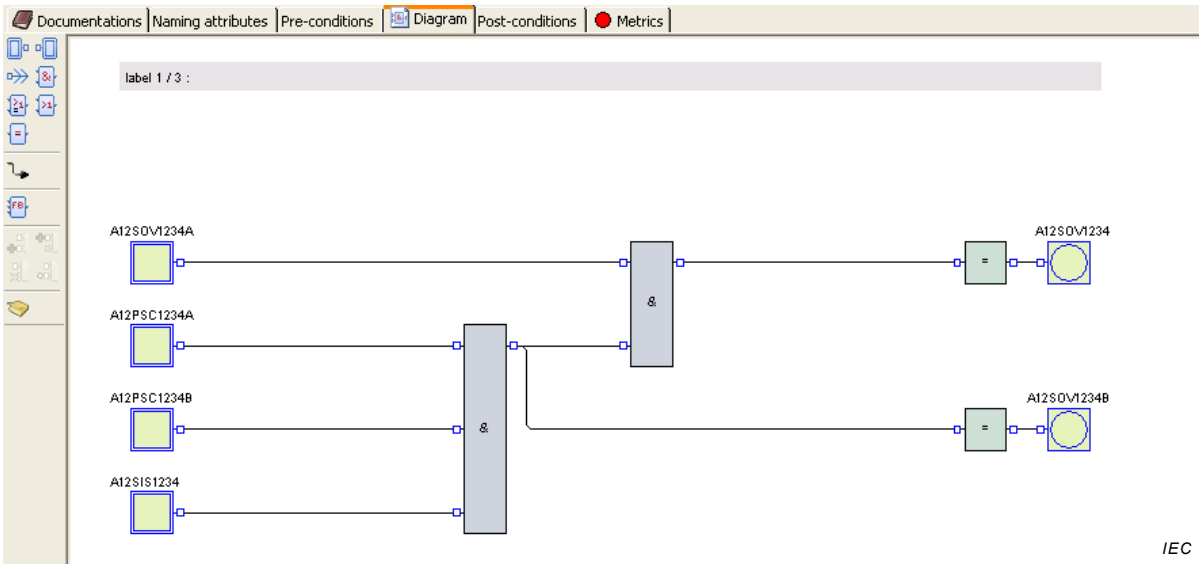
Il convient de mettre en œuvre la spécification de la Figure B.13 dans le langage graphique de l'environnement du bureau de vérification du modèle. La mise en œuvre tient compte du besoin d'isoler la partie de la logique relative au BPCS et la partie relative au SIS. La mise en œuvre aboutit, par exemple, à celle décrite à la Figure B.14 pour la partie du BPCS et à la Figure B.15 pour la partie du SIS. La modélisation de la partie du BPCS est exigée en particulier lorsqu'une interface existe entre le BPCS et le SIS afin de prouver l'indépendance de la SIF par rapport au BPCS mais également d'attester les exigences d'intégrité de sécurité, comme celle énonçant qu'en aucun cas le BPCS ne peut neutraliser la SIF. La plupart des bureaux de vérification du modèle permettent de mettre directement le modèle en œuvre sans avoir besoin de suivre la procédure décrite à la Figure B.12 et à la Figure B.13 indiquée dans le présent document, pour assurer la clarté de la démonstration.


Documentations
Naming attributes
Pre-conditions
Diagram
Post-conditions
Metrics
IEC

Anglais	Français
Documentations	Documentations
Naming attributes	Attributs de dénomination
Pre-conditions	Préconditions
Diagram	Diagramme
Post-conditions	Postconditions
Metrics	Métriques

Figure B.14 – Mise en œuvre du diagramme de blocs de modèle type – partie du BPCS

Mise en œuvre du modèle de logique de commande du SIS de la SOV



Anglais	Français
Documentations	Documentations
Naming attributes	Attributs de dénomination
Pre-conditions	Préconditions
Diagram	Diagramme
Post-conditions	Postconditions
Metrics	Métriques

Figure B.15 – Mise en œuvre du modèle type de programme d'application de la SOV – partie du SIS

Continuation de la modélisation:

La même approche est suivie pour modéliser:

- les propriétés de sécurité de cette SOV;
- les autres types nécessaires qui seraient dans le présent exemple:
  - vote 2oo3;
  - propriétés de sécurité 2oo3;
  - gestion de la communication réseau;
  - propriétés de sécurité de la communication réseau;
  - gestion du capteur;
  - propriétés de sécurité du capteur.

B.4.3.4.2.2 Niveau de la fonction instrumentée de sécurité

La même approche s'applique au niveau de la SIF au modèle:

- de verrouillage SIF 02.01;
- de propriétés de sécurité SIF 02.01;
- de verrouillage SIF 06.02;
- de propriétés de sécurité SIF 06.02.

B.4.3.4.2.3 Niveau de l'installation

La même approche s'applique au niveau de la SIF au modèle:

- de verrouillages de l'installation;
- de propriétés de sécurité de l'installation;
- de l'installation.

B.4.3.4.3 Résultats des essais des modèles et correction des défauts

Les modèles sont exécutés indépendamment par l'outil de vérification de modèle afin de détecter les violations de comportement de sécurité. Si des erreurs sont rencontrées par le vérificateur de modèle, les modèles concernés sont corrigés et réexécutés jusqu'à ce qu'ils ne comportent plus d'erreurs de conception systématiques.

B.4.3.5 Modélisation et soumission à l'essai de l'intégration du programme d'application

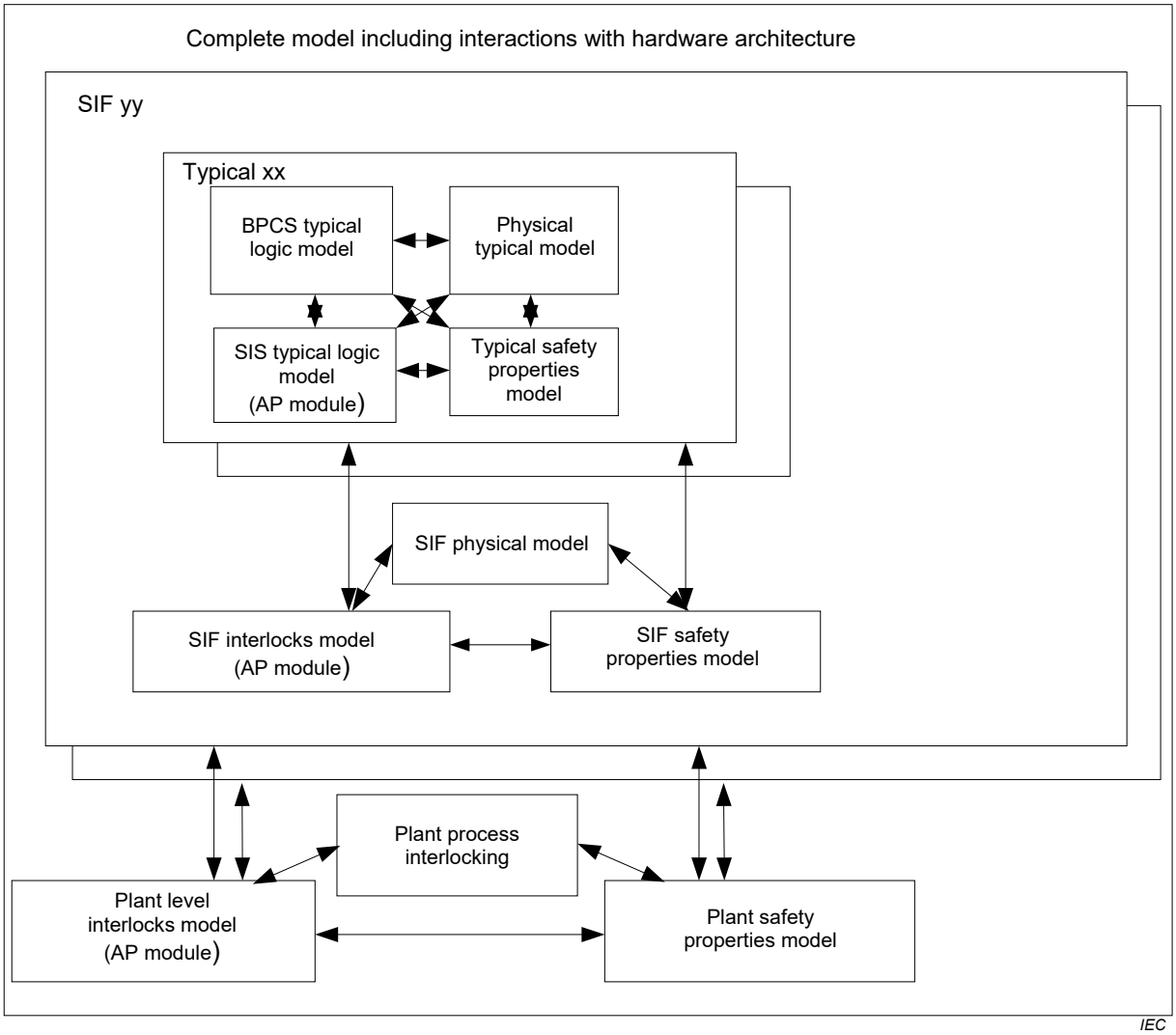
Les étapes précédentes ont permis à l'ingénieur de programme d'application de:

- décrire une architecture de programme d'application;
- décrire le contenu des modules du programme d'application fonctionnel;
- démontrer que les spécifications concernant l'architecture et les modules étaient:
  - conformes aux spécifications fonctionnelles du programme d'application;
  - conformes aux spécifications d'intégrité de sécurité du programme d'application.

Ces éléments ne sont pas suffisants pour démontrer la viabilité du concept de programme d'application lorsqu'il est intégré à l'architecture matérielle physique ciblée, car le comportement fonctionnel du programme d'application dépendra également des caractéristiques de l'architecture matérielle physique.

Cette phase de conception consiste à ajouter des modèles décrivant l'impact de la distribution du programme d'application sur l'architecture physique matérielle ciblée, afin de vérifier s'ils satisfont toujours à la SRS. Si ce n'est pas le cas, les modules du programme d'application et/ou l'architecture du programme d'application et/ou l'architecture physique seraient modifiés. L'étape de la Figure B.10 peut être ignorée si l'architecture matérielle physique est connue tôt au cours du cycle de vie du développement du programme d'application.

Les modèles suivants sont développés et ajoutés au modèle de vérification dans le cadre de la structure suivante, comme le décrit la Figure B.16.



Anglais	Français
Complete model including interactions with hardware architecture	Modèle complet incluant les interactions avec l'architecture matérielle
SIF yy	SIF yy
Typical xx	Type xx
BPCS typical logic model	Modèle de logique type du BPCS
Physical typical model	Modèle type physique
SIS typical logic model (AP module)	Modèle de logique type du SIS (module AP)
Typical safety properties model	Modèle des propriétés de sécurité type
SIF physical model	Modèle physique de la SIF
SIF interlocks model (AP module)	Modèle de verrouillages de la SIF (module AP)
SIF safety properties model	Modèle des propriétés de sécurité de la SIF
Plant level interlocks model (AP module)	Modèle de verrouillages au niveau de l'installation (module AP)
Plant process interlocking	Verrouillage du processus de l'installation
Plant safety properties model	Modèle des propriétés de sécurité de l'installation

Figure B.16 – Modèle complet pour la vérification du modèle de mise en œuvre finale

B.4.4 Production du programme d'application

Certains bureaux de programme d'application permettent la génération d'un code direct téléchargeable à partir des modèles déjà vérifiés. En outre, certains sont conformes à l'IEC 61508.

B.4.5 Vérification et essai du programme d'application

Si un code téléchargeable à partir d'un outil conforme à l'IEC 61508 ou d'utilisation préalable ne peut pas être généré automatiquement, le programme d'application est généré et soumis à l'essai manuellement.

B.4.6 Validation

Pour un programme d'application généré automatiquement à partir des modèles à l'aide d'un outil conforme à l'IEC 61511-1:2016 , 12.6, la validation consiste à vérifier, par une analyse de la documentation du vérificateur de modèle, que toutes les propriétés fonctionnelles et d'intégrité de sécurité décrites dans la SRS du programme d'application ont réellement été démontrées.

Pour un programme d'application généré manuellement, la validation consiste à vérifier que la mise en œuvre suit strictement l'hypothèse des modèles et que toutes les propriétés fonctionnelles et d'intégrité de sécurité décrites dans la SRS du programme d'application ont réellement été démontrées par les essais.

Annexe C
(informative)

Considérations lors de la conversion des technologies NP en technologies PE

De nombreuses installations du secteur des industries de transformation utilisent des appareils électriques ou solides pour la conception de leurs SIS. Ces installations peuvent souhaiter profiter des avantages offerts par la technologie PE, et ainsi planifier la modification ou l'addition de leur(s) SIS avec l'utilisation d'appareils programmables électroniques. Certaines considérations dont l'installation peut tenir compte avant et pendant cette transition sont énoncées dans les points suivants:

a) Il convient de ne pas utiliser les appareils programmables électroniques pour les SIS sauf si l'installation peut vérifier, valider, utiliser, exploiter et maintenir les appareils programmables électroniques dans leurs BPCS;

b) Il convient de ne pas utiliser les appareils programmables électroniques pour les SIS, sauf si l'installation a la capacité d'utiliser, de concevoir, de modifier et de maintenir le programme d'application pour les appareils programmables électroniques;

c) Il convient de passer en revue les éléments qui peuvent être transférés à partir de la capacité d'application de l'installation existante vers le programme d'application du SIS, tels que:

- les compétences et l'expérience (expérience de programmation, capacité, disponibilité, par exemple), la portabilité des compétences du programme d'application sur site pour le SIS et la connaissance et l'implication en matière de gestion du SIS avec le support PE;
- la capacité de sécurité puisqu'elle est liée à la permission d'accès (local et à distance);
- l'utilisation du langage de l'application dans l'installation existante;
- les modules (par exemple, algorithmes de commande existants comme le moteur démarrage/arrêt/essai, la comparaison de l'état de la position réelle avec la commande de position);
- la réponse en temps réel et les délais pour passer du système câblé au système PE;
- les interfaces (par exemple, interfaces existantes, prouvées, fiables vers le DCS, IHM, réseaux, interfaces électriques, planning);
- la documentation (capacité à fournir la fonctionnalité pour décrire clairement le programme d'application au personnel/aux opérateurs de maintenance, par exemple);
- le support pour dépanner le PE et le programme d'application 24 h/24 et 7 j/7;
- la couverture (disponibilité du support 24 h/24 et 7 j/7);
- la réponse (par exemple, le temps de résolution d'un problème);
- le simulateur (pour l'analyse, la modification, le développement, la formation du programme d'application hors ligne, par exemple);
- la capacité d'essai (approche et capacité des essais de l'installation par opposition aux essais nécessaires du programme d'application, par exemple);
- l'expérience de l'opérateur (avec le PE et le programme d'application);
- les procédures de dérivation de l'installation (et leur réalisation et contrôle en utilisant la programmation d'application);
- la conversion de la technologie NP de la solution IHM de l'installation en technologie PE;
- la formation (disponibilité, couverture de la programmation d'application, IHM);

- les outils (par exemple, programmation, développement, soumission à l'essai); le support pour le logiciel utilitaire;
- le support de gestion (existant, suffisant, connaissance de l'exigence par toutes les parties);
- la gestion de la procédure de changement, y compris le contrôle sur les modifications du programme d'application, le stockage sécurisé et la gestion de configuration, ainsi que les dispositions en matière de revalidation lorsque des changements ont été apportés ou pouvant affecter le programme d'application;
- les futures améliorations/mises à jour/obsolescences du (ou des) système(s);
- les normes de programmation d'application de l'entreprise/l'installation et la proclamation des codes de pratique de l'industrie;
- la compatibilité avec les solutions PE "sœurs" pour l'échange d'expérience, de processus, d'équipements, etc.

Annexe D
(informative)

Exemple présentant le passage d'un schéma de tuyauterie et d'instrumentation (P&ID) à un programme d'application

L'Annexe D montre comment un processus de séparation de l'huile et du gaz a évolué d'un schéma P&I vers un programme d'application. La Figure D.1 présente le schéma P&I. La Figure D.2 présente l'expression des fonctions de sécurité à l'aide d'un schéma de cause à effet. La Figure D.3 présente la conversion du schéma de cause à effet en programme d'application à l'aide de la programmation de blocs fonctionnels.

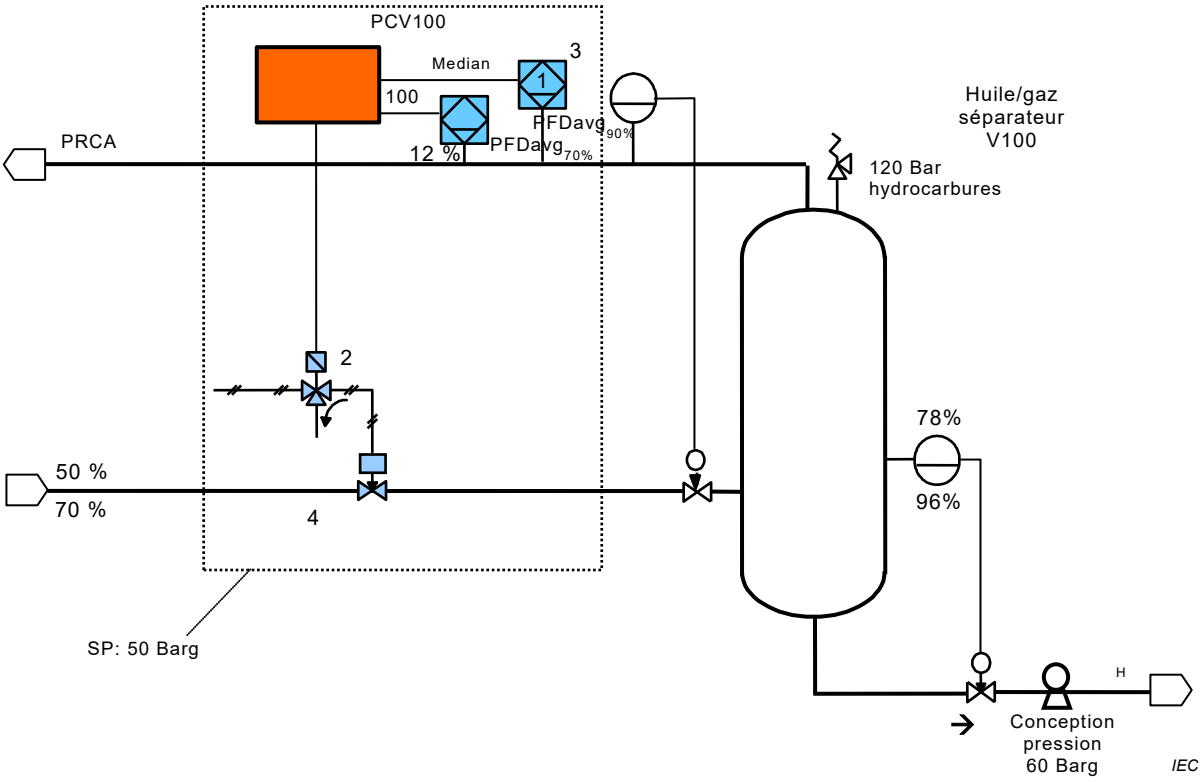
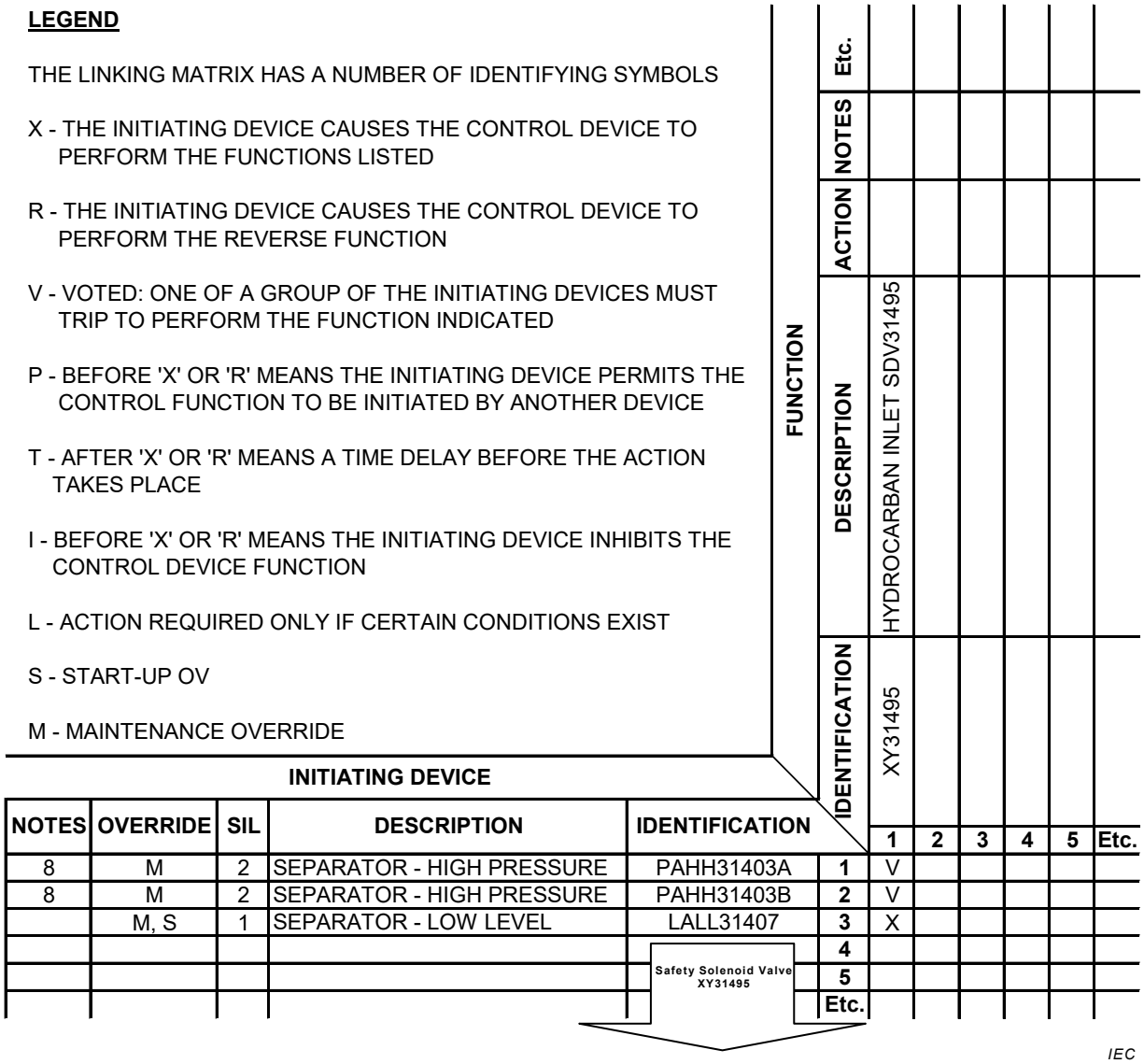


Figure D.1 – Exemple de schéma de tuyauterie et d'instrumentation d'un séparateur d'huile et de gaz

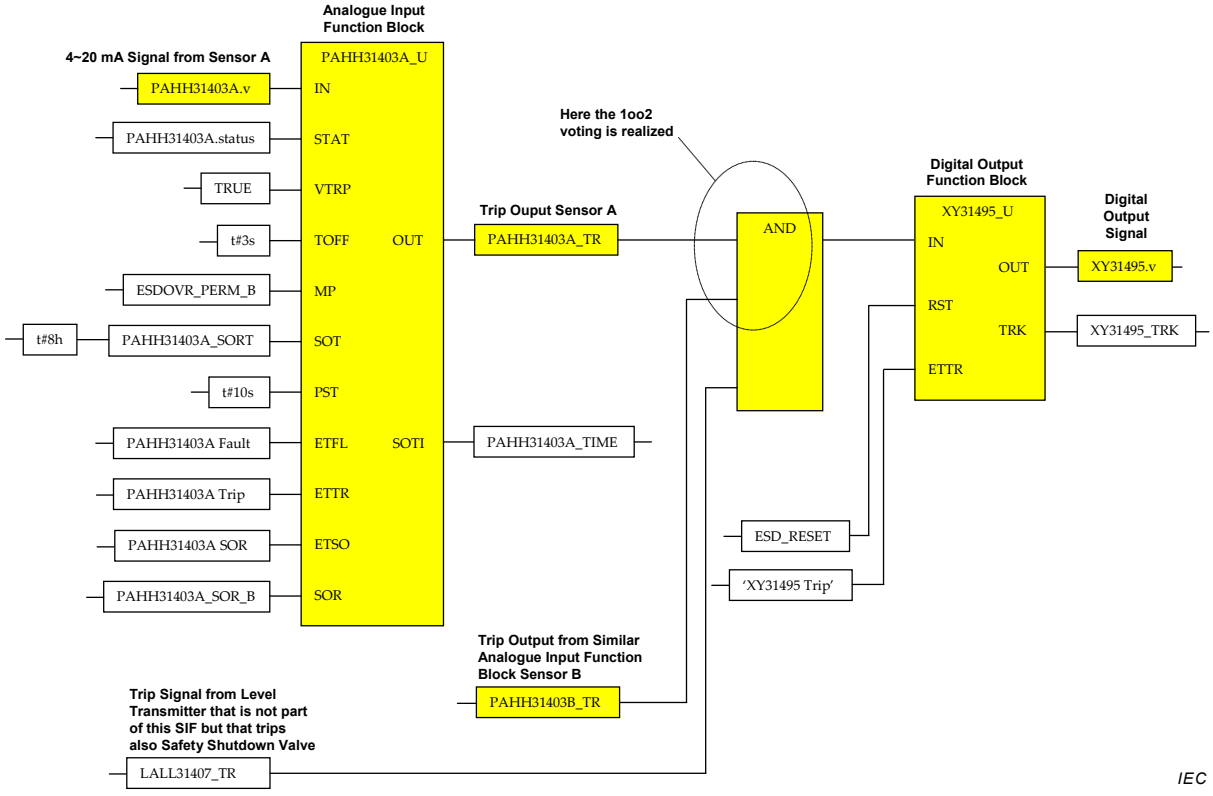


Anglais	Français
LEGEND	LEGENDE
THE LINKING MATRIX HAS A NUMBER OF IDENTIFYING SYMBOLS	LA MATRICE DE LIAISON COMPORTE PLUSIEURS SYMBOLES D'IDENTIFICATION
X – THE INITIATING DEVICE CAUSES THE CONTROL DEVICE TO PERFORM THE FUNCTIONS LISTED	X – L'APPAREIL INITIATEUR POUSSE L'APPAREIL DE COMMANDE A EFFECTUER LES FONCTIONS REPERTORIEES
R – THE INITIATING DEVICE CAUSES THE CONTROL DEVICE TO PERFORM THE REVERSE FUNCTION	R – L'APPAREIL INITIATEUR POUSSE L'APPAREIL DE COMMANDE A EFFECTUER LA FONCTION INVERSE
V – VOTED: ONE OF A GROUP OF THE INITIATING DEVICES MUST TRIP TO PERFORM THE FUNCTION INDICATED	V – VOTE: L'UN DES GROUPES DES APPAREILS INITIATEURS DOIT SE DECLENCHER POUR EFFECTUER LA FONCTION INDIQUEE
P – BEFORE 'X' OR 'R' MEANS THE INITIATING DEVICE PERMITS THE CONTROL FUNCTION TO BE INITIATED BY ANOTHER DEVICE	P – AVANT 'X' OU 'R' SIGNIFIE QUE L'APPAREIL INITIATEUR PERMET A LA FONCTION DE COMMANDE D'ETRE INITIEE PAR UN AUTRE APPAREIL
T – AFTER 'X' OR 'R' MEANS A TIME DELAY BEFORE THE ACTION TAKES PLACE	T – APRES 'X' OU 'R' SIGNIFIE QU'UN DELAI S'ECOULE AVANT LE DEMARRAGE DE L'ACTION
I – BEFORE 'X' OR 'R' MEANS THE INITIATING DEVICE INHIBITS THE CONTROL DEVICE FUNCTION	I – AVANT 'X' OU 'R' SIGNIFIE QUE L'APPAREIL INITIATEUR EMPECHE L'APPAREIL DE COMMANDE DE FONCTIONNER

Anglais	Français
L – ACTION REQUIRED ONLY IF CERTAIN CONDITIONS EXIST	L – ACTION EXIGEE UNIQUEMENT SI CERTAINES CONDITIONS EXISTENT
S – START-UP OV	S – NEUTR. DU DEMARRAGE
M – MAINTENANCE OVERRIDE	M – NEUTRALISATION DE LA MAINTENANCE
INITIATING DEVICE	APPAREIL INITIATEUR
NOTES	NOTES
OVERRIDE	NEUTRALISATION
SIL	SIL
DESCRIPTION	DESCRIPTION
IDENTIFICATION	IDENTIFICATION
FUNCTION	FONCTION
ACTION	ACTION
SEPARATOR – HIGH PRESSURE	SEPARATEUR – PRESSION ELEVEE
SEPARATOR – LOW LEVEL	SEPARATEUR – NIVEAU FAIBLE
HYDROCARBAN INLET	ENTRÉE D'HYDROCARBURE
Safety solenoid valve	Electrovanne de sécurité

Figure D.2 – Exemple de schéma de cause à effet d'une ESD (en partie)

Un exemple de programme d'application pour une SIF dotée de deux signaux analogiques de vote 1oo2 provenant des capteurs de pression et d'une sortie numérique vers un seul élément terminal est présenté ci-dessous. Le concept de sécurité est la DTS (mise hors tension vers l'état de sécurité). Le langage du programme est en blocs fonctionnels.



Anglais	Français
4~20 mA signal from sensor A	Signal 4~20 mA provenant du capteur A
Trip signal from level transmitter that is not part of this SIF but that trips also safety shutdown valve	Signal de déclenchement du transmetteur de niveau qui ne fait pas partie de cette SIF mais qui déclenche également la vanne d'arrêt de sécurité
Analogue input function block	Bloc fonctionnel d'entrée analogique
Trip output sensor A	Déclenchement du capteur de sortie A
Trip output from similar analogue input function block sensor B	Déclenchement de la sortie du capteur B du bloc fonctionnel d'entrée analogique similaire
Here the 1oo2 voting is realized	Ici, le vote 1oo2 est effectué
Digital output function block	Bloc fonctionnel de sortie numérique
Digital output signal	Signal de sortie numérique

Figure D.3 – Exemple de programme d'application (en partie) dans une programmation de blocs fonctionnels d'automate de sécurité

Annexe E
(informative)

Méthodes et outils de programmation d'application

E.1 Jeu d'outils type pour la programmation d'application

Le jeu d'outils de support pour la programmation PE inclura généralement les capacités suivantes:

a) Un éditeur de configuration. Cet éditeur est utilisé pour configurer le sous-système d'E/S SIS, les variables de mémoire d'E/S et les fonctions de communication;

b) Des éditeurs de langage. Ces éditeurs sont utilisés par le programmeur de l'application pour développer les programmes qui exécutent toutes les fonctions exigées par le système (de sécurité et de non-sécurité).

c) Les bibliothèques des fonctions préalablement évaluées et des blocs fonctionnels. Ces fonctions et blocs fonctionnels peuvent être utilisés dans les programmes d'application.

d) Des capacités de développement de fonction et de bloc fonctionnel personnalisés. Certains fournisseurs proposent un environnement de développement qui permet à l'utilisateur de développer des fonctions et des blocs fonctionnels personnalisés, qui peuvent être utilisés par les langages de l'application compatibles. Il convient que ces fonctions et blocs fonctionnels personnalisé(e)s soient intégralement soumis à l'essai avant leur utilisation dans le programme d'application.

e) Une fonction de planification de programme d'application. Ces fonctions d'ordonnancement assistent l'établissement de l'ordre de la séquence d'exécution souhaitée et des taux de balayage.

f) Des capacités de téléchargement. Cela permet au développeur de télécharger le programme d'application, les bibliothèques de blocs fonctionnels, les données variables et toutes autres informations de configuration dans le matériel du solveur logique, pour exécution.

g) Des capacités d'émulation. Certains fournisseurs proposent un environnement de développement permettant d'émuler tous les programmes d'application sur l'ordinateur qui prend en charge l'environnement de développement. Cela permet de soumettre les programmes d'application à des essais complets hors ligne avant qu'ils ne soient téléchargés dans le solveur logique.

h) Des capacités de surveillance de programme. Les capacités de surveillance permettent à l'utilisateur de visualiser des données du programme d'exécution sur des écrans définis par l'utilisateur ou sur des écrans de programme en langage en bloc fonctionnel réel ou en langage à contacts. L'environnement de développement peut également offrir des capacités pour surveiller l'exécution de l'émulateur. En plus, les programmes s'exécutant dans le solveur logique peuvent être surveillés.

i) Des affichages de diagnostic du solveur logique. Ces affichages présentent l'état des modules processeur principaux, des modules de communication et des modules d'E/S dans le système. Typiquement les états actifs "bon", "mauvais", de chaque module sont présentés et dans de nombreux cas, des informations plus détaillées sur les erreurs au sein du système sont disponibles.

Le système PE sera pris en charge par un environnement de programmation qui prend en charge le codage du programme d'application, la configuration des paramètres de l'application et des interfaces, et les essais/la surveillance de l'exécution du programme d'application. La plupart des systèmes PE destinés à être utilisés dans des applications de sécurité seront pris en charge par un jeu d'outils dédié, accompagné d'un manuel d'utilisation qui décrira la façon d'utiliser ces derniers, afin de garantir que le programme d'application atteint l'intégrité visée. Il convient que l'environnement de conception et le langage de l'application disposent de caractéristiques qui facilitent:

- l'abstraction, la modularité et d'autres caractéristiques qui permettent de maîtriser la complexité; dans la mesure du possible, il convient que le programme d'application s'appuie sur des modules logiciels éprouvés, qui peuvent inclure des fonctions de bibliothèque utilisateur et des règles bien définies de liaison des modules;
- l'expression de:
  - la fonctionnalité, idéalement en tant que description logique ou fonctions algorithmiques;
  - le flux d'informations entre les appareils modulaires des fonctions de l'application;
  - les exigences de séquencement;
  - l'assurance que les SIF fonctionnent toujours suivant les contraintes de temps définies;
  - l'absence de comportement indéterminé;
  - l'assurance que les données élémentaires internes ne sont pas dupliquées par erreur, tous les types de données utilisées sont définis et l'action appropriée se produit lorsque les données sont hors plage ou erronées;
  - les hypothèses de conception et leurs liens;
- il convient que les développeurs et les autres personnes qui en ont besoin comprennent la conception, à la fois du point de vue de la fonctionnalité de l'application et de la connaissance des contraintes de la technologie;
- la vérification et la validation, y compris la couverture du programme d'application, la couverture fonctionnelle de l'application intégrée, l'interface avec le SIS et sa configuration de matériel spécifique à l'application;
- la modification du programme d'application. Ces dispositions incluent la modularité, la traçabilité et la documentation.

E.2 Règles et contraintes pour la conception du programme d'application

Une liste des éléments à prendre en compte lors du développement du programme d'application pour les SIS est donnée ci-après:

a) scinder le programme d'application en SIF discrètes, avec un SIL pour chaque SIF;

b) comprendre l'architecture matérielle de chaque SIF et la reproduire dans chaque programme d'application de la SIF;

c) ne pas optimiser le programme d'application si cela augmente sa complexité (l'interprétation du programme d'application exige souvent la présence d'un programmeur très expérimenté);

d) utiliser les techniques de développement de programme d'application indiquées dans les instructions du constructeur (le manuel de sécurité, par exemple);

e) ne pas combiner le programme d'application d'une SIF avec une autre SIF;

f) utiliser le langage du programme d'application (type, fonction, par exemple) pour lequel le personnel a été formé, et est capable de comprendre et de dépanner;

g) fournir une description écrite du programme d'application, cohérente avec la description fonctionnelle, dans la documentation du programme d'application;

h) mettre le programme d'application sous forme de modules, en cohérence avec le procédé (le premier module est le programme d'application commun, non lié à une SIF, mais exigé dans le SIS, le deuxième module étant la première SIF située à l'entrée du processus, et le dernier module étant la dernière SIF située à la sortie du processus, par exemple);

i) soumettre à des essais précis (simuler, inspecter, passer en revue, par exemple) chaque module du programme d'application et obtenir une deuxième analyse indépendante (inclure le département d'exploitation et de maintenance ici et dans toutes les étapes suivantes);

j) soumettre à des essais précis la combinaison de modules qui compose un sous-système SIS de processus et obtenir une deuxième analyse indépendante;

k) soumettre à des essais précis le programme d'application du SIS et obtenir une deuxième analyse indépendante;

l) utiliser le programme d'application en vérifiant le matériel (en confirmant que les E/S sont connectées au capteur/à l'élément terminal correct, par exemple);

m) inclure les essais du programme d'application dans la mise en route (fonctionnement du processus sans matériel dangereux, par exemple);

EXEMPLE Contrôles de bout en bout des liaisons de communication, contrôles de limitation de zones adressables des entrées de capteur, contrôles de limitation de zones adressables des paramètres de données et exécution diverse des fonctions de l'application.

n) Les membres de l'équipe d'assistance du programme d'application doivent être présents pendant le déroulement du processus (à la mise en service, par exemple);

o) Pas de verrouillage entre les SIF.

E.3 Règles et contraintes pour la programmation d'application

Certaines règles de programmation d'application de solveurs logiques PE qu'il convient de prendre en considération sont énoncées ci-après. Leur validité dépendra de l'application:

a) Ne pas utiliser les fonctions SKIP et JUMP;

b) Ne pas utiliser les fonctions NOT;

c) Ne pas utiliser l'adressage indirect;

d) Ne pas utiliser les algorithmes de compression;

e) Ne pas utiliser de logique basée sur des résultats de calculs arithmétiques;

f) Ne pas utiliser de logique avec une mémoire d'état interne (les mémoires à bascule, par exemple);

g) Ne pas utiliser de variables de texte dans la SIF;

h) Ne pas utiliser de fonctions ou de sous-routines qui incluent la transmission de variables ou de paramètres;

i) Ne pas personnaliser les fonctions de bibliothèque;

j) Ne pas utiliser les interruptions;

k) Ne pas utiliser le verrouillage;

l) Ne pas utiliser la compression de variables booléennes dans des variables entières;

m) Ne pas inverser l'état physique des capteurs ou de l'actionneur dans la logique;

n) Ne pas répartir les verrouillages d'une SIF sur plusieurs solveurs logiques;

o) Ne pas utiliser de fonctions de communication réseau autres que les fonctions passives;

p) Utiliser des méthodes de programmation évaluées pour la sécurité et approuvées par l'installation;

q) Utiliser des modules normalisés ("types", par exemple);

r) Fournir à l'appareil des descripteurs alphanumériques qui donnent la description de la tâche et la référence croisée pour chaque capteur, élément terminal (par exemple, électrovannes, vannes, moteurs, alarmes), SIF, entre autres, en cohérence et en lien avec les dessins de conception (par exemple, diagrammes P&I, dessins de dispositions, diagrammes logiques);

s) Utiliser des fonctions de sécurité préprogrammées avec solveur logique, déjà analysées et approuvées par l'installation (arrêt d'urgence, barrières immatérielles, portes de sécurité, par exemple);

t) Séparer la programmation du solveur logique PE en trois zones distinctes: le circuit d'entrée, le circuit logique et le circuit de sortie;

- Il convient de dessiner les circuits d'entrée verticalement au format d'un diagramme à contacts. Chaque échelon est doté d'un capteur à gauche et de modules d'entrée à droite; il convient de câbler chaque capteur discrètement;
- Il convient de dessiner les diagrammes logiques verticalement au format d'un diagramme à contacts (ou du LVL approprié). Chaque échelon est doté d'entrées à gauche et d'une sortie à droite;
- Il convient de dessiner les diagrammes de sortie verticalement au format d'un diagramme à contacts. Chaque échelon est doté d'une sortie de solveur logique à gauche et d'un élément terminal à droite; il convient de câbler chaque capteur discrètement;

u) Il convient que l'approche de conception soit normalement "désactiver pour déclencher" vers un état de sécurité. Pour les systèmes "activer pour déclencher", des précautions spéciales seront exigées;

v) Il convient d'arranger l'adressage E/S du solveur logique et la programmation du solveur logique pour refléter l'application du processus (par exemple, il convient de relier la programmation initiale et les affectations E/S au cycle de démarrage de l'application et de continuer son développement au même format que le déroulement du processus l'impose, en terminant par la fonction arrêt);

w) Il convient d'identifier les fonctions de support, comme les essais périodiques, la commande manuelle, la dérivation, les alarmes et les diagnostics, comme telles et de les séparer de la SIF;

x) Fournir la capacité de mémoire, de traitement et d'E/S de rechange nécessaire pour que la capacité à fournir la programmation d'application nécessaire ainsi que sa simplicité soient maintenues pendant les futures exigences de modification/expansion;

y) Il convient que les diagrammes disposent de références croisées à l'emplacement de plusieurs utilisations d'un composant par le programme d'application (entrée, sortie, registre interne, par exemple);

z) S'assurer que l'ordre de traitement au sein du programme d'application satisfait à la réponse en temps réel.

Annexe F
(informative)

Exemple de projet de SIS présentant chaque phase du cycle de vie de sécurité avec le développement du programme d'application en utilisant le langage à relais

NOTE Le présent exemple est utilisé avec la permission de l'ISA et du CCPS de l'AIChE, *Guidelines for Safe Automation of Chemical Processes*, New York, 1993, disponible à: AIChE, 345 East 47th Street, New York, NY 10017, Tél.: (212) 705-7657.. L'exemple est modifié afin de satisfaire aux exigences de l'IEC 61511.

F.1 Présentation

L'exemple présenté à l'Annexe F montre la manière d'appliquer chaque phase de la mise en œuvre du cycle de vie de sécurité à l'aide d'un langage à contacts conforme à la série IEC 61511.

Il s'agit de la 3^{e} édition de cet exemple. La 1re édition a été publiée par le CCPS avant la publication de l'IEC 61508 et de l'IEC 61511. La 2^{e} édition a été publiée par l'ISA (TR84.00.04, partie 2) qui s'est appuyé sur les 1res éditions de l'IEC 61508 (2000) et de l'IEC 61511 (2003). Cette 3^{e} édition s'appuie sur l'IEC 61508 (2010) et sur la série IEC 61511. De plus, cet exemple a été divisé en cohérence avec la procédure de cycle de vie de sécurité de l'IEC 61511-1:2016 , Figure 7.

Il s'agit de démontrer une méthode pour satisfaire aux exigences de l'IEC 61511. Il convient que le lecteur sache que la série IEC 61511 s'appuie sur les performances et que de nombreuses approches peuvent être utilisées pour respecter la conformité. Certaines méthodes appliquées dans cet exemple incluent: des techniques de simulation et HAZOP pour l'analyse de danger et de risque, la procédure LOPA pour l'affectation des fonctions de sécurité aux couches de protection, l'analyse par arbre des défaillances pour la vérification du SIL et le langage à contacts pour documenter les exigences du programme d'application. D'autres techniques et outils pourraient être utilisés au cours de chacune de ces étapes dans le cycle de vie de sécurité du SIS afin de satisfaire aux exigences des normes.

L'exemple utilise le même processus chimique que celui présenté dans le document "CCPS AIChE, *Guidelines for Safe Automation of Process Applications*, 1993".

Cet exemple sélectionne le sous-système SIS d'un processus et lui applique la philosophie, les procédures, les techniques et la méthodologie de vérification de conception abordées dans l'IEC 61511.

Le présent exemple donne la documentation de A à Z (du concept au déclassement) pour chaque fonction instrumentée de sécurité (SIF). L'origine de la présente documentation offre aux auditeurs et au personnel de l'installation les moyens de suivre la SIF tout au long des phases du cycle de vie de sécurité du SIS jusqu'à l'analyse des dangers du processus (PHA) qui l'a créé. Chaque SIF est clairement identifiée dans chaque document afin de faciliter le suivi entre les phases du cycle de vie. L'aptitude à démontrer à des tiers (par exemple aux auditeurs, organismes de contrôle, compagnies d'assurances) que la réduction de risque obtenue par chaque SIF est adéquate constitue une partie essentielle de la sécurité.

Le présent exemple ne représente pas la conception complète pour un processus de polymérisation en raison de la précision des détails devant permettre d'obtenir une conception automatisée en toute sécurité et de haute intégrité. Par conséquent, le présent exemple inclut un certain nombre de simplifications.

Toutes les références présentées se reportent à des informations contenues dans le présent exemple, sauf indication contraire.

F.2 Définition du projet

F.2.1 Généralités

Le processus décrit est la polymérisation du monomère chlorure de vinyle (VCM),

$$CH_2=CHCl$$

en polychlorure de vinyle (PVC),

$$[-CH_2-CHCl-]_n$$

L'exemple comprend un réactant dangereux, le VCM, qui est inflammable et se compose de produits de combustion toxiques, tout en étant un carcinogène connu. Le processus représente également une opération de lot à plus grande échelle en fonctionnement semi-continu sur une période d'environ 10 heures pendant que la polymérisation progresse. Une description simplifiée des étapes du processus est également apportée.

F.2.2 Planification conceptuelle

Une fois qu'une décision opérationnelle visant à considérer la production d'un produit donné (dans le présent exemple, le polychlorure de vinyle) est prise, l'équipe chargée du projet initial est formée. L'équipe commencera par analyser les itinéraires de processus potentiels afin d'identifier une technologie qui satisfera aux exigences de production tout en satisfaisant aux responsabilités en matière de santé, sécurité et protection de l'environnement.

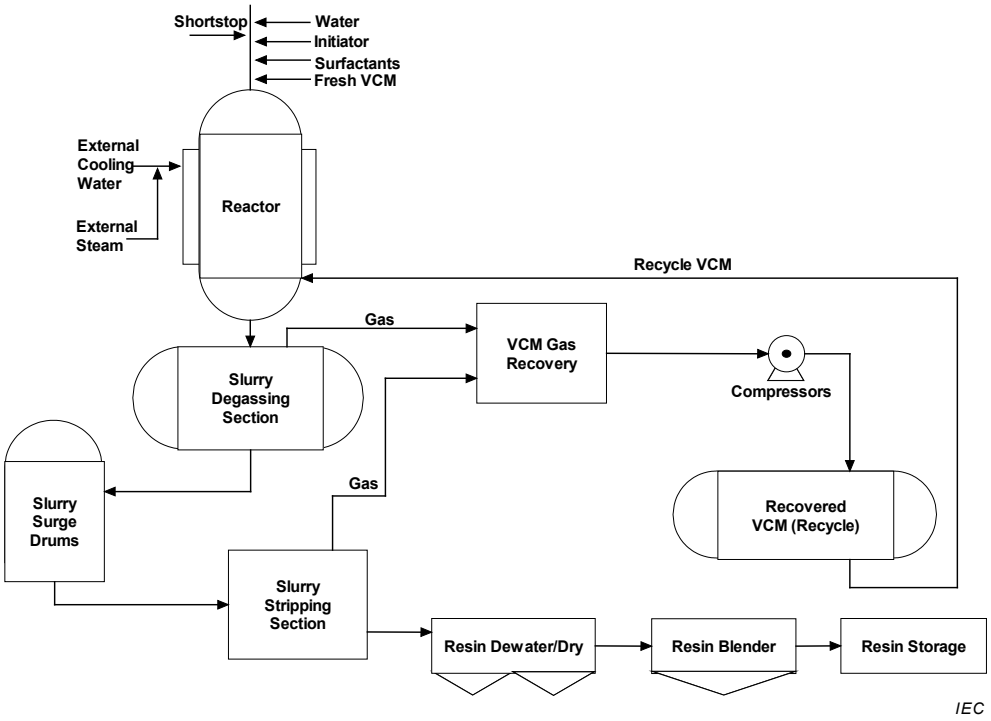
F.2.3 Analyse des dangers du processus

Lors des toutes premières étapes d'analyse du processus et de définition du projet, une équipe chargée de l'analyse des dangers du processus commence à interagir avec les concepteurs en étroite collaboration. Pour les projets nécessitant la gestion de matériaux dangereux, l'équipe sera composée non seulement d'ingénieurs de conception du processus, mais également de spécialistes de la santé et de la sécurité. Il convient que l'équipe ait régulièrement des contacts avec d'autres spécialistes – par exemple, les chimistes, le personnel d'exploitation, les consultants ou les sous-traitants d'ingénierie avec de l'expérience dans des processus identiques ou similaires, ainsi que des concédants de brevet de processus. Dans le présent exemple, un processus dûment éprouvé est disponible comme point de départ. Le présent exemple portera donc sur les aspects du processus de conception qui influencent ou impliquent directement la conception des systèmes de commande et des systèmes de verrouillage de sécurité du processus. Des informations plus détaillées sur les aspects relatifs au processus de conception peuvent être obtenues dans la liste suivante de textes du Center for Chemical Process Safety (Centre pour la sécurité des processus chimiques), American Institute of Chemical Engineers (Institut américain des ingénieurs chimistes):

- *Guidelines for Hazard Evaluation Procedures;*
- *Guidelines for Chemical Process Quantitative Risk Analysis;*
- *Guidelines for Safe Storage and Handling of High Toxic Hazard Material;*
- *Guidelines for Vapor Release Mitigation;*
- *Guidelines for the Technical Management of Chemical Process Safety.*

F.3 Description simplifiée du processus

La fabrication du PVC à partir du monomère est relativement simple. Le cœur du processus est le réservoir du réacteur dans lequel la polymérisation se produit sur une période d'environ dix heures, pendant laquelle le contenu du réacteur est mécaniquement agité et la chaleur de la réaction est neutralisée par la circulation d'eau de refroidissement à travers la chemise du réacteur. Etant donné que le processus implique le chargement d'un lot dans le réacteur, des systèmes de processus sont conçus avec des unités de réacteur multiples en parallèle. Ainsi, le processus peut être exploité sur une base semi-continue. A des fins de simplification, cet exemple se concentrera sur une des unités, en reconnaissant qu'une unité de production réelle aura généralement plusieurs unités parallèles exploitées en séquence.



Anglais	Français
Shortstop	Arrêt court
Water	Eau
Initiator	Initiateur
Surfactants	Surfactants
Fresh VCM	Monomère chlorure de vinyle (VCM) nouveau
External cooling water	Eau de refroidissement externe
External steam	Vapeur externe
Reactor	Réacteur
Recycle VCM	VCM recyclé
Gas	Gaz
VCM gas recovery	Récupération du gaz VCM
Compressors	Compresseurs
Slurry degassing section	Section de dégazage à la boue
Slurry surge drums	Tambours d'ondes de choc à boue
Recovered VCM (recycle)	VCM récupéré (recyclé)
Slurry stripping section	Section de dilution à la boue

Anglais	Français
Resin dewater/dry	Déshydratation/séchage de la résine
Resin blender	Mélangeur de résine
Resin storage	Stockage de résine

Figure F.1 – Schéma de procédé simplifié: processus pour le PVC

La Figure F.1 représente un diagramme simplifié du processus pour une installation type de fabrication de PVC. Si le réservoir du réacteur a été ouvert pour maintenance après traitement et déchargement du dernier lot, il convient d'abord de l'évacuer pour extraire tout air résiduel (oxygène) de la phase gazeuse afin de minimiser la réaction d'oxydation du monomère. En effet, cette réaction produit une HCl et peut mener à des dommages de corrosion sous contrainte sur le réservoir du réacteur mais également à une mauvaise qualité de produit. Sinon, la première étape consiste à traiter le réservoir du réacteur avec une solution antisalissure, afin d'empêcher la polymérisation sur les murs du réacteur. Cette étape est suivie par le chargement du réservoir avec de l'eau déminéralisée et des surfactants.

Ensuite, la charge du monomère chlorure de vinyle (VCM) liquide est ajoutée à sa pression de vapeur (environ 3,86 Barg à 21 °C – 56 psig à 70 °F).

L'initiateur de réaction est le peroxyde qui est dissous dans un solvant. Puisqu'il est relativement actif, il est stocké à de basses températures dans un contenant spécial. De petites quantités sont extraites pour l'utilisation quotidienne dans le processus et sont conservées dans un congélateur. Il est d'abord introduit dans un petit pot de charge associé au réacteur afin d'assurer que seule la quantité correcte est ajoutée.

A la suite de l'introduction de l'initiateur de réaction, de l'eau chauffée à la vapeur est appliquée à la chemise du réacteur afin d'augmenter la température jusqu'à environ 54,5 °C à 60 °C – 130 °F à 140 °F (en fonction de la formule de lot pour la classe particulière du produit), à laquelle la réaction aura lieu à un taux satisfaisant. L'agitation est nécessaire pour suspendre le VCM dans l'eau (contrôler la taille de la particule), améliorer le transfert de chaleur dans tout le lot et engendrer un produit uniforme. Puisque la réaction est exothermique, l'eau de refroidissement circule dans la chemise du réacteur afin de contrôler la température du réacteur. Les conditions du réacteur sont minutieusement contrôlées au cours de la période d'environ huit heures exigée pour la réalisation de la polymérisation.

La réaction est terminée lorsque la pression du réacteur diminue, ce qui signale que la plus grande partie du monomère a subi la réaction. Le polymère qui a subi la réaction est déchargé du réacteur et envoyé dans des unités de traitement en aval pour la récupération, la dilution, la déshydratation et le séchage du VCM résiduel.

F.4 Conception préliminaire

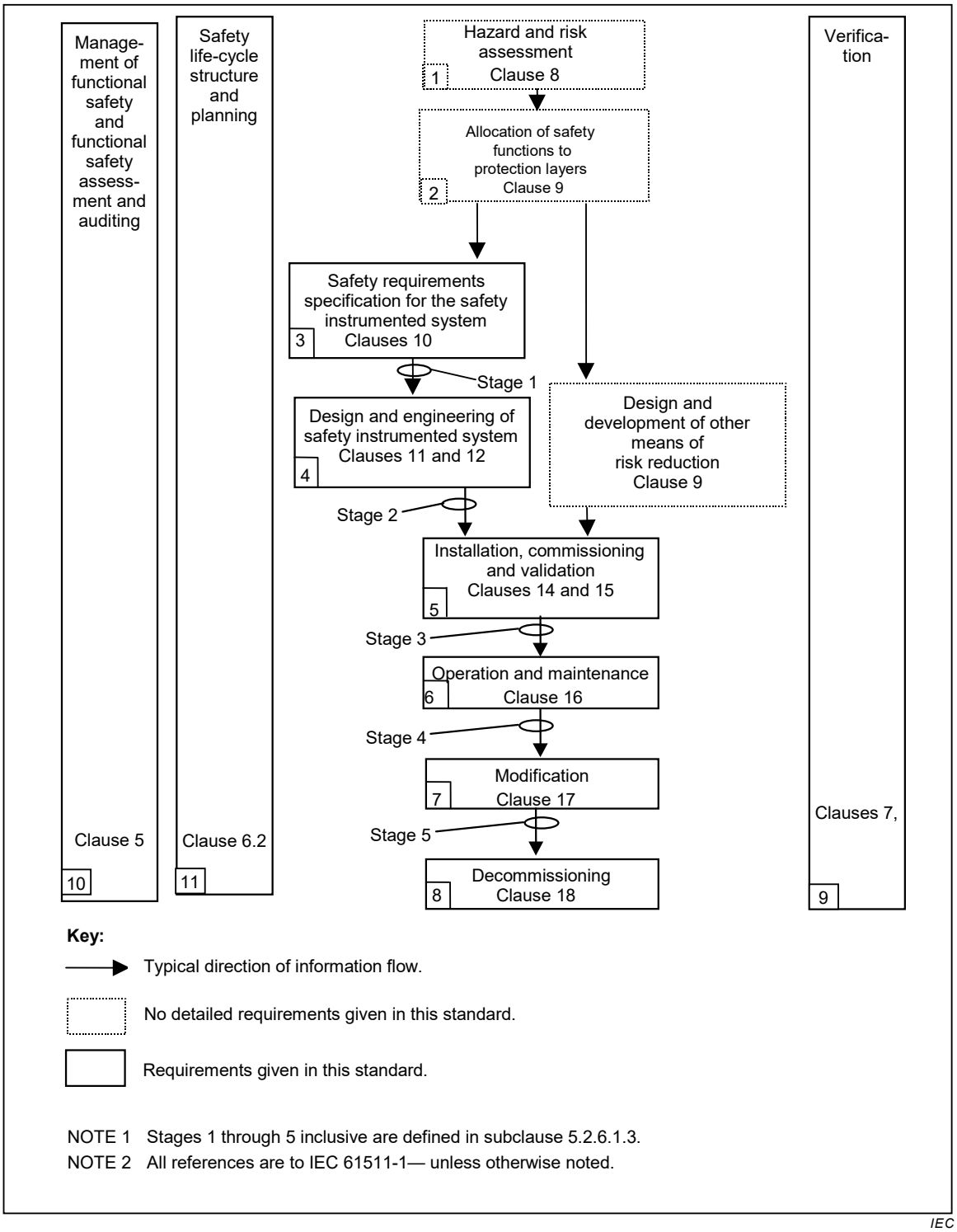
Toutes les exigences locales spéciales sont revues, les réglementations applicables sont identifiées et les lignes directrices de risque générales sont établies. Les exigences du réseau d'alimentation (par exemple l'air; l'eau de refroidissement, la puissance électrique) sont revues et confirmées pour être adéquates à l'application.

F.5 Application de l'IEC 61511

F.5.1 Généralités

A l'issue de la planification préliminaire (voir les Articles F.2 à F.4 inclus), la mise en œuvre de l'IEC 61511 commence.

Pour cet exemple, la stratégie de conception consiste à initialiser la conception du cycle de vie (Figure F.2) et à décomposer les phases du cycle de vie en dix étapes cohérentes avec la Figure F.2 et le Tableau F.1 (vue d'ensemble du cycle de vie de sécurité). A ce stade du projet, il peut être judicieux d'utiliser le tableau de cycle de vie pour attribuer les responsabilités de chacune des phases du cycle de vie (voir le Tableau F.1).



IEC

Anglais	Français
Management of functional safety and functional safety assessment and auditing Clause 5	Gestion de la sécurité fonctionnelle et évaluation et audit de la sécurité fonctionnelle Article 5

Anglais	Français
Safety life-cycle structure and planning Subclause 6.2	Structure et planification du cycle de vie de sécurité Paragraphe 6.2
Hazard and risk assessment Clause 8	Analyse de danger et de risque Article 8
Allocation of safety functions to protection layers Clause 9	Affectation des fonctions de sécurité aux couches de protection Article 9
Safety requirements specification for the safety instrumented system Clauses 10	Spécification des exigences concernant la sécurité du système instrumenté de sécurité Article 10
Stage	Etape
Design and engineering of safety instrumented system Clauses 11 and 12	Conception et ingénierie du système instrumenté de sécurité Articles 11 et 12
Design and development of other means of risk reduction Clause 9	Conception et développement d'autres moyens de réduction du risque Article 9
Installation, commissioning and validation Clauses 14 and 15	Installation, mise en service et validation Articles 14 et 15
Operation and maintenance Clause 16	Fonctionnement et maintenance Article 16
Modification Clause 17	Modification Article 17
Decommissioning Clause 18	Déclassement Article 18
Verification Clause 7	Vérification Article 7
Key	Légende
Typical direction of information flow	Sens type du flux d'informations
No detailed requirements given in this standard	Aucune exigence détaillée donnée dans la présente norme
Requirements given in this standard	Exigences données dans la présente norme
NOTE 1 Stages 1 through 5 inclusive are defined in 5.2.6.1.3.	NOTE 1 Les étapes 1 à 5 (incluse) sont définies dans en 5.2.6.1.3.
NOTE 2 All references are to IEC 61511-1:2016 unless otherwise noted.	NOTE 2 Sauf indication contraire, toutes les références se reportent à l'IEC 61511-1 :—.

Figure F.2 – Phases de cycle de vie de sécurité du SIS et étapes de la FSA

Tableau F.1 – Vue d'ensemble du cycle de vie de sécurité du SIS

Phase ou activité du cycle de vie de sécurité		Objectifs	Exigences Article ou paragraphe de l'IEC 61511-1:2016	Entrées	Sorties	Responsabilité
Figure F.2 N° de zone	Titre					
1	H&RA	Déterminer les dangers et les événements dangereux du processus et des équipements associés, la séquence des événements conduisant à l'événement dangereux, le(s) risque(s) de processus associé(s) à l'événement dangereux, les exigences concernant la réduction de risque et les fonctions de sécurité exigées pour réaliser la réduction de risque nécessaire	8	Conception du processus, agencement, équipes de personnel, cibles de sécurité	Une description des dangers, des fonctions de sécurité exigées et de la réduction de risque associée	Equipe PHA Voir F.2.2
2	Affectation des fonctions de sécurité aux couches de protection	Affectation des fonctions de sécurité aux couches de protection et pour chaque SIF, le SIL associé		Description des SIF exigées et des exigences associées concernant l'intégrité de sécurité	Description de l'affectation des exigences de sécurité (voir l'Article 9 de l'IEC 61511:—)	Equipe PHA Voir F.2.2
3	SRS du SIS	Spécifier les exigences pour chaque SIS, en termes de SIF exigées et leur intégrité de sécurité associée, afin d'obtenir la sécurité fonctionnelle exigée	10	Description de l'affectation des exigences de sécurité (voir l'Article 9 de l'IEC 61511:—)	Exigences de sécurité du SIS; exigences de sécurité du programme d'application	Equipe E & I
4	Conception et ingénierie du SIS	Concevoir le SIS pour satisfaire aux exigences des SIF et leur intégrité de sécurité	11 et 12.4	Exigences concernant la sécurité du SIS; Exigences de sécurité du programme d'application	Conception du SIS en conformité avec les exigences de sécurité du SIS; planification de l'essai d'intégration du SIS	Equipe E & I

Phase ou activité du cycle de vie de sécurité		Objectifs	Exigences Article ou paragraphe de l'IEC 61511-1:2016	Entrées	Sorties	Responsabilité
Figure F.2 N° de zone	Titre					
5	Installation, mise en service et validation du SIS	Intégrer et soumettre à l'essai le SIS; Valider que le SIS satisfait, en tous points, aux exigences de sécurité, en termes de SIF et d'intégrité de sécurité exigées	12.3, 14, 15	Conception du SIS; Plan d'essai d'intégration du SIS; Exigences concernant la sécurité du SIS; Plan de validation de sécurité du SIS	SIS fonctionnant totalement en conformité avec les résultats des essais d'intégration du SIS, prévus à la conception du SIS; Résultats des activités d'installation, de mise en service et de validation	Construction
6	Fonctionnement et maintenance du SIS	Assurer que la sécurité fonctionnelle du SIS est conservée pendant le fonctionnement et la maintenance	16	Exigences du SIS; Conception du SIS; Plan pour le fonctionnement et la maintenance du SIS	Résultats des activités de fonctionnement et de maintenance	Opérations
	Modification du SIS	Faire des corrections, des améliorations ou des adaptations au SIS, en s'assurant que le SIL exigé est obtenu et maintenu	17	Exigences concernant la sécurité du SIS révisées	Résultats des modifications du SIS	Opérations
8	Déclassement	Assurer la revue, l'organisation sectorielle ad hoc, mais aussi assurer que la SIF reste appropriée	18	Exigences de sécurité et informations de processus conformes à la construction	SIF déclarée hors service	Opérations
9	Vérification du SIS	Soumettre à l'essai et évaluer les sorties d'une phase donnée, pour assurer la véracité et la cohérence par rapport aux produits et aux normes donnés comme entrées à cette phase	7, 12.5	Plan de vérification du SIS, pour chaque phase	Résultats de la vérification du SIS, pour chaque phase	Opérations
10	FSA du SIS	Enquêter et arriver à un jugement sur la sécurité fonctionnelle obtenue par le SIS	5	Planification pour la FSA du SIS; Exigence concernant la sécurité du SIS	Résultats de la FSA du SIS	Opérations

F.5.2 Etape F.1: Analyse de danger et de risque

Voir la phase Cycle de vie dans le Tableau F.2 ci-dessous.

Tableau F.2 – Cycle de vie de sécurité du SIS – Zone 1

Présentation					
Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigences Article ou paragraphe de l'IEC 61511:—**	**Entrées**	**Sorties**
Figure 2, zone 1	H&RA	Déterminer les dangers et les événements dangereux du processus et des équipements associés, la séquence des événements conduisant à l'événement dangereux, le(s) risque(s) de processus associé(s) à l'événement dangereux, les exigences concernant la réduction de risque et les fonctions de sécurité exigées pour réaliser la réduction de risque nécessaire	8	Conception du processus, agencement, équipes de personnel, cibles de sécurité	Une description des dangers, des fonctions de sécurité exigées et de la réduction de risque associée

F.5.3 Identification de danger

Le processus d'identification de danger a commencé pendant l'analyse de décision opérationnelle (Article F.2). Il s'agit de l'une des fonctions les plus importantes de l'équipe PHA, qui est continue jusqu'à la transition du processus vers une exploitation de l'installation. Elle fait l'objet d'une revue de sécurité en exploitation et à des programmes d'audit.

F.5.4 Evaluation de danger préliminaire

La première étape d'un planning de développement de processus consiste à identifier les paramètres larges du processus de production, à identifier les dangers liés à la sécurité et à l'environnement (ou les événements dangereux), mais aussi à rechercher les opportunités qui permettent de rendre le processus intrinsèquement plus sûr. Pour cela, des informations sont exigées sur les propriétés physiques et dangereuses de tous les matières de base, intermédiaires, produits et déchets impliqués dans des processus alternatifs éventuels. Pour cet exemple, dans lequel un polymère spécifique est créé d'après son monomère, le choix est restreint concernant le réactant de base. Les processus alternatifs disponibles modifient le moyen de polymérisation: solution, suspension ou émulsion. Les propriétés significatives du VCM sont résumées au Tableau F.3 (il convient d'utiliser la dernière fiche technique de sécurité du matériau VCM dans un exemple "réel").

Cependant, il convient de choisir attentivement les conditions de réaction et l'initiateur (ainsi que les additifs le cas échéant) afin de garantir que le taux de réaction peut être contrôlé en toute sécurité pour éviter les réactions de fuite, tout en fournissant une qualité et un rendement adéquats. La technologie sélectionnée implique la polymérisation dans l'eau, mais exige de petites quantités d'un initiateur liquide relativement dangereux. Les dangers liés à

l'initiateur exigent également une attention particulière, mais ne sont pas inclus dans cet exemple simplifié.

F.5.5 Historique de l'accident

Ensuite, les dangers sont identifiés. Dans cet exemple, les dangers principaux sont associés avec l'inflammabilité et la toxicité des produits de combustion du VCM. Dans un cas de conception dans une installation réelle, les limites d'exposition du personnel et du VCM ambiant environnemental seraient également des considérations importantes; pour plus de simplicité, elles ne sont pas traitées dans cet exemple. En tant que première étape, il est utile de passer en revue l'historique des accidents associés à des exploitations similaires.

Dans le cas du VMC, il est question d'une référence à un accident dans une installation de PVC, dans lequel quatre personnes sont décédées et dix ont été blessées. Cet accident a été provoqué par le déchargement d'un lot à partir du mauvais réservoir de réacteur. Le monomère a donc été libéré dans une salle contenant les réacteurs parallèles. La vapeur du VCM s'est probablement enflammée avec une étincelle issue des machines électriques ou avec l'électricité statique et le bâtiment qui abritait les réacteurs a explosé.

Dans un autre accident, un employé a ouvert par erreur la trappe d'un trou d'homme sur un réacteur en service, libérant une grande quantité de chlorure de vinyle qui s'est enflammée et a causé un embrasement éclair provoquant la mort de l'employé de maintenance et de deux autres employés.

Un autre accident impliquait le chargement d'un réacteur avec 946 litres (250 gallons) de VCM alors que la vanne de fond du réacteur était ouverte. Ce dégagement a créé un grave danger, mais aucune inflammation ne s'est produite et personne n'a été blessé. D'autres incidents sont notés, comme celui dans lequel une explosion s'est produite pendant les travaux de maintenance sur une pompe de chlorure de vinyle (à cause de la présence d'un contaminant polyperoxyde résultant de trois situations anormales simultanées). Du VCM a également été libéré à partir d'un épurateur dans une installation de production de VCM en raison de problèmes de maintenance avec une vanne bloquée pendant le rechargement périodique. L'inflammation du VCM a provoqué un décès et plusieurs blessures.

Il y a également eu des dégagements de VCM et des incendies liés au transport. Un déraillement de 16 wagons à proximité de Houston, au Texas (Etats-Unis) a provoqué le dégagement de VCM d'un train-citerne de 182 000 litres (48 000 gallons), déclenchant une inflammation immédiate. Après 45 minutes d'exposition à l'incendie, un second wagon de VCM s'est violemment rompu, produisant une énorme boule de feu qui a tué un pompier et blessé 37 autres personnes. Après l'explosion, de grandes parties d'un wagon-citerne ont été trouvées à environ 120 mètres (400 pieds) de l'endroit du déraillement.

En outre, de nombreux incidents mineurs sont susceptibles de se produire pour chaque accident majeur répertorié. Il convient de porter une attention particulière au potentiel de petits dégagements puisqu'ils peuvent être des voies partielles menant à de graves accidents. Particulièrement avec des matériaux sous pression très inflammables, de petits dégagements qui s'enflamment peuvent provoquer de plus grandes défaillances s'ils chauffent d'autres appareils du système. Il convient donc que l'intégrité d'un système VCM soit à un niveau élevé.

Tableau F.3 – Propriétés physiques du chlorure de vinyle

Formule: CH_2=CHCl
Synonymes: monomère chlorure de vinyle (VCM)
Monochloroéthylène
Chloroéthène
Chlorure de vinyle (VCI)
Transporté sous forme de gaz liquéfié comprimé; pression = 5,17 bar.a /75 psia
Gaz, incolore, odeur douceâtre, masse mol. = 62,5; Dens. Grav. (vap) = 2,16
Point d'ébullition normal = -13,4 °C/7,1 °F; Dens. Gr. (liqNBP) = 0,97; Flotte et bout dans l'eau
Température critique = 431 K/317 °F; pression critique = 55,4 bar.a / 775 psia; point de fusion = -154 °C/-245 °F
Chaleur de vaporisation = 372,16 kJ/kg / 160 Btu / lb; chaleur de combustion = 18 924 kJ/kg / 8 136 Btu/lb
Chaleur de polymérisation = 1 695,6 kJ/kg/-729 Btu/lb; normalement stable dans des conditions ambiantes; il se polymérise en présence d'air, de lumière du soleil, d'humidité, de chaleur ou d'initiateurs radicaux libres, sauf s'il est stabilisé avec des inhibiteurs.
DANGERS LIES AUX INCENDIES:
Limite d'inflammabilité dans l'air: 3,6–33 %
Point d'éclair: -61 °C/-108 °F (en creuset ouvert); Autoallumage *T* = 472 °C/882 °F
Déclenche un éclair, bout et produit un nuage de gaz plus lourd que l'air qui peut être enflammé avec un retour de flamme.
Gaz toxiques (HCL, CO, etc.) produits dans l'incendie
Peut exploser si s'enflamme dans un espace confiné
L'exposition de l'incendie externe au contenant peut devenir un BLEVE
DANGERS LIES A LA SANTE:
Vapeur irritante pour les yeux, le nez et la gorge.
Si elle est inhalée, elle provoque des vertiges, des difficultés respiratoires et peut entraîner de graves effets néfastes, voire la mort.
Une exposition excessive peut développer des effets sur les poumons, le foie et les reins. Carcinogène humain listé par l'OSHA, l'International Agency for Research on Cancer (IARC), et l'US National Institute of Health National Toxicology Program (NTP).
Valeur du seuil: 5 ppm
OSHA PEL: MPT égale à 1 ppm, limite d'excursion moyenne de 5 ppm sur toute période n'excédant pas les 15 minutes.
Seuil d'odeur: 260 ppm
Un contact avec le liquide peut provoquer des gelures.
POLLUTION DE L'EAU:
Limite dans l'eau de processus: 10 ppm
Limite dans l'eau déversée hors du site: 1 ppm
EMISSIONS ATMOSPHERIQUES:
Limite dans le déchargement de processus dans l'atmosphère: 10 ppm (norme locale)
Limite de concentration annuelle à la limite de l'installation: 0,2 $\mu g/m^3$ VCM dans l'air
REPONSE A LA DECHARGE:
Adresser un avertissement: inflammabilité élevée, supprimer les sources d'inflammation, ventiler
Arrêter le flux
Evacuer la zone, ne permettre l'entrée qu'avec l'équipement de protection approprié
Laisser brûler les grands incendies; éteindre les petits incendies avec de la poudre extinctrice ou avec du CO_2
Refroidir le contenant exposé avec de l'eau
Empêcher l'entrée dans les systèmes d'assainissement afin d'éviter des explosions potentielles

F.6 Considérations de sécurité de conception du processus préliminaire

Dans cet exemple, la capacité de production souhaitée de PVC est de 90 millions de kilogrammes/200 millions de livres par an ou d'environ 10 400 kg/h/23 000 lb/h. Selon la cinétique de réaction connue, à une température de réaction d'environ 60 °C/140 °F, la durée de cycle correspondante est d'environ 8 heures. En configurant le stock du réacteur, la décision est généralement prise en sachant que la magnitude de danger pour une défaillance catastrophique du réservoir est relative à la quantité de matériaux dangereux. A un extrême, un seul réacteur pourrait être utilisé, avec un lot de production de 81,6 tonnes/180 000 lb de PVC dans un mélange de boue de 40 %, exigeant un réacteur dimensionné pour disposer d'une capacité d'environ 189 000 litres/50 000 gallons. Cette décision ne serait pas raisonnable, puisqu'aucune redondance n'est présente et qu'il s'agit d'un très grand stock à pression élevée et inflammable. De plus, puisque la capacité n'est pas distribuée, les lots de production seraient grands et peu fréquents et exigeraient des équipements en aval dimensionnés pour contenir de grands stocks. En outre, ce réacteur exigerait l'addition d'une grande quantité de la solution initiatrice dangereuse, correspondant à un stock suffisamment considérable pour soulever de sérieuses inquiétudes à propos de la sécurité.

A l'autre extrême, un grand nombre de petits réacteurs (dix, par exemple) conçus chacun pour un lot de production de 8,16 tonnes/18 000 lb (environ 18 900 litres/5 000 gallons) peuvent être utilisés. Pour le premier extrême, les stocks sont grands. Pour le second, les lots sont petits, les exploitations d'échanges sont beaucoup plus fréquentes et il existe bien plus de lignes, de vannes et de complexités d'interconnexion. Des compromis seraient considérés, en fonction des exigences d'exploitation, de la disponibilité des équipements et du coût, mais également de la sécurité.

La décomposition de telles analyses conduit à sélectionner le nombre de réacteurs en parallèle et la taille de l'unité de réacteur. A ce stade, il est pertinent d'indiquer tout potentiel pour une expansion future de capacité. Dans cet exemple, il est décidé d'installer trois réacteurs en parallèle, dotés chacun d'une capacité de 64 400 litres/17 000 gallons. La solution initiatrice de 20 litres/5 gallons exigée par lot représente une quantité gérable pour une manipulation sûre. Le stock maximal de VCM dans un réacteur est estimé à 27,2 tonnes/60 000 lb.

La température de réaction est sélectionnée pour parvenir à une masse moléculaire souhaitée, qui est axée sur l'utilisation finale. Un contrôle de la température de l'eau de refroidissement du réacteur approprié est exigé pour l'exploitation stable du réacteur afin d'éviter une réaction de fuite. Le contrôle stable de la température de réaction de polymérisation exige une faible différence de température entre l'eau de refroidissement et la température de réaction. Pour cet exemple, la température d'alimentation de l'eau de refroidissement tempérée est suffisamment élevée pour procurer une faible différence de température, par opposition aux 60 °C/140 °F de la température de réaction, pour une exploitation sûre. L'eau de refroidissement tempérée provient d'une source établie et très fiable avec une quantité et une pression suffisantes disponibles.

Pour cet exemple, par hypothèse, les vannes de limitation et les vannes de l'évent mènent à un épurateur afin que les déchargements ne provoquent pas d'incident sur l'environnement.

F.7 Dangers de processus reconnus

Les principaux dangers importants associés au dégagement de VCM sont l'incendie et l'explosion, qui entraînent la génération de produits de combustion toxiques. Ces types de dangers incluent les dangers suivants:

a) Jet de feu: Une fuite d'un système pressurisé s'enflamme et forme un jet brûlant qui pourrait heurter d'autres équipements et causer des dommages. En substance, la longueur du jet équivaut à environ 150 fois le diamètre de l'orifice du jet, un jet issu d'un orifice de 50 mm/2 pouces qui pourrait produire un jet brûlant d'environ 9 mètres/30 pieds de long.

b) Embrasement éclair: Un liquide pressurisé libère des éclairs, qui produisent de la vapeur inflammable qui se déplace jusqu'à une source d'inflammation. Au moment de l'inflammation, la flamme retourne à son point d'origine à travers le nuage de vapeur inflammable. Dans ce cas, le panache inflammable peut être beaucoup plus grand que le jet de flamme.

c) Feu en nappes: Du liquide résiduel provenant de la libération d'un éclair forme une nappe qui peut s'enflammer et brûler, générant une flamme haute de trois fois la largeur de la nappe.

d) Liquide bouillant dégageant des vapeurs explosives (BLEVE): Un réservoir sous pression de VCM ou de tuyauterie associée exposé à un feu externe peut être endommagé à cause de l'affaiblissement métallurgique. Une telle défaillance peut causer une défaillance du réservoir catastrophique, une boule de feu et la flambée potentielle de fragments. La protection contre la surpression de la vanne de limitation n'empêchera pas le liquide bouillant dégageant des vapeurs explosives (BLEVE).

e) Explosions: La fuite de gaz inflammable dans un espace confiné et l'inflammation qui en découle peut mener à des explosions ou des détonations avec des surpressions considérables.

f) Défaillance hydraulique: Le remplissage excessif d'un réservoir et l'expansion de liquide qui en découle lors du chauffage peuvent mener à l'effondrement de tout espace de vapeur et à une pressurisation rapide. La défaillance soudaine du réservoir peut se produire.

g) Défaillance de corrosion sous contrainte: La quantité d'air (d'oxygène) dans le système peut augmenter la présence d'ions de chlorure et peut mener à la perte d'intégrité métallurgique.

h) Produits de combustion toxiques: Les produits de combustion de VCM comprennent du phosgène, du chlorure d'hydrogène et du monoxyde de carbone avec d'autres toxiques. (Ces éléments seront présents après un feu, en particulier si le feu a pris dans un espace confiné).

i) Réaction de polymérisation d'emballement: La polymérisation de VCM a le potentiel pour provoquer une rupture du réacteur, libérant le VCM susceptible de provoquer des dommages importants.

De plus, le VCM présente des dangers d'exposition chronique puisqu'il est un carcinogène humain reconnu et une substance régulée. L'exposition du personnel à ses vapeurs est limitée par un OSHA PEL (limite d'exposition du personnel – moyenne pondérée) de 1 ppm dans l'air sur 8 heures (limite de 5 ppm sur 15 minutes). De plus, les réglementations fédérales et locales limitent son niveau de décharge des processus d'évent et des systèmes de traitement des eaux de l'installation. Des limites rigoureuses ont aussi été définies concernant le VCM résiduel qui peut être présent dans le produit PVC.

L'inhalation de vapeurs de VCM et le potentiel d'autoréfrigération des fluides instantanés provoquent des dangers à court terme moindres. Il est exigé que le personnel soit protégé contre l'inhalation et les brûlures provoquées par le gel.

A ce stade, les estimations de la portée des zones de danger sont menées pour indiquer la magnitude des accidents potentiels importants. La libération de 27,2 tonnes/60 000 lb de VCM pourrait produire un nuage de vapeur inflammable équivalent au volume contenu par un cube de près de 120 mètres/400 pieds de côté. Le VCM étant un gaz lourd et pouvant contenir des aérosols dus aux éclairs, un nuage de vapeur important est plus susceptible de prendre une forme de crêpe tout en ayant une empreinte inflammable de 300 à 450 mètres/1 000 à 1 500 pieds de diamètre. Cela indique que l'accident le plus grave impliquant un seul réacteur pourrait avoir des répercussions hors site et pourrait remplir un volume confiné considérable de gaz inflammable. Selon les termes des critères d'évaluation traités au Tableau F.8 ci-dessous, il convient de considérer ces répercussions au moins comme "graves", voire "très graves", en fonction des données spécifiques considérées. Pour se montrer prudente, l'équipe PHA considère que ces répercussions relèvent de la catégorie "très grave". *(Note:* Le stockage en vrac de VCM sur site n'est pas pris en compte dans cet exemple limité.)

F.8 Stratégie des définitions de conception du processus

Les détails de la conception exigent la définition des procédures d'exploitation de base et des stratégies de maintenance de l'installation. La Figure F.3, un schéma P&I préliminaire, est donnée pour faciliter la tâche. Les étapes opérationnelles du processus sont mentionnées ci-dessous:

a) Pré évacuation de l'air: Si les réacteurs ont été ouverts pour la maintenance, il convient de purger l'oxygène du système pour des raisons de qualité et d'intégrité métallurgique.

b) Préparation du réacteur: Le réacteur vide est rincé avec de l'eau à pression élevée, soumis à des essais de fuite si l'écoutille a été ouverte et traité avec un produit antisalissure.

c) Chargement de l'eau déminéralisée: Une charge d'eau contrôlée est ajoutée. Une surcharge pourrait mener à un débordement hydraulique; une insuffisance peut causer des problèmes qualitatifs et une réaction d'emballement potentielle. Un surfactant ou un autre additif est introduit au cours de cette étape.

d) Chargement de VCM: Une charge précise de VCM est ajoutée au réacteur.

e) Chauffage du réacteur: L'initiateur est ajouté du pot de charge au lot et de la vapeur est ajoutée à l'eau de refroidissement qui circule à travers la chemise du réacteur, jusqu'à ce que le lot atteigne la température à laquelle la réaction se produira (environ 5,5 °C/10 °F en dessous de la température de réaction en régime établi).

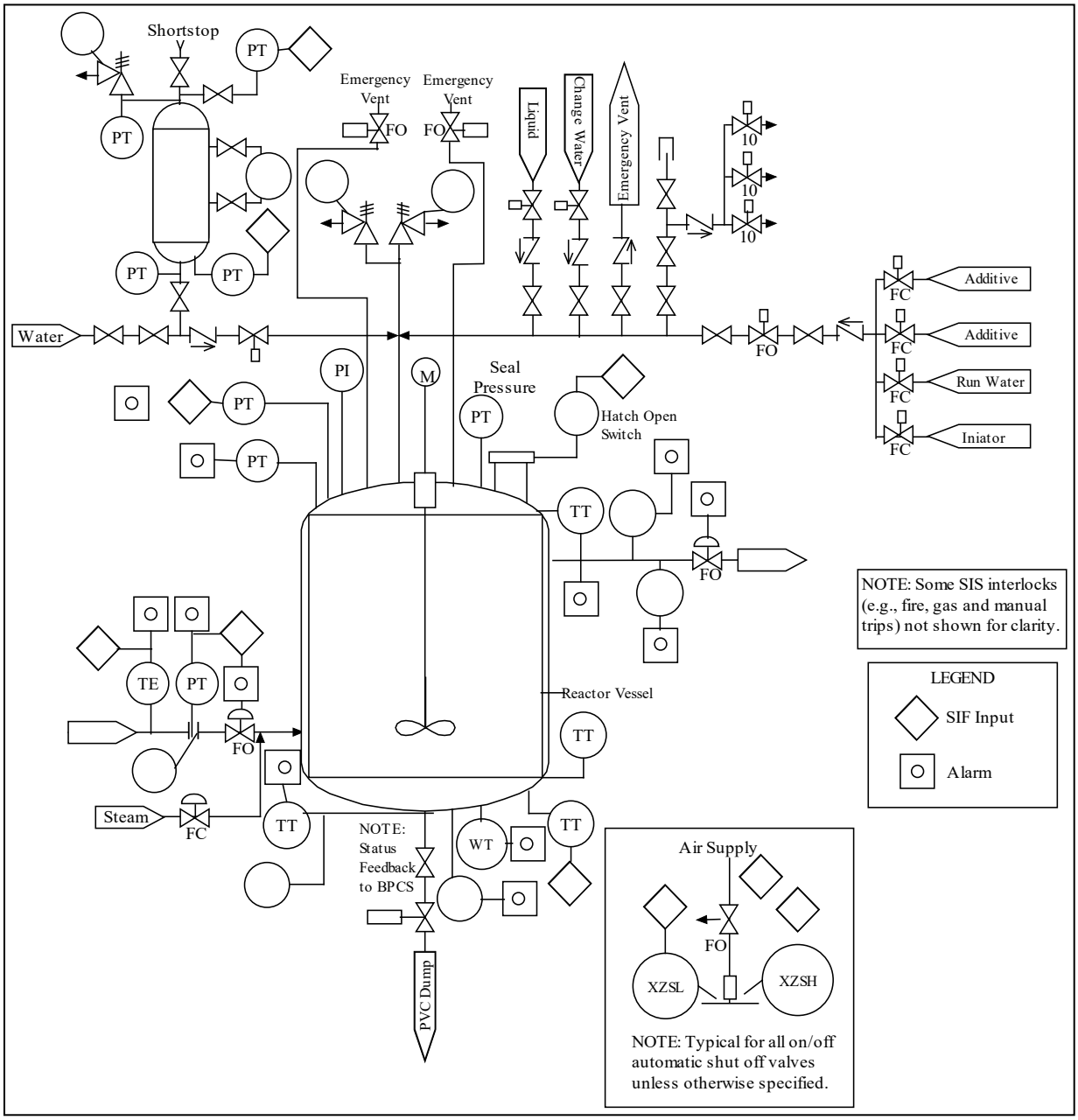
f) Réaction: Le système à vapeur est isolé, et de l'eau de refroidissement circule à travers la chemise du réacteur pour contrôler la température en dissipant la chaleur de la polymérisation pendant la progression de réaction.

g) Largeur brasable: Lorsque la pression du réacteur commence à diminuer (la plus grande partie du VCM présent ayant été consommée par la polymérisation), le lot sera déchargé.

h) Décharge du réacteur: Le contenu du réacteur est déchargé sous pression vers une installation de récupération en aval où le système est dégazé pour ensuite être dilué et séché. Pour éviter que de la résine s'installe dans le réacteur, l'agitateur est exécuté au cours de la procédure de décharge. Le VCM n'ayant pas réagi est récupéré pour être réutilisé.

Il existe deux systèmes de processus supplémentaires fournis pour une situation d'urgence. Dans l'éventualité d'une réaction non contrôlée ou du potentiel pour un tel événement, la polymérisation peut être arrêtée rapidement grâce à l'ajout d'un agent chimique d'arrêt court (agent d'arrêt de chaîne) au lot. Toutefois, il est nécessaire d'agiter le lot pour que l'agent d'arrêt court soit également distribué afin de terminer rapidement la polymérisation. Si l'agitateur a échoué, il convient d'ajouter l'agent d'arrêt court dans un délai d'une minute ou deux, pour permettre le mélange avant que le tourbillon de liquide se dissipe dans le réacteur. Comme système de secours, le contenu du réacteur peut être mélangé par "renvoi" du réacteur, diminuant la pression pour générer des bulles dans la masse liquide en vrac. Ces deux événements sont activés par un opérateur.

Le second système d'urgence est un système de dépressurisation automatique. Dans l'éventualité d'une réaction non contrôlée, la réaction peut être limitée en toute sécurité en dépressurisant le réacteur vers le système d'évacuation. La chaleur de la vaporisation de la masse de réaction d'ébullition élimine en toute sécurité la chaleur du réacteur. Le système d'évacuation d'urgence sera de taille à prendre en charge les crêtes de besoins d'évacuation du système du réacteur.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
Shortstop	Arrêt court
Emergency vent	Ventilation d'urgence
Liquid	Liquide
Change water	Changement d'eau
Water	Eau
Additive	Additif
Run water	Eau courante

Anglais	Français
Initiator	Initiateur
Seal pressure	Pression du sceau
Hatch open switch	Commutateur ouvert écoutille
NOTE Some SIS interlocks (e.g., fire, gas and manual trips) are not shown for clarity.	NOTE Certains verrouillages du SIS (p. ex.: feu, gaz et déclenchements manuels) ont été omis pour plus de clarté.
Reactor vessel	Réservoir du réacteur
LEGEND SIF input Alarm	LEGENDE Entrée de la SIF Alarme
Steam	Vapeur
NOTE Status feedback to BPCS	NOTE Information sur l'état retournée au BPCS
Air supply	Alimentation en air
PVC dump	Déchargement PVC
NOTE Typical for all on/off automatic shut off valves unless otherwise specified.	NOTE Type pour toutes les vannes de fermeture automatique activées/désactivées, sauf indication contraire.
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.3 – Exemple de schéma de tuyauterie et d'instrumentation préliminaire pour unité de réacteur PVC

Les collecteurs de tuyauterie sont représentés de manière consolidée à des fins de transparence. Voir la Figure F.11 pour la clarté des collecteurs.

F.9 Evaluation du danger préliminaire

F.9.1 Généralités

Une fois la conception développée en détail, l'équipe PHA a soumis la conception à une évaluation du danger préliminaire. L'évaluation est considérée comme préliminaire car la conception n'est pas encore terminée. L'équipe PHA a utilisé une revue de simulation/liste de contrôle (Tableau F.4) pour les parties les plus simples du processus, et une étude HAZOP (Tableau F.5) pour les parties plus complexes du processus.

Selon le processus d'identification du danger et l'historique des accidents passés, il semble que l'exemple de réacteur du processus présente un potentiel d'événements de gravité "mineure" jusqu'à "très grave" (voir le Tableau F.8).

De plus, il convient pour l'intégrité de la conception de satisfaire aux besoins de conformité aux exigences pour prévenir l'émission de VCM qui pourrait compromettre la sécurité et la santé des employés. Il convient de documenter minutieusement les résultats de cette revue du danger et de porter une attention toute particulière aux séquences d'événements pouvant mener à des émissions non contrôlées.

Le Tableau F.4 et le Tableau F.5 répertorient en partie les dangers correspondant à cet exemple. Un projet type présenterait une liste beaucoup plus longue d'éléments de simulation et HAZOP.

Tableau F.4 – Simulation/Liste de contrôle

Préparé et approuvé par l'équipe d'analyse des dangers du processus (voir l'Article F.2).

Simulation...	Danger	Conséquences	Protections	N° Réf	Recommandations	Par
Simulation d'une défaillance de puissance électrique étendue de la zone. (L'énergie de l'instrumentation UPS demeure)	Réaction d'emballement au cours de la perte d'agitation. Indiqué par la désactivation du moteur de l'agitateur, un flux de refroidissement faible, une pression du réacteur élevée et une température du réacteur élevée.	La réaction d'emballement provoque la surpression et la perte de confinement du réacteur.	Ajouter un arrêt court et un réacteur d'émission de gaz pour arrêter la fuite. Dépressuriser le réacteur – SIS (soupapes de sécurité adaptée à cet événement).		Utiliser LOPA pour déterminer le SIL exigé	
Erreur de formule de lot – deux charges de l'initiateur sont utilisées	La concentration élevée de l'initiateur provoque une réaction d'emballement. Indiqué par la température et la pression du réacteur élevées.	La réaction d'emballement mène à la surpression et à la perte de confinement du réacteur.	Ajouter un arrêt court. Dépressuriser le réacteur – SIS (soupapes de sécurité adaptée à cet événement).		Utiliser LOPA pour déterminer le SIL exigé	
Simulation d'une défaillance du sceau de l'agitateur du réacteur	Emission de fumée du VCM. Indiqué par une pression élevée dans le sceau du réacteur et le détecteur de fumée de la zone.	Les fumées du VCM sont inflammables.	Ventilation supplémentaire autour du sceau du réacteur. Dépressuriser le réacteur sous pression élevée du sceau – SIS.		Utiliser LOPA pour déterminer le SIL exigé	
NOTE Il ne s'agit que d'une liste partielle des dangers.						

Tableau F.5 – HAZOP

Préparé et approuvé par l'équipe d'analyse des dangers du processus (voir l'Article F.2).

Mots-guides (GW)	Ecart	Causes	Conséquences	Protections	N° Réf	Recommandations	Par
Non	Pas de flux	Défaillance du système de contrôle de l'eau de refroidissement	Une réaction d'emballement éventuelle via une température élevée et/ou une pression élevée du réacteur	Ajouter un arrêt court. Dépressuriser le SIS du réacteur (soupapes de sécurité de surpression adaptée à cet événement)		Utiliser LOPA pour déterminer le SIL exigé	
		Arrêt de la pompe dû à une défaillance de puissance de la pompe	Une réaction d'emballement éventuelle via une température élevée et/ou une pression élevée du réacteur	Une transmission de vapeur se trouve sur la pompe en plus de la puissance électrique. Ajouter un arrêt court. Dépressuriser le SIS du réacteur (soupapes de sécurité de surpression adaptée à cet événement)		Utiliser LOPA pour déterminer le SIL exigé	
Non	Pas d'agitation	Défaillance de l'entraînement du moteur de l'agitateur	La température de refroidissement réduite et la non-uniformité mènent à une réaction d'emballement. Comme indiqué par la température et la pression du réacteur élevées ainsi que la faible intensité du moteur de l'agitateur.	Ajouter un arrêt court et un réacteur d'émission de gaz pour arrêter la fuite. Dépressuriser le SIS du réacteur (soupapes de sécurité de surpression adaptée à cet événement)		Utiliser LOPA pour déterminer le SIL exigé	
Plus	Température plus élevée	La défaillance du contrôle de la température provoque une surchauffe au cours du chauffage de la vapeur	Une température élevée conduit à une réaction de fuite. Indiqué par la pression et la température du réacteur élevées.	Ajouter un arrêt court. Dépressuriser le SIS du réacteur (soupapes de sécurité de surpression adaptée à cet événement)		Utiliser LOPA pour déterminer le SIL exigé	
Plus	Niveau le plus élevé	La défaillance de contrôle du niveau permet le débordement du réacteur	Le réacteur devient complètement liquide au fur et à mesure que la température augmente; possibilité de dommage de réacteur hydraulique et libération VCM. Indiqué par un niveau de charge, un poids de charge et une pression du réacteur élevés.	Comparer le niveau et le poids élevés avec la formule. Dépressuriser le SIS du réacteur (soupapes de sécurité de surpression adaptée à cet événement)		Utiliser LOPA pour déterminer le SIL exigé	
NOTE Il ne s'agit que d'une liste partielle des dangers.							

D'après ces résultats, une équipe de processus PHA appropriés et des experts de l'instrumentation ont établi une liste des événements accidentels où les SIF peuvent servir à atténuer le danger.

Le Tableau F.6 liste partiellement les événements accidentels et les stratégies préventives associées utilisés pour proposer une stratégie et des actions de verrouillage afin d'aider à identifier ou à créer des couches de protection indépendantes supplémentaires. Le Tableau F.6 a été préparé et approuvé par l'équipe d'analyse des dangers du processus (voir l'Article F.2).

Tableau F.6 – Récapitulatif partiel de l'évaluation du danger pour le développement de stratégie SIF

N°	Initiation de l'événement	Perte de contrôle du processus	Variables du processus concernées	Stratégie préventive
1	Défaillance du contrôle de l'eau de refroidissement	Perte de refroidissement qui conduit à une réaction de fuite	– Faible C.W.* Flux – Temp. du réacteur élevée – Pression du réacteur élevée	– Ajouter un arrêt court – Dépressuriser le réacteur (SIS) – Soupapes de sécurité (IPL)
2	Défaillance de l'entraînement du moteur de l'agitateur	La réduction du refroidissement et la non-uniformité mènent à une réaction d'emballement	– Faible intensité du moteur de l'agitateur – Temp. du réacteur élevée – Pression du réacteur élevée	– Ajouter un arrêt court et un réacteur d'émission de gaz pour arrêter la fuite. – Dépressuriser le réacteur (SIS) – Soupapes de sécurité (IPL)
3	Perte de la puissance électrique normale sur toute une zone (l'énergie de l'instrumentation UPS demeure)	Perte d'agitation qui conduit à une réaction de fuite	– Moteur de l'agitateur désactivé – Débit de refroidisseur faible – Pression du réacteur élevée – Temp. du réacteur élevée	– Ajouter un arrêt court et un réacteur d'émission de gaz pour arrêter la fuite. – Dépressuriser le réacteur (SIS) – Soupapes de sécurité (IPL)
4	Arrêt des pompes d'eau de refroidissement, défaillance de puissance de la pompe	Perte de refroidissement qui conduit à une réaction de fuite	– Faible C.W. Flux – Temp. du réacteur élevée – Pression du réacteur élevée	– Injection de vapeur sur les pompes – Ajouter un arrêt court – Dépressuriser le réacteur (SIS) – Soupapes de sécurité (IPL)
5	Erreur de formule de lot; deux charges de l'initiateur sont utilisées.	La concentration élevée de l'initiateur provoque une réaction d'emballement	– Pression du réacteur élevée – Temp. du réacteur élevée	– Ajouter un arrêt court – Dépressuriser le réacteur (SIS) – Soupapes de sécurité (IPL)
6	La défaillance du système de commande provoque le débordement du réacteur	Le réacteur devient complètement liquide au fur et à mesure que la température augmente; possibilité de dommage de réacteur hydraulique et libération VCM.	– Niveau de forte charge – Poids de forte charge – Pression du réacteur élevée	– Comparer le niveau et le poids avec la formule – Dépressuriser le réacteur (SIS) – Soupapes de sécurité (IPL)

N°	Initiation de l'événement	Perte de contrôle du processus	Variables du processus concernées	Stratégie préventive
7	La défaillance du contrôle de la température provoque une surchauffe au cours de l'étape de chauffage de la vapeur	Une température élevée conduit à une réaction de fuite.	– Pression du réacteur élevée – Temp. du réacteur élevée	– Ajouter un arrêt court – Dépressuriser le réacteur (SIS) – Soupapes de sécurité (IPL)
8	Défaillance du sceau de l'agitateur du réacteur	La défaillance du sceau peut mener à des émissions de fumée VCM dangereuses	– Pression élevée dans le sceau du réacteur – Détection de fumée dans la zone de réaction	– Ventilation supplémentaire autour du sceau – Dépressuriser le réacteur sous pression élevée du sceau (SIS)
* C.W. signifie eau de refroidissement.				

L'identification des dangers identifiés ci-dessus a permis à l'équipe PHA d'établir les recommandations suivantes:

a) Mise en œuvre de la stratégie préventive du SIS suivante qui traite les scénarios de réaction de fuite:

   – Si une condition de température ou de pression élevée se produit, l'opérateur dispose d'assez de temps pour ajouter un arrêt court à distance.

   NOTE Pour les éléments 2 et 3 du Tableau F.6, une "émission de gaz" du réacteur est exigée suite à l'ajout de l'arrêt court pour le mélanger dans la masse de réaction, étant donné que l'agitateur ne fonctionne pas.

   – Si cela ne suffit pas à arrêter la fuite, la température ou la pression très élevée de la SIF ouvrira les vannes de ventilation de dépressurisation d'urgence pour contrôler l'emballement en toute sécurité.

b) Pour les fuites qui surviennent parce que l'agitateur ne fonctionne pas (élément 2 et 3 du Tableau F.6), une protection est nécessaire en plus des recommandations données au point a) ci-dessus:

   – La perte d'agitation (faible intensité) sera indiquée à l'opérateur par une alarme. Après l'ajout de l'arrêt court, une "émission de gaz" doit mélanger l'arrêt court dans la masse de réaction.

   – Tel qu'indiqué dans la recommandation a) ci-dessus, les SIF de dépressurisation d'urgence constituent un système de secours pour contrôler la fuite.

c) Les pertes de contrôle du flux d'eau de refroidissement faible ou inexistant sont contrôlées par la protection de la recommandation a) ci-dessus. Si un flux d'eau de refroidissement faible a été causé par une perte de puissance des pompes à eau, l'alarme de flux faible indique à l'opérateur d'activer la transmission de pompe à eau de la turbine à vapeur.

d) Surcharger le réacteur d'eau ou de VCM peut provoquer le débordement et des dommages possibles de surpression hydraulique du réacteur. Cette perte de contrôle est évitée en prévenant le chauffage du lot si les cellules de poids ou le niveau du réacteur excèdent la limite "élevée" pour cette étape d'ajout du lot dans le BPCS. Un système de secours est fourni par la SIF de pression du réacteur "très élevée", qui active les vannes de ventilation de dépressurisation d'urgence.

e) La défaillance du sceau de l'agitateur du réacteur provoque des émissions dangereuses de VCM. Afin de se prémunir contre cela, il est recommandé d'activer la ou les SIF de dépressurisation d'urgence en cas de pression élevée dans le sceau de l'agitateur.

f) Le système d'arrêt court étant très important pour le contrôle des réactions de fuite, l'équipe recommande également les verrouillages dans le BPCS afin de garantir la disponibilité d'arrêt court. Les verrouillages du BPCS ne permettent pas de charger le VCM dans le réacteur si le niveau du réservoir d'arrêt court est trop faible ou si la pression de la plage d'azote de ce réservoir est trop faible.

F.9.2 Etape F.2: Affectation des fonctions de sécurité

Le Tableau F.7 fournit une vue des éléments clef dans l'affectation des fonctions de sécurité.

Tableau F.7 – Cycle de vie de sécurité du SIS – Zone 2

Présentation					
Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigences** **Article ou paragraphe de l'IEC 61511-1:2016**	**Entrées**	**Sorties**
IEC 61511-1:2016 Figure 7, zone 2	Affectation des fonctions de sécurité aux couches de protection	Affectation des fonctions de sécurité aux couches de protection et pour chaque SIF, le SIL associé	9	Description des SIF exigées et des exigences associées concernant l'intégrité de sécurité	Description de l'affectation des exigences de sécurité (voir l'Article 9 de l'IEC 61511-1:2016)

F.10 Détermination du niveau d'intégrité de sécurité de la SIF

D'après la liste de SIF proposée, l'équipe PHA se réunit pour déterminer le SIL exigé pour la SIF. La méthode d'analyse de la couche de protection (LOPA) sera utilisée. Pour une description de la méthode LOPA, voir l'IEC 61511-3:—, Annexe F. Des lignes directrices supplémentaires sont fournies par l'AIChE, CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment,* 2001.

F.11 Analyse de la couche de protection (LOPA) appliquée à un exemple

L'Article F.11 explique la transition des données présentées dans le résumé partiel des informations sur l'évaluation du danger (Tableau F.6) vers la LOPA (Tableau F.9).

La liste ci-dessous présente des descriptions de scénario LOPA:

– Evénement 1: Défaillance du contrôle de l'eau de refroidissement

Cette perte de contrôle initie une réaction de fuite qui peut causer la rupture catastrophique du réacteur. L'impact de cet événement a été jugé "très grave" ce qui, comme indiqué au Tableau F.8 Note 1, donne une fréquence tolérable de 10^{-5}/an pour un seul scénario. Plusieurs défaillances du système de commande pourraient causer cette perte de contrôle. L'expérience d'exploitation prouve que ce type de perte de contrôle a lieu environ une fois tous les dix ans. La protection selon le Tableau F.6 était assurée par l'ajout de l'arrêt court, mais la réaction de fuite peut être trop rapide et ne pas laisser le temps à l'opérateur de répondre à une alarme. Cette couche de protection n'est pas incluse pour la réduction du risque. La zone étant occupée normalement, il a été pris pour hypothèse que le personnel pourrait être affecté par l'événement. Les soupapes de sécurité de surpression (PSV) ont une efficacité estimée à seulement 90 %, le blocage étant un problème courant au sein de ce service. Les PSV partageant une ligne de limitation commune, elles sont considérées, par mesure de prudence, comme une seule couche de protection indépendante. Cela a mené à une probabilité d'événement intermédiaire de 10^{-2} par an. Selon les hypothèses prudentes utilisées dans cet exemple, seules les PSV sont qualifiées d'IPL. L'équipe PHA a revu tous les problèmes de risque de sécurité du processus et a décidé qu'une SIF était appropriée. Comme le montre le Tableau F.9, cela exige une SIF de SIL 3.

NOTE Les PSV sont nécessaires pour assurer la conformité aux codes relatifs aux récipients sous pression mais, comme le montre la LOPA (qui utilise le critère de risque d'entreprise du Tableau F.8), ils n'offrent pas la sécurité nécessaire pour satisfaire à la limite de risque de ce scénario. Cette note est valable pour tous les scénarios LOPA de cet exemple.

– Evénement 2: Défaillance de l'entraînement du moteur de l'agitateur

Cette perte de contrôle est à l'origine d'une réaction de fuite similaire à celle de l'événement n° 1. Toutefois, étant donné que l'agitation s'est arrêtée, l'étape supplémentaire d'émission de gaz du réacteur (F.8) est exigée pour interrompre la réaction de fuite par l'ajout d'un arrêt court. A nouveau, cette fuite peut être tellement rapide que l'opérateur peut ne pas avoir la possibilité de répondre. Ainsi, aucune réduction du risque n'est prise pour la réponse des opérateurs aux alarmes. Plusieurs défaillances du système de commande de l'agitateur pourraient causer cette perte de contrôle. L'expérience d'exploitation prouve que ce type de perte de contrôle a lieu environ une fois tous les dix ans. La SIF S-1 est la seule SIF efficace pour cet événement et elle exige un SIL 3.

– Evénement 3: Perte de la puissance électrique sur une zone entière

Bien que la perte de contrôle soit différente de celle de l'événement F.2, la sélection du SIL de la SIF produit un résultat similaire à celui de l'événement F.2.

– Evénement 4: Défaillance de la puissance de pompe de l'eau de refroidissement

La perte de contrôle de l'événement 4 s'apparente à celle de l'événement 1. L'intervention d'un opérateur peut arrêter cette fuite par l'activation des pompes à eau actionnées par une turbine à vapeur ou par l'ajout de l'arrêt court. Bien que cette action d'opérateur ait été jugée très efficace, aucune confiance relative à la réduction du risque ne lui a été accordée en raison de la disponibilité de l'opérateur. L'analyse présentée au Tableau F.9 a mené au SIL 3 pour la SIF S-1.

– Evénement 5: Charge double de l'initiateur

Cette perte de contrôle engendre une réaction de fuite très énergique avec un taux élevé de génération de chaleur et l'augmentation rapide de la pression malgré l'exploitation de l'eau de refroidissement. L'augmentation de la pression serait trop rapide pour considérer la température comme mesure efficace de déclenchement de la SIF. Les PSV et la SIF de dépressurisation sont conçues pour contrôler cette fuite en toute sécurité. En raison des fonctionnalités de sécurité de conception et de procédure, cette perte de contrôle exige une combinaison de défaillances très peu probable. Ainsi, une probabilité d'occurrence d'événement modérée de 10^{-1} a été sélectionnée. La probabilité modérée, un IPL non-SIS et le niveau de gravité "très important" ont induit un SIL 3 pour la SIF S-2.

– Evénement 6: Débordement du réacteur causé par une défaillance du système de commande

Les conséquences de cette perte de contrôle causeraient la surpression hydraulique du réacteur, provoquant la rupture du joint de bride ou une émission similaire. Avec le grand nombre de lots par an et leurs formules variées, la probabilité d'occurrence d'un tel événement est jugée modérée (1 tous les 10 ans). L'efficacité des alarmes de cellules de niveau et de poids du BPCS avec l'intervention d'un opérateur a été évaluée à 90 % par l'équipe (10^{-1}) car les alarmes sont localisées dans un contrôleur BPCS séparé. Les vannes de sécurité de pression et le SIS de dépressurisation seront efficaces pour la gestion de cette perte de contrôle. Le niveau de gravité "important" avec une probabilité d'occurrence de l'événement modérée et deux IPL non-SIS ont indiqué qu'un SIL 1 était approprié pour dépressuriser la SIF. Bien qu'une SIF SIL 1 soit indiquée, il convient de concevoir une SIF S-2 pour le SIL 3 selon les exigences de l'événement 5 ci-dessus.

– Evénement 7: Défaillance du contrôle de la température au cours de l'étape de chauffage – Lot surchauffé

Cet événement mène à une réaction de fuite similaire à l'événement 1. Les conséquences et les aspects liés à la protection de l'événement sont similaires à ceux de l'événement 1. Toutefois, le transmetteur de température n'est pas considéré comme étant approprié pour réduire le risque de cet événement. Au cours du chauffage, l'opérateur a le temps d'ajouter l'arrêt court pour éviter la fuite. Cependant, comme le transmetteur de température est utilisé pour le contrôle, il peut faire partie des causes initiatrices de ce danger. Ainsi, la réponse de

l'opérateur relative à une alarme de température élevée ne serait pas un IPL pour cet événement. Il convient de concevoir la SIF S-1 pour le SIL 3, déjà exigé pour l'événement 1.

– Evénement 8: Défaillance du sceau de l'agitateur

La conception du sceau spéciale utilisée pour ce réacteur limite les émissions de VCM à des taux de flux faibles dans le cas d'une défaillance du sceau. La ventilation ponctuelle fournie sera suffisante pour réduire ce danger d'incendie et d'explosion. L'équipe PHA a jugé le niveau de gravité comme "important" et a décidé que la ventilation ponctuelle était efficace à 90 % (10^{-1}). N'ayant pas d'IPL, le niveau de gravité étant "important" et la probabilité étant élevée, selon le Tableau F.9, un SIL de 2 est donc approprié.

F.12 Critères de risque tolérables

Les critères de risque tolérables utilisés pour cet exemple sont présentés au Tableau F.8 ci-dessous.

Ces critères sont spécifiques à l'entreprise. Chaque entreprise devra appliquer ses propres critères de risque lors de la définition des fonctions de sécurité nécessaires et l'accord avec l'autorité de réglementation locale, si applicable.

Tableau F.8 – Classement du risque tolérable

Gravité	Définition	Fréquence tolérable (événements/an) (voir la Note 1)
Très grave	Un ou plusieurs décès ou effet(s) sur la santé irréversible	10^{-4}
Grave	Cas de blessures à traitement médical multiple; 1 ou 2 cas de jours ouvrés réduits ou cas de jours ouvrés perdus ou cas d'effets sur la santé modérés	10^{-3}
Mineur	Blessure mineure ou effets sur la santé réversibles	10^{-2}

NOTE 1 Les fréquences tolérables représentées concernent le risque total de tous les dangers. La fréquence tolérable pour chaque scénario de LOPA est définie sur un ordre de magnitude en dessous pour prendre en compte de nombreux dangers (c'est-à-dire à chaque scénario de gravité "très importante" est assignée une fréquence tolérable de 10^{-5}). Cette approche est acceptable pour cet exemple car la zone d'exploitation n'est pas occupée normalement par les patrouilles d'opérateurs habituels (une seule personne par patrouille). Ils constituent d'ailleurs la raison principale d'exposition du personnel aux dangers associés à cette opération.

NOTE 2 Les données du Tableau F.8 représentent la Norme de l'entreprise.

NOTE 3 L'entreprise utilisée pour cet exemple est une entreprise qui opère en Grande-Bretagne aussi bien qu'aux Etats-Unis. Pour les projets mis en œuvre en Grande-Bretagne, des critères de risque supplémentaire seraient appliqués. En Grande-Bretagne, selon le HSE, le risque d'un événement préjudiciable doit être réduit jusqu'à ce que le coût engendré par toute réduction de risque supplémentaire soit manifestement disproportionné par rapport aux bénéfices obtenus. Références: *Reducing Risk Protecting People*, HSE, ISBN No. 07176-2151-0, publié en 2001; www.hsebooks.co.uk; IEC 61511-3.

Tableau F.9 – Exemple de réacteur VCM: Niveau d'intégrité LOPA

Préparé et approuvé par l'équipe d'analyse des dangers du processus (voir l'Article F.2).

N°	1	2	3	4	5			6	7	8	9	10	11	12
	Evénement à impact	Niveau de gravité/ Fréquence tolérable	Cause initiatrice	Fréquence initiatrice (événements/an)	COUCHES DE PROTECTION			Atténuation supplé-mentaire	Fréquence d'événement intermédiaire (événements/an)	Nombre d'IPL	SIF nécessaire?	Niveau d'intégrité SIF	Fréquence d'événe-ment atténué (par an)	Notes (ID SIF)
					Etude de procédé	BPCS	Alarmes, etc.							
1	Rupture du réacteur	E 10^{-5}	Défaillance du contrôle H2O du refroidisseur	10^{-1}	Non	Non	Non	PSV 10^{-1}	10^{-2}	1 (PSV)	Oui	3 (Dépress.) 10^{-3}	10^{-5}	S-1
2	Rupture du réacteur	E 10^{-5}	Défaillance de l'entraînement du moteur de l'agitateur	10^{-1}	Non	Non	Non	PSV 10^{-1}	10^{-2}	1 (PSV)	Oui	3 (Dépress.) 10^{-3}	10^{-5}	S-1
3	Rupture du réacteur	E 10^{-5}	Perte de puissance électrique normale d'une zone entière	10^{-1}	Non	Non	Non	PSV 10^{-1}	10^{-2}	1 (PSV)	Oui	3 (Dépress.) 10^{-3}	10^{-5}	S-1
4	Rupture du réacteur	E 10^{-5}	Défaillance de la puissance de pompe de l'eau de refroidissement	10^{-1}	Non	Non	Non	PSV 10^{-1}	10^{-2}	1 (PSV)	Oui	3 (Dépress.) 10^{-3}	10^{-5}	S-1
5	Rupture du réacteur	E 10^{-5}	Charge double de l'initiateur	10^{-1}	Non	Non	Non	PSV 10^{-1}	10^{-2}	1 (PSV)	Oui	3 (Dépress.) 10^{-3}	10^{-5}	S-2
6	Surpression hydraulique, dommage du réacteur	S 10^{-4}	Débordement du réacteur, défaillance du système de commande	10^{-1}	Non	Non	Alarmes de cellules de niveau (400 LSH) et de poids (300 WTH)10^{-1}	PSV 10^{-1}	10^{-2}	1 (PSV)	Oui	3 (Dépress.) 10^{-3} (SIL 1 exigé)	10^{-6} (10^{-4} exigé)	S-2
7	Rupture du réacteur	E 10^{-5}	Défaillance du contrôle de la température d'ajout d'excès de vapeur	10^{-1}	Non	Non	Non	PSV 10^{-1}	10^{-2}	1 (PSV)	Oui	3 (Dépress.) 10^{-3}	10^{-5}	S-1
8	Libération de VCM	S 10^{-4}	Défaillance du sceau de l'agitateur	10^{-1}	Ventilation ponctuelle au sceau du réacteur 10^{-1}	Non	Non	Non	10^{-2}	0	Oui	2 (Dépress.) 10^{-2}	10^{-4}	S-3

Niveau de gravité E – très important (*Extensive*); S – grave (*Severe*); M – mineur (voir le Tableau F.8). Les valeurs de probabilité sont des événements par an. Les autres valeurs numériques sont des probabilités.

Pour des raisons de simplification, cet exemple ne prend pas en compte le fait que le réacteur ne soit pas opérationnel 100 % du temps. Il ne prend pas non plus en compte le fait que les dangers existent pour chacun des trois réacteurs.

A l'issue de la LOPA, les probabilités d'événements mitigés pour les scénarios 1 à 5 et 7 ont été ajoutées. La fréquence totale de 6E-5 satisfait aux critères de fréquence tolérable de l'entreprise pour les événements "très graves" de 10^{-4} (voir le Tableau F.8). La fréquence d'événement mitigé totale pour les scénarios 6 et 8 était 1.01E-4, ce qui satisfait aux critères de fréquence tolérable de l'entreprise de 10^{-3} pour les événements "graves".

F.13 Etape F.3: Spécifications des exigences concernant la sécurité du SIS

F.13.1 Présentation

Tableau F.10 – Cycle de vie de sécurité du SIS – Zone 3

Présentation					
Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigences Article ou paragraphe de l'IEC 61511-1:2016**	**Entrées**	**Sorties**
IEC 61511-1:2016 Figure 7, zone 3	SRS du SIS	Spécifier les exigences pour chaque SIS, en termes de SIF exigées et leur intégrité de sécurité associée, afin d'obtenir la sécurité fonctionnelle exigée	10	Description de l'affectation des exigences de sécurité (voir l'Article 9 de l'IEC 61511-1:2016)	Exigences de sécurité du SIS; exigences de sécurité du programme d'application

Les informations de cet exemple de SRS peuvent être contenues dans un format de document unique. D'autre part, elles peuvent également être contenues dans plusieurs documents combinés. Les exigences suivantes concernent cet exemple uniquement.

F.13.2 Exigences d'entrée

Les informations du Tableau F.11, la SIF et les SIL associés, étaient les sorties de l'étape 2 et ont été utilisées pour le développement de la SRS.

Tableau F.11 – Fonctions instrumentées de sécurité et SIL

Identifiant	Variables de processus surveillées	SIL
S-1	Pression et température élevées du réacteur	3
S-2	Pression élevée du réacteur	3
S-3	Pression élevée du sceau de l'agitateur	2

Le BPCS effectue des fonctions opérationnelles pour un démarrage en ordre et une extinction normale. Ces éléments ne sont pas inclus dans cet exemple.

L'équipe PHA a identifié le blocage comme un problème potentiel de cette application. Il convient pour l'équipe de conception de prendre en compte ce problème lors de la conception du SIS.

Aucune exigence réglementaire qui aurait une incidence sur la conception du SIS n'a été identifiée.

F.13.3 Exigences fonctionnelles de sécurité

Le Tableau F.12 énumère l'état de sécurité de chaque SIF et présente la relation fonctionnelle entre les processus d'entrées et de sorties, y compris la logique exigée.

Tableau F.12 – Relation fonctionnelle d'E/S pour la/les SIF

N° de SIF	SIL	Capteur	Description	Etat de sécurité de l'élément terminal
S-1	3	100PT 100PT1 100TT	Si la pression du réacteur est supérieure à 125 psig ou la température du réacteur supérieure à 200 °F	Ouvrir 100PV Ouvrir 100PV1
S-2	3	100PT 100PT1	Si la pression du réacteur est supérieure à 125 psig	Ouvrir 100PV Ouvrir 100PV1
S-3	2	200PT	Si la pression du sceau est supérieure à 10 psig	Ouvrir 100PV Ouvrir 100PV1

Le Tableau F.13 représente les entrées d'instruments de processus du SIS, leur point de déclenchement, les plages de fonctionnement normal et les limites d'exploitation.

Tableau F.13 – Capteurs du SIS, plages de fonctionnement normal et points de déclenchement

Etiquette	Plage d'étalonnage	Plage de fonctionnement normal	Alarme prédéclenchement		Point de déclenchement	
100PT	0 psig - 200 psig	60 psig - 100 psig	115 psig	incr	125 psig	incr
100PT1	0 psig - 200 psig	60 psig - 100 psig	115 psig	incr	125 psig	incr
100TT	0°F - 250 °F	125°F - 175 °F	180 °F	incr	200 °F	incr
200PT	0 psig - 50 psig	0 psig - 20 psig	5 psig	incr	10 psig	incr

Toutes les SIF doivent être conçues pour une plage d'opérations allant du hors tension jusqu'au déclenchement.

Les éléments terminaux passent à l'état de sécurité sur perte d'alimentation (voir le Tableau F.9). Les éléments terminaux sont votés (1oo2) pour satisfaire aux exigences architecturales et de PFD_{avg}.

Un temps de réponse égal ou inférieur à une minute est considéré adéquat pour chaque SIF, sauf mention contraire.

Les transmetteurs et le solveur logique évalués selon l'IEC 61508 sont utilisés pour le SIS. Les transmetteurs évalués satisfont aussi aux exigences pour une utilisation préalable.

Une revue de l'équipe PHA a indiqué qu'aucune combinaison d'états de processus de sécurité, lorsqu'ils se produisent simultanément, ne crée de danger séparé.

Les transmetteurs ont une capabilité systématique SC 2 et le solveur logique une SC 3.

Les transmetteurs pour S-1 sont votés 1oo3 et pour S-2 sont votés 1oo2 pour satisfaire aux exigences architecturales et de PFD_{avg}.

L'IHM du BPCS constituera l'interface principale homme-machine du SIS. Toutes les fonctions d'affichage d'alarme seront mises en œuvre dans l'IHM du BPCS; aucune annonciation câblée n'est exigée. Une interface d'ingénierie/maintenance sera localisée dans un endroit sécurisé.

A l'issue d'une perte de l'IHM, l'opérateur dispose d'un bouton d'arrêt monté sur la console qui sera utilisé pour initier une séquence d'actions, nécessaires pour mener le processus à un état de sécurité de manière ordonnée. Le bouton-poussoir d'arrêt fournit des entrées discrètes aux solveurs logiques du SIS et BPCS et provoque l'ajout chimique d'arrêt court par l'action du BPCS.

L'équipe PHA a revu le manuel de sécurité du solveur logique du SIS sélectionné et a déterminé qu'une action manuelle sur les vannes de sécurité, indépendante du solveur logique, n'est pas exigée. Selon cette revue et les conséquences indésirables d'une dépressurisation de processus immédiat, l'activation manuelle directe ne sera pas incluse dans le SRS. Voir le schéma logique (Figure F.11).

Cela étant une opération de lot, le processus sera arrêté si des anomalies sont détectées dans le SIS. Ainsi, le processus ne sera pas exécuté si le SIS fonctionne en mode dégradé.

Il convient d'assigner la priorité la plus haute aux alarmes de prédéclenchement auxquelles l'opérateur peut répondre afin d'empêcher le SIS d'arrêter les systèmes.

Toutes les réinitialisations de déclenchements du SIS seront réinitialisées manuellement. Les interrupteurs de réinitialisation manuelle doivent être localisés sur la console de l'opérateur dans la salle de commande.

Cette opération étant une opération de lot et des bonnes pratiques d'ingénierie de système de commande étant utilisées, le taux de déclenchement parasite ne constitue pas un problème.

La duplication (duplication fonctionnelle de la logique d'application du SIS dans le BPCS) a été prévue pour résoudre les erreurs systématiques du programme d'application. Il a été prouvé que la duplication augmente le taux de déclenchement parasite, mais concernant le processus de lot de cet exemple, les déclenchements parasites n'ont pas posé de problème.

La détection d'anomalies de l'appareil de terrain et de l'IHM par diagnostics empêchera le démarrage, mais l'alarme seulement lorsque le lot est opérationnel.

Lorsque le SIS arrête le processus, toutes les boucles de commande BPCS seront placées en mode manuel et les sorties seront paramétrées sur l'état de sécurité.

Il convient de surveiller chaque circuit du SIS (par exemple, E/S, communication, diagnostics) afin de s'assurer qu'ils se trouvent à l'état sous tension avant le démarrage du SIS.

Il convient de vérifier automatiquement chaque transmetteur afin de s'assurer qu'il n'existe pas de mauvaise valeur (par exemple, inférieure à 4 mA) avant le démarrage du SIS.

Les modes de fonctionnement incluent le chargement, la réaction et le déchargement. Il convient que toutes les fonctions du SIS soient opérationnelles dans chaque mode.

Il convient de ne pas fournir de limitation, de neutralisation ou de dérivation.

Il n'existe pas d'exigence spéciale relative à la survivance du SIS à un événement accidentel majeur.

F.13.4 Exigences d'intégrité de sécurité

Le SIL exigé pour chaque SIF est défini au Tableau F.9.

Les fonctionnalités de matériel pour parvenir au SIL exigé sont:

- le solveur logique doit avoir un SC de 3 (c'est-à-dire, PFD_{avg} de l'appareil comprise entre 0,001 et 0,000 1) pris en charge par les évaluations de l'IEC 61508;
- la sélection des capteurs et des éléments terminaux selon la conformité à l'IEC 61508 et l'approbation utilisateur (voir ISA TR84.00.04-Part 1);
- l'équipement de tous les éléments terminaux avec des capteurs de position et la vérification visant à assurer la position cohérente de la vanne avec la commande de porte logique.

Les fonctionnalités de diagnostic pour parvenir au SIL exigé sont:

- diagnostics fournis avec le solveur logique;
- vérification des limites maximales et minimales de tous les capteurs d'entrée dans le SIS et le BPCS;
- comparaison de diagnostic sur 100PT et 100PT1 dans le SIS et le BPCS;
- duplication dans le BPCS.

Le réacteur sera arrêté deux fois par an pour une maintenance hors-ligne et des essais de verrouillage de sécurité. Il convient de soumettre à l'essai toutes les couches de protection identifiées dans la LOPA qui assurent la réduction du risque, à la même fréquence. Note: Cela étant une opération de lot, certains appareils du SIS pourraient être soumis plus fréquemment à l'essai (par exemple, les vannes de ventilation pourraient être soumises à l'essai avant le démarrage de chaque lot) si cela s'avère nécessaire pour atteindre la PFD_{avg} cible. A l'heure actuelle, les calculs de vérification du SIL décrits à l'Article F.16 ("paramètres de l'appareil SIF") indiquent que la fréquence d'essai la plus élevée n'est pas exigée. Toutefois, l'expérience d'exploitation prouve que les taux de défaillances de l'appareil SIF sont en fait plus élevés que ce qui est assumé par les calculs PFD_{avg}. Pour certains appareils, des essais à une fréquence plus soutenue pourraient être mis en œuvre.

Toutes les SIF sont alimentées depuis une UPS pour réduire les déclenchements parasites. Cela étant un processus de lot, il n'existe pas de disposition supplémentaire pour éviter les déclenchements parasites.

Défaillances de cause commune à minimiser par:

- des prises séparées pour les transmetteurs de pression redondants;
- des lignes séparées pour les vannes de ventilation redondantes;
- vérification que les alarmes revendiquées comme IPL dans l'événement 6 du Tableau 7 sont complètement indépendantes de la SIF (c'est-à-dire que des contrôleurs DCS séparés sont utilisés pour les fonctions de commande, d'alarme et de duplication du BPCS);
- l'application de pratiques d'ingénierie appropriées (mise à la terre, protection contre les ondes de choc, sources d'alimentation, diversité) telle que mentionnée à l'Article F.18 et à l'Article F.19;
- examiner les facteurs humains (par exemple, configuration, étalonnage, essai) grâce au concours de personnel différent pour la vérification et l'approbation.

F.14 Description fonctionnelle et modèle conceptuel

L'Article F.14 décrit la manière dont les exigences fonctionnelles de sécurité et les exigences d'intégrité de sécurité ont été intégrées pour permettre le développement des architectures de la SIF, la vérification du SIL pour chaque SIF et le développement du programme d'application du SIS.

F.14.1 Texte rédactionnel pour l'exemple de logique du système du réacteur

Trois SIF automatiques, de S-1 à S-3 sont mises en œuvre dans le SIS:

- les SIF S-1 et S-2 protègent contre les fuites du réacteur dues à une température/pression trop élevée, puisque la réaction est exothermique et que la pression élevée est causée par une température élevée;
- si les transmetteurs de pression 100PT ou 100PT1 dépassent 125 psig ou que la température du transmetteur 100TT dépasse 200 °F, la fonction de sécurité S-1 ouvre la vanne de ventilation du réacteur.

Etant donné l'extrême rapidité avec laquelle la pression augmente lors de l'ajout d'une double charge de l'initiateur ou lors du débordement du réacteur, une SIF S-2 assure la prévention de ces événements. Le transmetteur de température, dont le temps de réponse est plus long, peut ne pas détecter cet événement extrêmement rapide. Le transmetteur de température 100TT n'est donc pas inclus dans le calcul de la PFD_{avg}. Les vannes de ventilation s'ouvriront si 100PT ou 100PT1 dépassent 125 psig.

Des transmetteurs de pressions intelligents et identiques sont utilisés pour cette application. De ce fait, il convient de prendre en compte la probabilité qu'une erreur systématique pourrait causer une défaillance des deux transmetteurs en même temps. Des diagnostics sont fournis dans les solveurs logiques du SIS et du BPCS pour détecter les valeurs du transmetteur au-dessus de la plage, en dessous de la plage, ou qui dévient l'une de l'autre. La couverture du diagnostic est prise en compte pour les calculs PFD_{avg} (voir l'Article F.16).

La SIF S-3 assure l'ouverture des vannes de ventilation 100PV et 100PV1 lorsque la pression du sceau est supérieure à 10 psig selon les mesures de 200PT.

Etant donné que les causes initiatrices pour les scénarios 1 à 8 envoient des sollicitations à des appareils ayant la même SIF, il convient que les sollicitations soient regroupées pour déterminer le mode de fonctionnement pour chaque SIF. Dans cet exemple, elles totalisent 0,8 sollicitation/an, ce qui représente moins d'une sollicitation par an pour la SIF. Ainsi, chaque SIF sera exécutée en mode à faible sollicitation. Voir l'ISA TR84.00.04:2015 et A.9.2.3 pour obtenir des lignes directrices sur le mode de fonctionnement par sollicitation par rapport au mode continu.

Tableau F.14 – Schéma de cause à effet

Schéma de cause à effet du réacteur (format tableau)						
Cause				**Effet**		
No. de fonction de sécurité	Capteur/ Entrée	Description	Réglage de déclenchement	Mesures finales Appareil	Action	Commentaires
S-1	100PT 100PT1	Pression du réacteur **OU**	> 125 psig	100PV	OUVERT	Dépressuriser le réacteur
	100TT	Température du réacteur	> 200 °F	100PV1	OUVERT	Dépressuriser le réacteur
S-2	100PT 100PT1	Pression élevée du réacteur	> 125 psig	100PV 100PV1	OUVERT OUVERT	Dépressuriser le réacteur
S-3	200PT	Pression du sceau du réacteur	>10 psig	100PV 100PV1	OUVERT OUVERT	Dépressuriser le réacteur

F.15 Calculs de vérification du SIL

Compte tenu des exigences fonctionnelles et d'intégrité ci-dessus, une esquisse (c'est-à-dire un schéma architectural tel que présenté à la Figure F.4, à la Figure F.6 et à la Figure F.8) a été développée pour chaque SIF, pour:

- décrire comment les exigences fonctionnelles et de sécurité ont été satisfaites;
- montrer dans quelle mesure l'architecture de la SIF satisfait aux exigences du SIL;
- donner la PFD_{avg} pour chaque sous-système de la SIF (sous-système de capteur, sous-système de solveur logique et sous-système d'élément terminal);
- fournir une base pour le développement de l'architecture du SIS;
- fournir une base pour le calcul de la PFD_{avg} de la SIF.

Les schémas architecturaux ont alors été utilisés pour développer un arbre des défaillances pour chaque SIF, à l'aide de logiciels disponibles dans le commerce. La sortie du logiciel d'analyse par arbre des défaillances documente la PFD_{avg} de la SIF (voir la Figure F.5, la Figure F.7 et la Figure F.9). A ce stade, la PFD_{avg} calculée a été comparée à la PFD_{avg} exigée (voir le Tableau F.9, colonne 10). La PFD_{avg} calculée n'ayant pas satisfait aux exigences du Tableau 7, le modèle conceptuel a été modifié en conséquence.

Chaque type d'appareil SIF figure au Tableau F.15 ci-dessous, avec ses paramètres de fiabilité. Les paramètres ont été développés à partir des utilisations préalables, des données constructeur et des bases de données industrielles, l'attention étant tout particulièrement portée sur les données de terrain.

Temps moyen avant défaillance dangereuse *(MTTFd)*:

Tableau F.15 – Chiffres MTTFd des appareils F.1 du SIS

Vanne de ventilation d'urgence	60 ans
Transmetteur de pression	60 ans
Transmetteur de température avec RTD	60 ans
Electrovanne	35 ans
Solveur logique du SIS	2 500 ans

Cause commune:

Les questions de cause commune ont été résolues grâce aux techniques décrites à l'Article F.18. Les défaillances de cause commune résiduelles ont été résolues grâce à l'ajout de facteurs à l'arbre des défaillances pour chaque SIF. Ces facteurs étaient basés sur l'expérience de l'installation. Pour les vannes et les électrovannes, les défaillances de cause commune ont été estimées à 1 % du total des défaillances dangereuses non détectées. Pour les transmetteurs, les défaillances de cause commune ont été estimées à 2 % du total des défaillances dangereuses non détectées (c'est-à-dire que le taux de défaillances dangereuses non détectées dû aux défaillances de cause commune est égal à 0,02 × (1/60) pour les transmetteurs, à 0,01 × (1/60) pour les vannes et à 0,01 × (1/35) pour les électrovannes).

Erreurs systématiques:

Le solveur logique du SIS a une capabilité systématique de SC 3 qui résout les défaillances du matériel, satisfait aux exigences architecturales (tolérance aux anomalies) et du logiciel intégré. Il est à noter que les défaillances systématiques du programme d'application n'ont pas été résolues dans l'évaluation du solveur logique. Des problèmes de défaillance du programme d'application du solveur logique systématiques ont été résolus par la duplication de la logique dans le BPCS (voir les schémas architecturaux de

la Figure F.4, de la Figure F.6 et de la Figure F.8). Le BPCS a été utilisé pour réduire les défaillances systématiques du programme d'application du SIS. Toutefois, la contribution du matériel BPCS à la PFD_{avg} n'a pas été incluse dans l'analyse par arbre des défaillances pour chaque SIF.

NOTE 1 La technique ci-dessus a été utilisée en plus de la mise en œuvre des techniques définies par l'IEC 61511-1:2016 , Article 12.

Les transmetteurs de pression et de température sont des appareils intelligents, contiennent des appareils programmables (langage de programme figé) et ont une capabilité systématique de SC 2 conformément à l'IEC 61508. Les transmetteurs ont été utilisés dans des applications SIL 3 (c'est-à-dire SIF S-1 et SIF S-2). Pour résoudre les défaillances systématiques, plusieurs techniques ont été mises en œuvre sur chaque SIF SIL 3.

- Pour la SIF S-1, les performances d'utilisations préalables ont été utilisées pour la sélection d'équipement, la diversité (température et pression) et les diagnostics (voir F.14.1 "Texte rédactionnel pour l'exemple de logique du système du réacteur") l'ayant été pour s'assurer que le niveau des erreurs de logiciel systématiques est compatible avec l'application du SIL 3.
- Pour la SIF S-2, l'analyse des utilisations préalables (voir la note ci-dessous), l'analyse par arbre des défaillances (voir la Figure F.7) et les diagnostics ont été utilisés pour s'assurer que le niveau des défaillances de logiciel systématiques dans les transmetteurs est compatible avec l'application du SIL 3.

NOTE 2 Selon des données d'utilisations préalables, l'équipe a estimé que 2 % du total des défaillances de cause commune des transmetteurs était dû à des erreurs logicielles. L'arbre des défaillances de la Figure F.7 présente la manière dont les erreurs logicielles ont été prises en compte pour le calcul de la PFD_{avg} de la SIF S-2. Si peu de données relatives à l'utilisation préalable étaient disponibles, une alternative consisterait pour l'utilisateur à s'assurer auprès du fabricant du transmetteur que les techniques utilisées pour développer le logiciel intégré étaient conformes aux lignes directrices de l'IEC 61508 dans le cas du logiciel SIL 3.

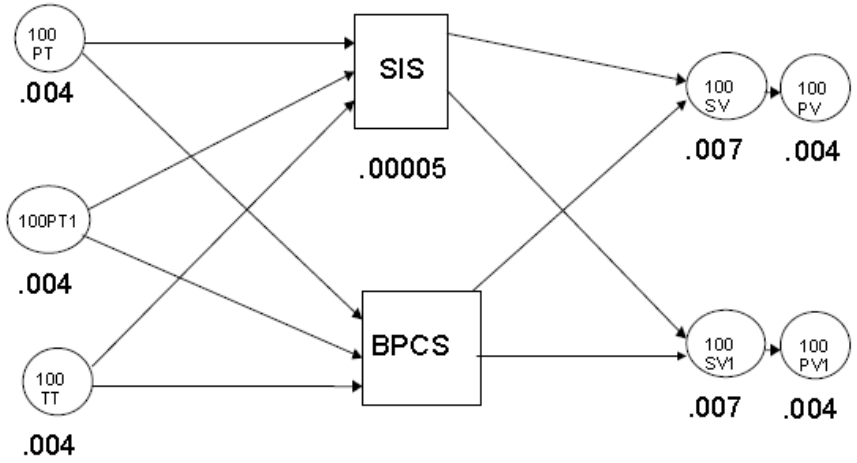
Tolérance aux défauts du matériel (HFT):

Pour la SIF S-1 et la SIF S-2, la tolérance aux défauts utilisée pour les capteurs et les vannes s'appuie sur l'IEC 61511-1:2016 , Tableau 6 (SIL 3).

Pour la SIF S-3, la tolérance aux défauts utilisée pour les capteurs et les vannes s'appuie sur l'IEC 61511-1:2016 Tableau 6 (SIL 2).

Le solveur logique a été conçu et évalué par une tierce partie afin de satisfaire aux exigences de l'IEC 61508 (y compris la tolérance aux anomalies) pour les applications SIL 3. Par conséquent, les exigences de tolérance aux anomalies de l'IEC 61511 sont satisfaites pour la SIF S-1, la SIF S-2 et la SIF S-3.

SIF S-1



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

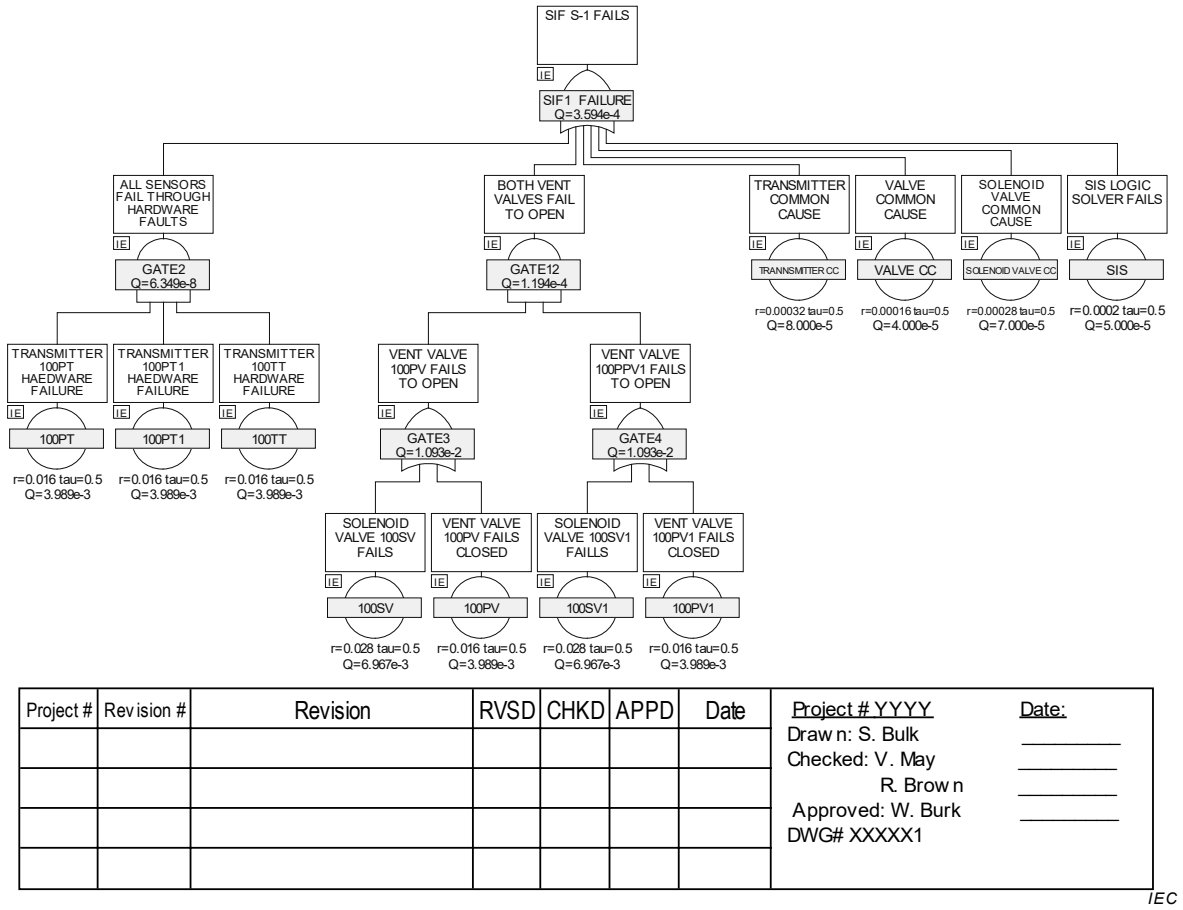
Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.4 – Schéma architectural de la SIF S-1 présentant la PFD_{avg} de chaque appareil du SIS

Voir la Figure F.5 pour les calculs d'arbre des défaillances.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk
Checked: V. May
R. Brown
Approved: W. Burk
DWG# XXXXX1

IEC

Anglais	Français
SIF S-1 FAILS	DEFAILLANCE DE LA SIF S-1
SIF1 FAILURE	DEFAILLANCE DE LA SIF1
ALL SENSORS FAIL THROUGH HARDWARE FAULTS	DEFAILLANCE DE TOUS LES CAPTEURS A CAUSE DE DEFAUTS MATERIELS
BOTH VENT VALVES FAIL TO OPEN	DEFAILLANCE DE L'OUVERTURE DES DEUX VANNES DE VENTILATION
TRANSMITTER COMMON CAUSE	CAUSE COMMUNE DU TRANSMETTEUR
VALVE COMMON CAUSE	CAUSE COMMUNE DE LA VANNE
SOLENOID VALVE COMMON CAUSE	CAUSE COMMUNE DE L'ELECTROVANNE
SIS LOGIC SOLVER FAILS	DEFAILLANCE DE L'UNITE LOGIQUE DU SIS
GATE	PORTE
TRANSMITTER CC	CC TRANSMETTEUR
VALVE CC	CC VANNE
SOLENOID VALVE CC	CC ELECTROVANNE
SIS	SIS
TRANSMITTER 100PT HARDWARE FAILURE	DEFAILLANCE MATERIELLE DU TRANSMETTEUR 100PT
VENT VALVE 100PV FAILS TO OPEN	DEFAILLANCE DE L'OUVERTURE DE LA VANNE DE VENTILATION 100PV
SOLENOID VALVE 100SV FAILS	DEFAILLANCE DE L'ELECTROVANNE 100SV

Anglais	Français
VENT VALVE 100PV FAILS CLOSED	DEFAILLANCE DE LA VANNE DE VENTILATION 100PV FERME
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Légende

E Evénement d'activation

Q Indisponibilité (PFD_{avg})

r Taux de défaillances (défaillances/an)

tau Intervalle d'essai (ans)

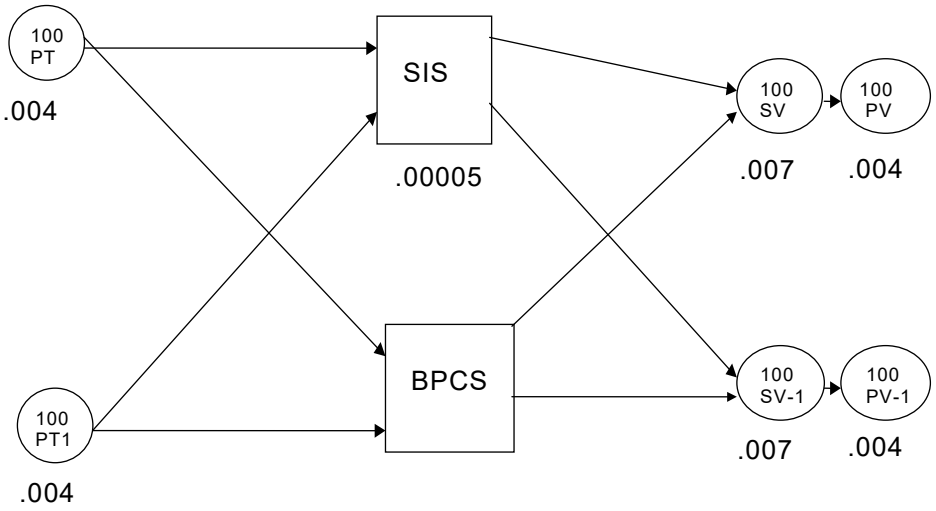
La SIF S-1 a une PFD_{avg} arrondie à 3,6e-4 et satisfait donc au SIL 3.

Figure F.5 – Arbre des défaillances S-1

SIF S-2

Si la pression du réacteur est supérieure à 125 psig, les vannes de ventilation 100PV et 100PV1 sont ouvertes. Le SIL exigé = 3 (ce qui implique PFD_{avg} = 10^{-3} à 10^{-4})

S-2



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

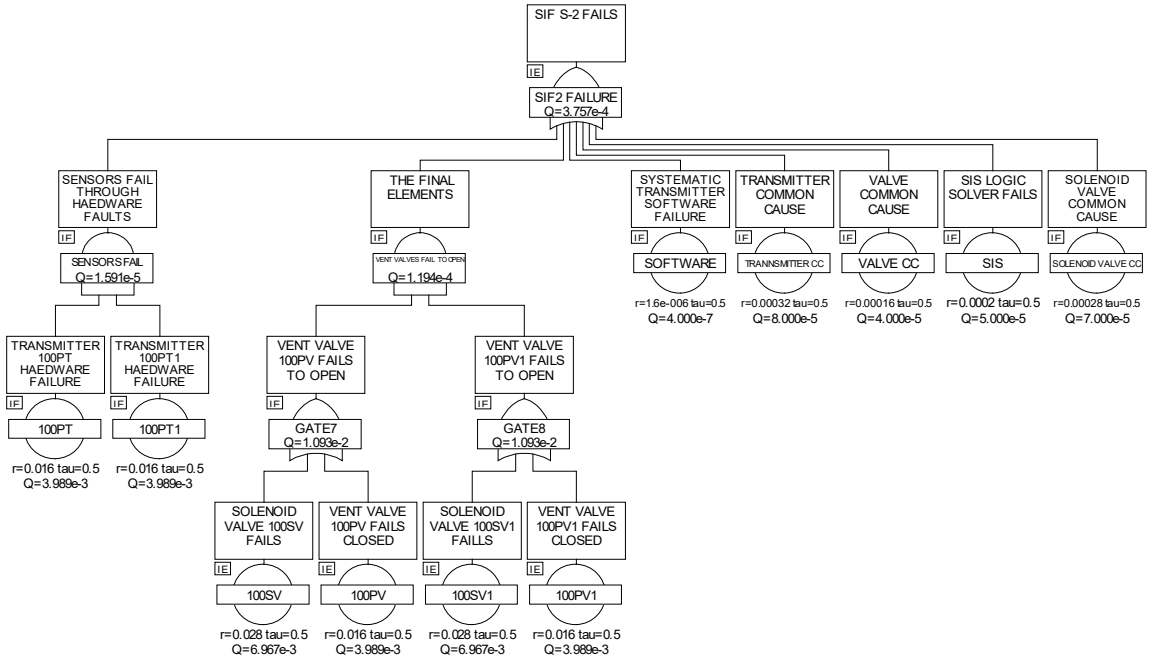
Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.6 – Schéma architectural de la SIF S-2 présentant la PFD_{avg} de chaque appareil du SIS

Voir Figure F.7 pour les calculs d'arbre des défaillances.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
SIF S-2 FAILS	DEFAILLANCE DE LA SIF S-2
SIF2 FAILURE	DEFAILLANCE DE LA SIF2
SENSORS FAIL THROUGH HARDWARE FAULTS	DEFAILLANCE DES CAPTEURS A CAUSE DE DEFAUTS MATERIELS
THE FINAL ELEMENTS	LES ELEMENTS TERMINAUX
SYSTEMATIC TRANSMITTER SOFTWARE FAILURE	DEFAILLANCE SYSTEMATIQUE DU LOGICIEL DU TRANSMETTEUR
TRANSMITTER COMMON CAUSE	CAUSE COMMUNE DU TRANSMETTEUR
VALVE COMMON CAUSE	CAUSE COMMUNE DE LA VANNE
SOLENOID VALVE COMMON CAUSE	CAUSE COMMUNE DE L'ELECTROVANNE
SIS LOGIC SOLVER FAILS	DEFAILLANCE DE L'UNITE LOGIQUE DU SIS
SENSORS FAIL	DEFAILLANCE DES CAPTEURS
VENT VALVES FAIL TO OPEN	DEFAILLANCE DE L'OUVERTURE DES VANNES DE VENTILATION
SOFTWARE	LOGICIEL
TRANSMITTER CC	CC TRANSMETTEUR
VALVE CC	CC VANNE
SOLENOID VALVE CC	CC ELECTROVANNE
SIS	SIS
TRANSMITTER 100PT HARDWARE FAILURE	DEFAILLANCE MATERIELLE DU TRANSMETTEUR 100PT

Anglais	Français
VENT VALVE 100PV FAILS TO OPEN	DEFAILLANCE DE L'OUVERTURE DE LA VANNE DE VENTILATION 100PV
GATE	PORTE
SOLENOID VALVE 100SV FAILS	DEFAILLANCE DE L'ELECTROVANNE 100SV
VENT VALVE 100PV FAILS CLOSED	DEFAILLANCE DE LA VANNE DE VENTILATION 100PV FERME
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Légende

E Evénement d'activation

Q Indisponibilité (PFD_{avg})

r Taux de défaillances (défaillances/an)

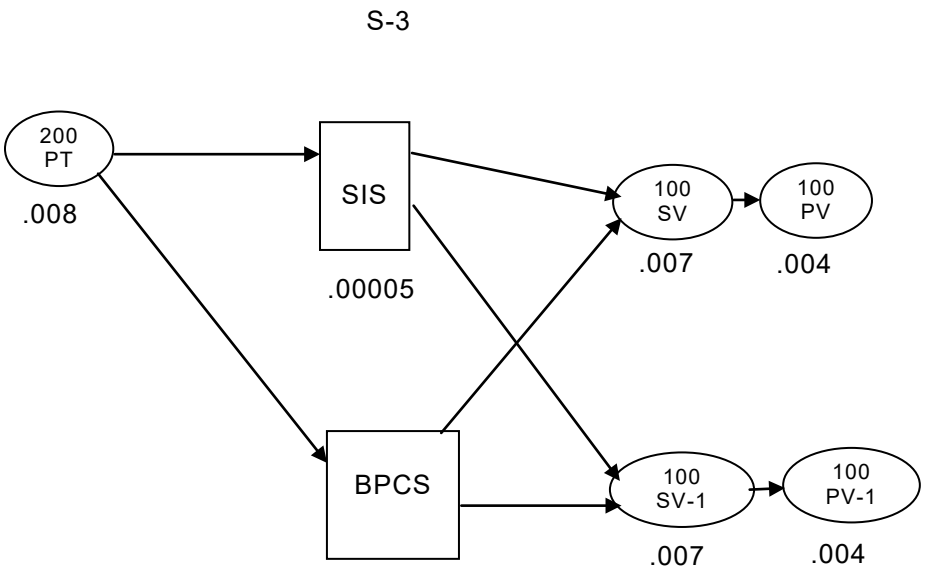
tau Intervalle d'essai (ans)

La fonction de sécurité S-2 a une PFD_{avg} arrondie à 3,8e-4 et satisfait donc au SIL S-3.

Figure F.7 – Arbre des défaillances de la SIF S-2

SIF S-3

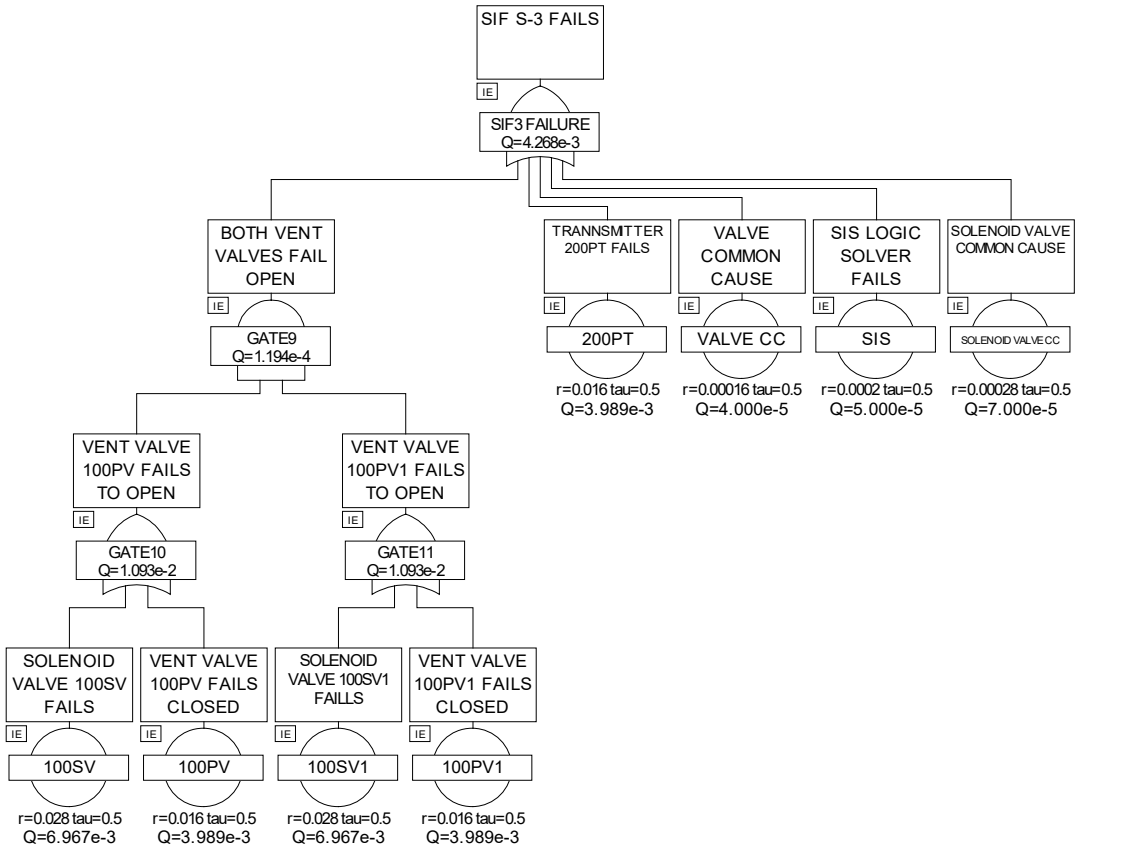
Si la pression du sceau de l'agitateur est supérieure à 10 psig, ouvrir 100PV et 100PV-1. Le SIL exigé = 2 (PFD_{avg} = 10^{-2} à 10^{-3})



Anglais	Français
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.8 – Schéma architectural de la SIF S-3 présentant la PFD_{avg} de chaque appareil du SIS

Voir la Figure F.9 pour les calculs d'arbre des défaillances.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
SIF S-3 FAILS	DEFAILLANCE DE LA SIF S-3
SIF3 FAILURE	DEFAILLANCE DE LA SIF3
BOTH VENT VALVES FAIL OPEN	DEFAILLANCE DES DEUX VANNES DE VENTILATION OUVERT
TRANSMITTER 200PT FAILS	DEFAILLANCE DU TRANSMETTEUR 200PT
VALVE COMMON CAUSE	CAUSE COMMUNE DE LA VANNE
SOLENOID VALVE COMMON CAUSE	CAUSE COMMUNE DE L'ELECTROVANNE
SIS LOGIC SOLVER FAILS	DEFAILLANCE DE L'UNITE LOGIQUE DU SIS
VENT VALVE 100PV FAILS TO OPEN	DEFAILLANCE DE L'OUVERTURE DE LA VANNE DE VENTILATION 100PV
GATE	PORTE
SOLENOID VALVE 100SV FAILS	DEFAILLANCE DE L'ELECTROVANNE 100SV
VENT VALVE 100PV FAILS CLOSED	DEFAILLANCE DE LA VANNE DE VENTILATION 100PV FERME
Project #	N° de projet
Revision #	N° de révision

Anglais	Français
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Légende

E Evénement d'activation

Q Indisponibilité (PFD_{avg})

r Taux de défaillances (défaillances/an)

tau Intervalle d'essai (ans)

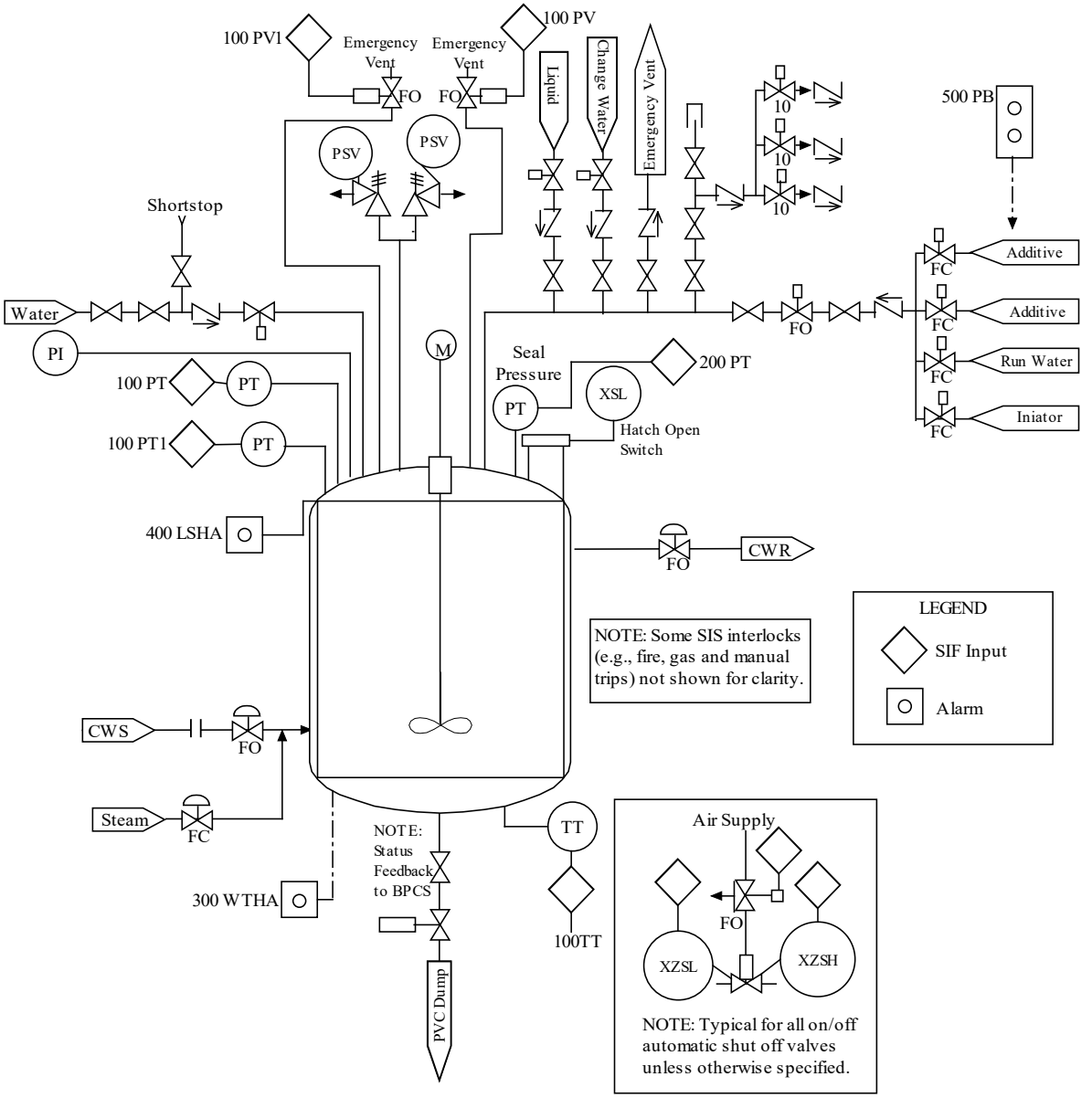
La fonction de sécurité S-3 a une PFD_{avg} arrondie à 4,3e-3 et satisfait donc au SIL S-2.

Figure F.9 – Arbre des défaillances de la SIF S-3

F.16 Exigences du programme d'application

La SRS (en particulier, le texte rédactionnel de la logique (Paragraphe F.14.1), le diagramme de cause à effet (Tableau F.14) et le schéma P&I (Figure F.10)) ont été utilisés pour développer les exigences du programme d'application, comme présenté dans le diagramme à contacts (Figure F.11).

Les diagrammes à contacts reflétant les exigences fonctionnelles de chaque SIF sont représentés à la Figure F.11 et dans les feuilles 1 à 5 incluses. Le diagramme à contacts donne également les caractéristiques de tension de ligne électrique, les caractéristiques de mise à la terre, les exigences de circuit et les diagnostics pour aider le concepteur/programmeur à développer le programme d'application.



Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

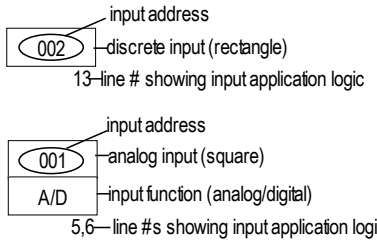
Anglais	Français
Shortstop	Arrêt court
Emergency vent	Ventilation d'urgence
Liquid	Liquide
Change water	Changement d'eau
Water	Eau
Additive	Additif
Run water	Eau courante

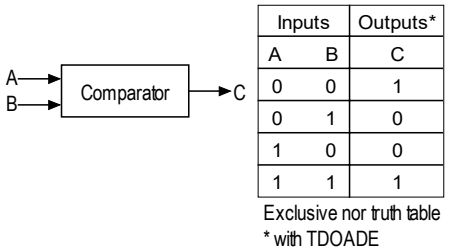
Anglais	Français
Initiator	Initiateur
Seal pressure	Pression du sceau
Hatch open switch	Commutateur ouvert écoutille
NOTE 1 Some SIS interlocks (e.g., fire, gas and manual trips) not shown for clarity.	NOTE 1 Certains verrouillages du SIS (p. ex.: feu, gaz et déclenchements manuels) ont été omis pour plus de clarté.
LEGEND SIF input Alarm	LEGENDE Entrée de la SIF Alarme
Steam	Vapeur
NOTE 2 Status feedback to BPCS	NOTE 2 Information sur l'état retournée au BPCS
Air supply	Alimentation en air
NOTE 3 Typical for all on/off automatic shut off valves unless otherwise specified.	NOTE 3 Type pour toutes les vannes de fermeture automatique activées/désactivées, sauf indication contraire.
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

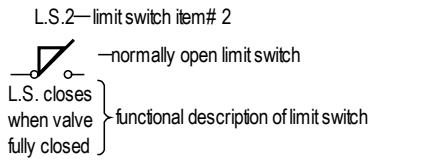
Figure F.10 – Schéma de tuyauterie et d'instrumentation pour SIF d'unité de réacteur PVC

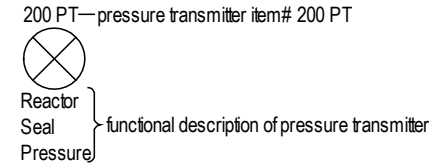
Application Logic Legend

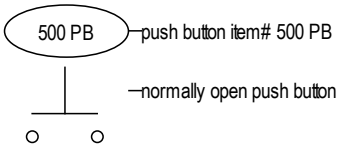
Devices

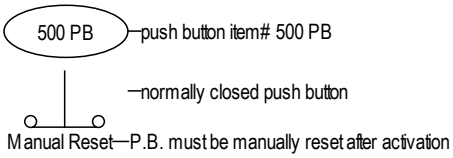


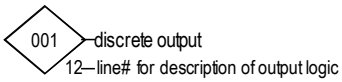


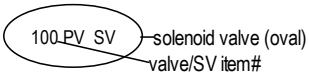


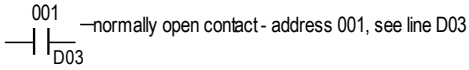


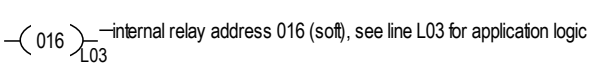


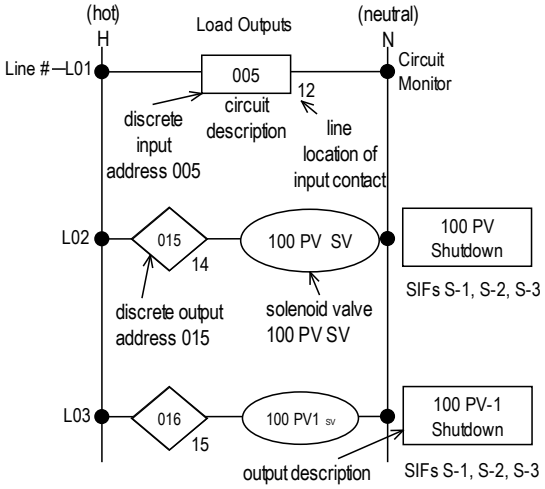












Circuit Functional Description

TDOADE = Time Delay Opening After De-Energization

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

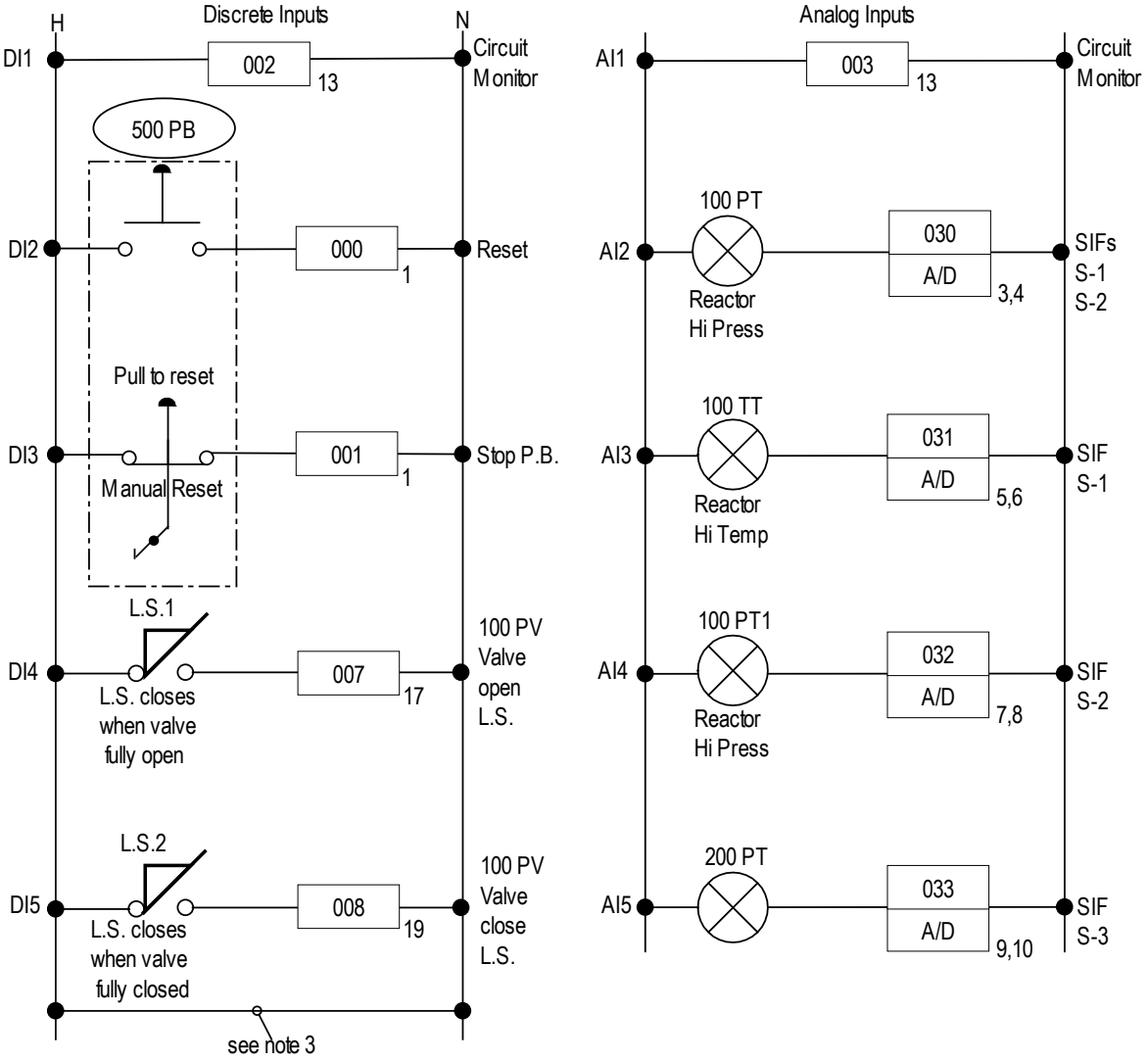
Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
Application Logic Legend	Légende de la logique d'application
Devices	Appareils
Input address	Adresse d'entrée
Discrete input (rectangle)	Entrée discrète (rectangle)
Line # showing input application logic	N° de ligne affichant la logique d'application
Input address	Adresse d'entrée
Analog input (square)	Entrée analogique (carré)
Input function (analog/digital)	Fonction d'entrée (analogique/numérique)
Line #s showing input application logic	N° de ligne affichant la logique d'application
Limit switch item # 2	Interrupteur de fin de course – élément n° 2
Normally open limit switch	Interrupteur de fin de course ouvert normalement
L.S. closes when valve fully closed	L'interrupteur de fin de course se ferme lorsque la vanne est entièrement fermée
Functional description of limit switch	Description fonctionnelle de l'interrupteur de fin de course
Pressure transmitter item # 200 PT	Transmetteur de pression – élément n° 200 PT
Reactor Seal Pressure	Pression du sceau du réacteur
Functional description of pressure transmitter	Description fonctionnelle du transmetteur de pression
Push button item # 500 PB	Bouton-poussoir – élément n° 500 PB
Normally open push button	Bouton-poussoir ouvert normalement
Normally closed push button	Bouton-poussoir fermé normalement
Manual reset – P.B. must be manually reset after activation	Réinitialisation manuelle – le bouton-poussoir doit être réinitialisé manuellement après activation
Discrete output	Sortie discrète
Line # for description of output logic	N° de ligne pour la description de la logique de sortie
Solenoid valve (oval)	Electrovanne (oval)
Valve/SV item #	Vanne/Electrovanne – N° d'élément
Normally open contact – address 001, see line D03	Contact ouvert normalement – adresse 001, voir ligne D03
Internal relay address 016 (soft), see line L03 for application logic	Adresse relais interne 016 (molle), voir ligne L03 pour la logique d'application
Comparator	Comparateur
Inputs	Entrées
Outputs*	Sorties
Exclusive nor truth table	Table de vérité exclusive NOR
* with TDOADE	* avec TDOADE
Line #	N° de ligne
(hot)	(chaud)
Load Outputs	Sorties à charge
(neutral)	(neutre)
Circuit Monitor	Moniteur de circuit
Discrete input address 005	Adresse d'entrée discrète 005
Circuit description	Description du circuit
Line location of input contact	Localisation de la ligne de contact d'entrée
Discrete output address 015	Adresse de sortie discrète 015

Anglais	Français
Solenoid valve 100 PVSV	Electrovanne 100 PVSV
Shutdown	Arrêt
Output description	Description de la sortie
Circuit functional description	Description fonctionnelle du circuit
TDOADE = Time Delay Opening After De-Energization	TDOADE = Délai d'ouverture après mise hors tension
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.11 – Légende *(1 de 5)*



NOTES:
1) Figure 11 not for construction.
2) Safety manual(s) requirements to be added.
3) Lines D14 and D15 to be duplicated for 100PV1.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

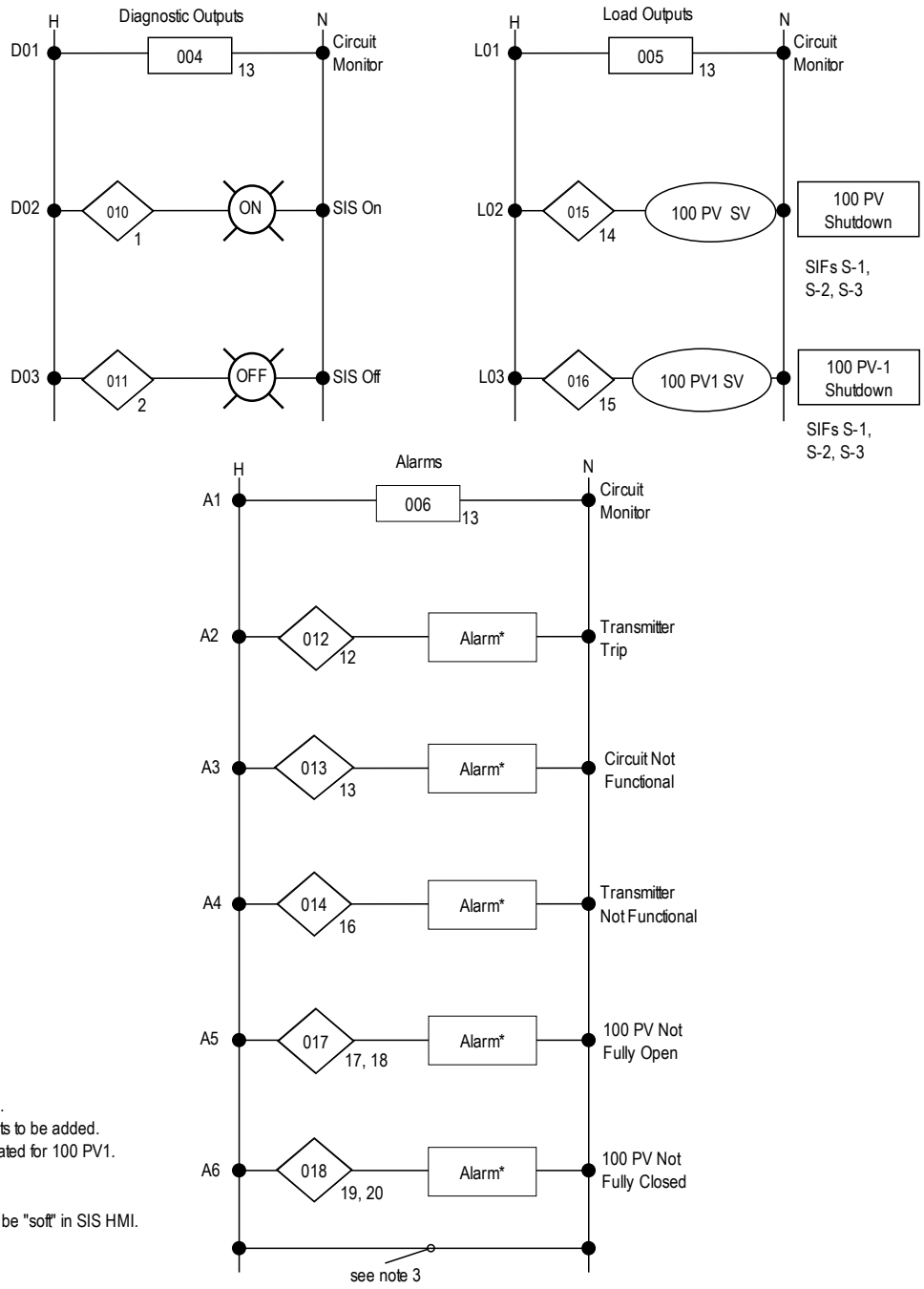
Project # YYYY Date:
Drawn: S. Bulk
Checked: V. May
R. Brown
Approved: W. Burk
DWG# XXXXX1

IEC

Anglais	Français
Discrete inputs	Entrées discrètes
Circuit monitor	Moniteur de circuit
Analog inputs	Entrées analogiques
Reset	Réinitialiser
Reactor hi press	Réacteur pression élevée
Pull to reset	Tirer pour réinitialiser
Manual reset	Réinitialisation manuelle

Anglais	Français
Stop P.B.	Arrêt bouton-poussoir
Reactor hi temp	Réacteur température élevée
L.S. closes when valve fully open	L'interrupteur de fin de course se ferme lorsque la vanne est entièrement ouverte
L.S. closes when valve fully closed	L'interrupteur de fin de course se ferme lorsque la vanne est entièrement fermée
Valve open L.S.	Interrupteur de fin de course de la vanne ouvert
Valve close L.S.	Interrupteur de fin de course de la vanne fermé
See Note 3	Voir Note 3
NOTE 1 Figure 11 not for construction. NOTE 2 Safety manual(s) requirements to be added. NOTE 3 Lines D14 and D15 to be duplicated for 100PV1.	NOTE 1 Figure 11 non prévue pour construction. NOTE 2 Exigences du/des manuel(s) de sécurité à ajouter. NOTE 3 Lignes D14 et D15 à dupliquer pour 100PV1.
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.11 *(2 de 5)*



NOTES:
1) Figure 11 not for construction.
2) Safety manual(s) requirements to be added.
3) Lines A5 and A6 to be duplicated for 100 PV1.

*(asterisk) indicates alarms may be "soft" in SIS HMI.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

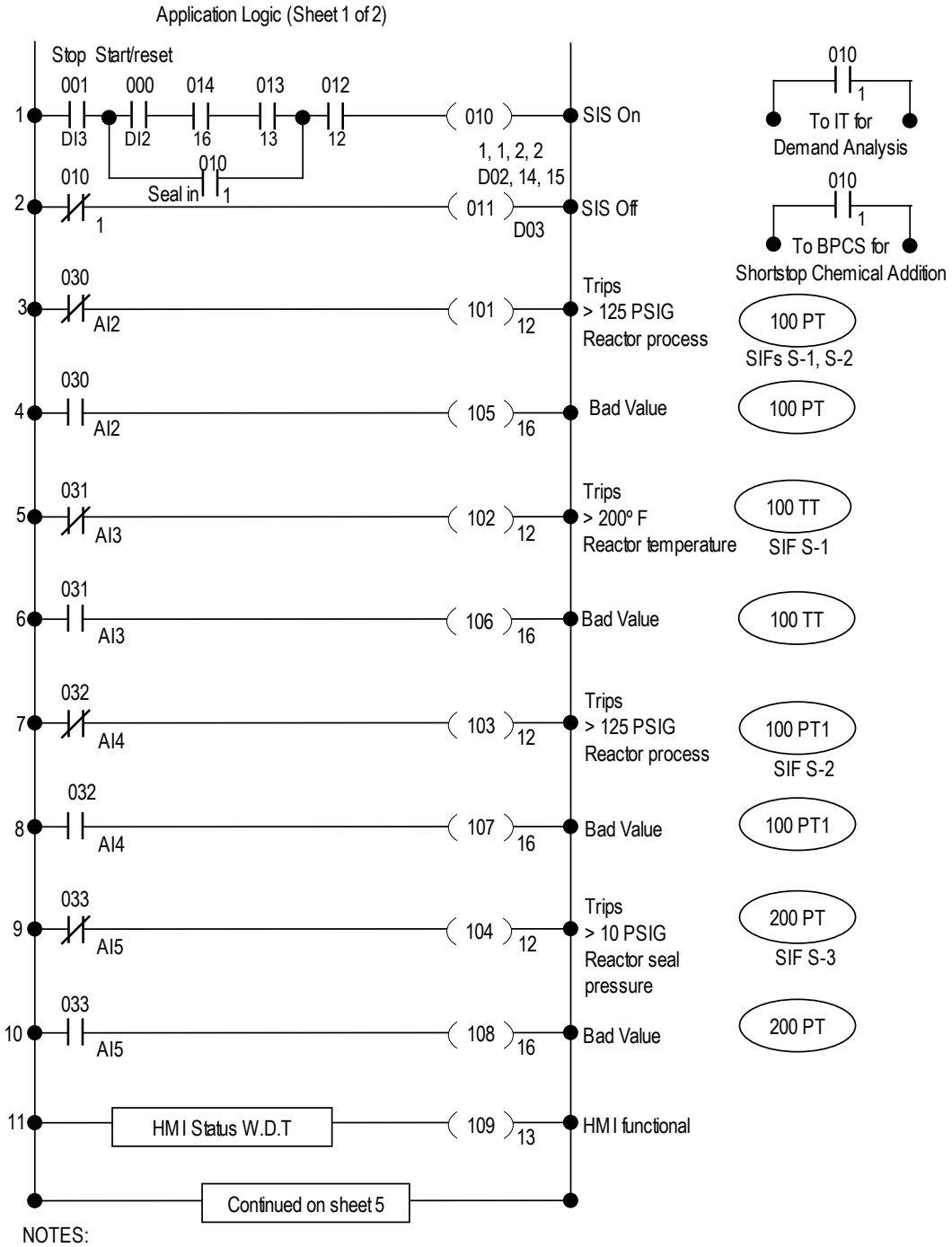
Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
Diagnostic outputs	Sorties de diagnostic
Circuit monitor	Moniteur de circuit
Load outputs	Sorties à charge
Shutdown	Arrêt
Alarms	Alarmes

Anglais	Français
Transmitter trip	Déclenchement du transmetteur
Circuit not functional	Circuit non fonctionnel
Transmitter not functional	Transmetteur non fonctionnel
100 PV not fully open	100 PV non ouvert entièrement
100 PV not fully closed	100 PV non fermé entièrement
See Note 3	Voir Note 3
NOTE 1 Figure 11 not for construction. NOTE 2 Safety manual(s) requirements to be added. NOTE 3 Lines A5 and A6 to be duplicated for 100 PV1.	NOTE 1 Figure 11 non prévue pour construction. NOTE 2 Exigences du/des manuel(s) de sécurité à ajouter. NOTE 3 Lignes A5 et A6 à dupliquer pour 100 PV1.
*(asterisk) indicates alarms may be “soft” in SIS HMI.	L'astérisque (*) indique que des alarmes peuvent être "molles" dans l'IHM SIS
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.11 *(3 de 5)*



NOTES:
1) Figure 11 not for construction.
2) Safety manual(s) requirements to be added.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

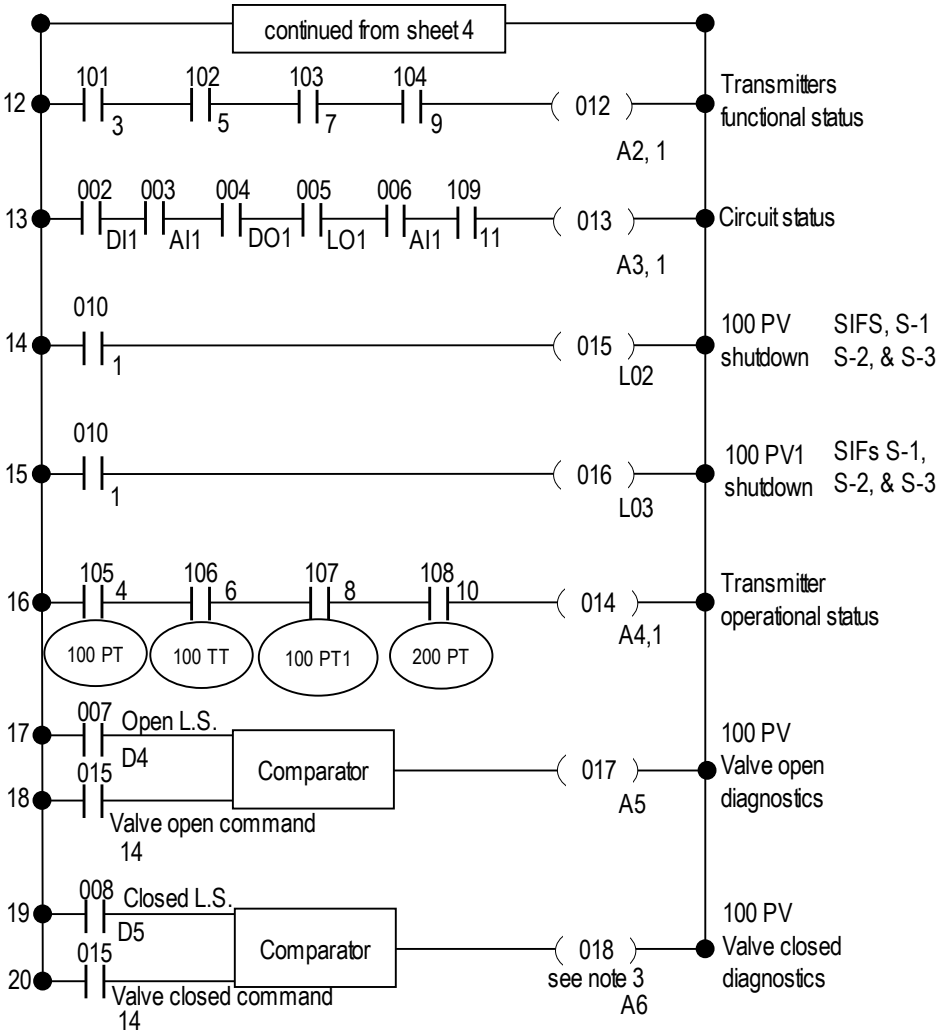
Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
Application logic (Sheet 1 of 2)	Logique d'application (Feuille 1 sur 2)
Stop	Arrêt
Start/reset	Démarrage/Réinitialisation
SIS on	SIS activé
Seal in	Sceau activé
To IT for demand analysis	Vers service informatique pour analyse de la demande
SIS off	SIS désactivé
To BPCS for shortstop chemical addition	Vers BPCS pour ajout chimique d'arrêt court
Trips >125 PSIG reactor process	Déclenche le processus >125 PSIG du réacteur
Bad value	Mauvaise valeur
Trips > 200 °F reactor temperature	Déclenche la température >200 °F du réacteur
Trips >125 PSIG reactor process	Déclenche le processus > 125 PSIG du réacteur
Trips >10 PSIG reactor seal pressure	Déclenche la pression du sceau >10 PSIG du réacteur
HMI status W.D.T	Etat IHM WDT
HMI functional	IHM fonctionnelle
Continued on sheet 5	Suite sur feuille 5
NOTE 1 Figure 11 not for construction. NOTE 2 Safety manual(s) requirements to be added.	NOTE 1 Figure 11 non prévue pour construction. NOTE 2 Exigences du/des manuel(s) de sécurité à ajouter.
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.11 *(4 de 5)*

Application Logic (Sheet 2 of 2)



NOTES:
1) Figure 11 not for construction.
2) Safety manual requirements to be added.
3) Lines 17, 18, 19, and 20 to be duplicated for 100 PV1.

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
Application logic (Sheet 2 of 2)	Logique d'application (Feuille 2 sur 2)
Continued from sheet 4	Suite de la feuille 4
Transmitters functional status	Etat fonctionnel des transmetteurs
Circuit status	Etat du circuit
Shutdown	Arrêt
Transmitter operational status	Etat opérationnel du transmetteur

Anglais	Français
Open L.S.	Interrupteur de fin de course ouvert
Comparator	Comparateur
Valve open command	Commande de vanne ouverte
Valve open diagnostics	Diagnostics de vanne ouverte
Closed L.S.	Interrupteur de fin de course fermé
Valve closed command	Commande de vanne fermée
Valve closed diagnostics	Diagnostics de vanne fermée
See Note 3	Voir Note 3
NOTE 1 Figure 11 not for construction. NOTE 2 Safety manual requirements to be added. NOTE 3 Lines 17, 18, 19, and 20 to be duplicated for 100 PV1.	NOTE 1 Figure 11 non prévue pour construction. NOTE 2 Exigences du manuel de sécurité à ajouter. NOTE 3 Lignes 17, 18, 19 et 20 à dupliquer pour 100 PV1.
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.11 *(5 de 5)*

F.17 Etape F.4: Cycle de vie de sécurité du SIS

Tableau F 16 – Cycle de vie de sécurité du SIS – Zone 4

Phase ou activité du cycle de vie de sécurité		Objectifs	Exigences Article ou paragraphe de l'IEC 61511-1:2016	Entrées	Sorties
IEC 61511-1:2016 Figure 7, zone 4	Conception et ingénierie du SIS	Concevoir le SIS pour satisfaire aux exigences des SIF et leur intégrité de sécurité	11 et 12.4	Exigences concernant la sécurité du SIS Exigences de sécurité du programme d'application	Conception du SIS en conformité avec les exigences de sécurité du SIS; planification de l'essai d'intégration du SIS

Le Tableau F.16 donne les objectifs, les entrées, les sorties et les références aux articles et paragraphes connexes pour la conception et l'ingénierie du SIS.

F.18 Choix de la technologie et de l'appareil

F.18.1 Généralités

L'Article F.18 répertorie certains des paramètres principaux utilisés lors du choix des technologies et des appareils dans cet exemple.

a) l'équipe PHA de l'installation approuve tous les appareils utilisés dans le service du SIS;

b) des appareils de faible complexité, familiers avec l'installation;

c) une capabilité systématique avec une source documentée;

d) une philosophie de maintenance et d'essais cohérente avec la capacité/expérience du personnel de l'installation;

e) une interface opérateur/maintenance basée sur les critères existants de l'installation;

f) une estimation des coûts et minutage de l'ordonnancement pour chaque projet;

g) l'utilisation du BPCS pour la diversité du programme d'application (duplication);

h) l'ensemble de la technologie sélectionnée a été précédemment utilisé sur l'installation (c'est-à-dire, utilisations préalables) et est bien compris par le personnel de maintenance de l'installation;

i) les modes et les taux de défaillances pour tout l'équipement (y compris la source de données) sont fournis avec la documentation;

j) l'immunité aux interférences électromagnétiques est présente sur un site industriel;

k) la protection contre les vibrations (par exemple, les cartes à circuit vibrant hors des ports, appareil et défaillance de câbles) garantie pour tout l'équipement.

F.18.2 Solveur logique

Les paramètres de solveur logique incluent:

a) l'application de chaque élément des "Généralités" en F.18.1;

b) le solveur logique du SIS est évalué selon l'IEC 61508 avec une capabilité systématique de SC 3. Elle utilise un langage de variabilité limitée (c'est-à-dire le langage à contacts) pour la programmation d'application;

c) la localisation de tous les solveurs logiques dans la salle de commande de l'installation de fabrication;

d) le temps de sécurité du processus pour les SIF est assez long pour que les temps de réponse PLC types soient adéquats;

e) l'exploitation de l'installation et l'expérience de maintenance (c'est-à-dire, utilisations préalables) ont été considérées pour la sélection du solveur logique de sécurité;

f) l'intégration appropriée avec le BPCS.

F.18.3 Capteurs

Des transmetteurs ont été utilisés à la place d'interrupteurs discrets excepté pour les interrupteurs de position de vanne, où les interrupteurs de proximité ont été utilisés (pour tirer parti des caractéristiques relatives à l'absence de contact).

Les transmetteurs ont été complétés par des diagnostics de valeur de sortie hors plage et incorrects dans les solveurs logiques du SIS et du BPCS.

Les données de taux de défaillances du transmetteur reposaient sur la capabilité systématique fournie soit avec l'évaluation de l'IEC 61508 soit avec les données de conformité de l'IEC 61508, et il a été pris pour hypothèse que de bonnes pratiques d'installation ont été suivies.

Des prises individuelles ont été fournies pour chaque capteur.

Les transmetteurs ont utilisé des appareils programmables (intelligents) avec les fonctionnalités suivantes:

a) Diagnostics, accès à distance aux informations d'étalonnage et fonctions de description de l'appareil à bord qui offre un meilleur niveau d'assurance pour la mise en place et la mise en service correctes de l'appareil correspondant;

b) Les fonctionnalités de sécurité (c'est-à-dire, protection d'écriture, mot de passe, verrouillage) pour restreindre l'accès aux ajustements d'étalonnage qui pourrait entraîner des changements accidentels qui empêchent l'appareil d'effectuer ses fonctions de sécurité;

c) Temps de mise à jour du transmetteur approprié (c'est-à-dire, le délai entre un changement dans le processus et la réponse de sortie du capteur est acceptable);

d) Lorsque nécessaire, les transmetteurs disposent de drains, d'évents et de capacité de connexion d'essais;

e) Les sorties de capteur 4-20 mA des transmetteurs sont connectées directement au SIS et câblées parallèlement au BPCS.

F.18.4 Eléments terminaux

Les appareils de commande terminaux utilisés sont des électrovannes et des vannes de ventilation d'urgence. Les appareils de commande terminaux sont à l'état "désactiver pour déclencher" et atteignent leurs états de sécurité en cas de perte d'alimentation en air ou électrique (c'est-à-dire en cas de défaillance d'ouverture des vannes de ventilation d'urgence).

Les appareils de commande terminaux ont été sélectionnés en fonction de leur utilisation préalable.

F.18.5 Electrovannes

Les électrovannes sont spécifiées d'après les critères suivants:

a) deux bobines moulées à température élevée, de classe H ou F pour rallonger la durée de vie à l'état sous tension en continu (type pour les applications "désactiver pour déclencher");

b) les températures assignées élevées et faibles d'exploitation du solénoïde satisfont ou sont supérieures aux conditions ambiantes dans lesquelles il sera installé;

c) la capacité du chemin de sortie du flux de l'opérateur de la vanne vers l'évent dimensionné afin de satisfaire aux spécifications de temporisation de l'application (temps de réponse de la vanne en dessous de 10 secondes suffisants);

d) la valeur d'arrêt de la (ou des) sortie(s) du solveur logique est suffisamment faible pour garantir que l'électrovanne s'ouvrira lorsque les sorties seront en mode "hors tension".

Le temps moyen pour arriver à une défaillance dangereuse (MTTFd) pour les électrovannes a été déterminé comme suit:

1) les informations sur l'utilisation préalable ont été obtenues à partir de l'expérience d'exploitation réelle (interne et externe) et par l'intermédiaire de données fournies par le fabricant;

2) les informations sur l'utilisation préalable ont indiqué que pendant 140 unités d'années d'utilisation dans des applications similaires, deux défaillances dangereuses d'électrovanne se sont produites (la vanne ne s'ouvrait pas). D'après ces éléments, la limite de confiance inférieure à 70 % (voir l'IEC 61511-1:2016 , notes en 11.9.3 et 11.9.4, et TR84.00.04 -1, TR84.00.09) pour le MTTFd a été calculée à 38,7 ans. Un MTTFd de 35 ans a été sélectionné pour les calculs de la PFD_{avg}.

F.18.6 Vannes de ventilation d'urgence

Les vannes de ventilation d'urgence sont conçues pour assurer l'action des vannes de ventilation en cas de perte d'alimentation et garantir que les signaux d'exploitation satisfont aux exigences de sécurité fonctionnelle. D'après ces éléments et l'évaluation PHA de toutes exigences d'action pour une défaillance différente, les vannes de ventilation d'urgence s'ouvrent en cas de:

a) perte de puissance;

b) perte d'alimentation en air;

c) signal ouvert à partir du solveur logique du SIS ou du solveur logique du BPCS vers l'électrovanne.

En outre, les vannes de ventilation d'urgence sont dotées des caractéristiques suivantes:

1) indication visuelle de la position réelle de la vanne fournie, comprenant:
   – l'indication locale via l'indicateur de position de la tige de manœuvre;
   – indication à distance de la position de la vanne à l'aide d'interrupteurs de fin de course;

2) utilisation d'actionneurs à rappel par ressort. Le dimensionnement de l'actionneur et les considérations de la conception du ressort à sécurité intrinsèque incluent l'analyse appropriée de la pression maximale d'arrêt exigée.

NOTE Pour cette application, des robinets à soupape ont été utilisés, avec le flux sous le blocage.

La surveillance de chaque vanne comprend la comparaison des signaux de vanne avec la position de la vanne, accompagnée du déclenchement d'alarme.

F.18.7 Vannes de modulation

Dans cet exemple, les vannes de modulation n'étaient pas exigées pour la SIF à l'étude.

F.18.8 Vannes de dérivation

L'analyse de l'équipe PHA a déterminé que les vannes de dérivation n'étaient pas nécessaires puisqu'il existe un processus de lot offrant un nombre d'opportunités hors-ligne pour la maintenance. Les équipes d'exploitation et de maintenance ont été consultées à ce sujet et ont approuvé la présente approche.

F.18.9 Interfaces homme-machine (IHM)

F.18.9.1 Généralités

La capacité de l'interface du solveur logique a été conçue pour permettre une interface de sécurité fonctionnelle pour le BPCS pour la duplication, l'interface opérateur, le système d'alarme, les diagnostics et l'échange de valeurs spécifiques.

Les caractéristiques suivantes ont été mises en œuvre dans les interfaces des SIS pour le BPCS:

- utilisation de la console IHM redondante;
- utilisation des liaisons de communication redondantes;
- utilisation d'un chien de garde pour la communication interne des interfaces de gestion des données critiques (toutes les données vers la console d'opérateur du BPCS, par exemple);
- bouton-poussoir d'arrêt (500 PB) installé sur l'une des consoles IHM et recouvert d'un cache de sécurité en plastique afin d'éviter les arrêts accidentels.

Les facteurs considérés dans la conception de l'interface opérateur comprennent:

- les exigences de gestion d'alarme;
- les besoins de réponse de l'opérateur;
- une bonne ergonomie.

Les changements du programme d'application (comprenant les réglages de déclenchement) du SIS peuvent uniquement être effectués par l'intermédiaire des consoles d'ingénierie du SIS avec les mesures de sécurité appropriées (Article F.22).

F.18.9.2 Gestion d'alarme

La gestion d'alarme garantit que les problèmes et dangers sont présentés à l'opérateur de manière à être rapidement et facilement identifiés mais également compris grâce à l'utilisation de la définition des priorités d'alarme. La définition des priorités d'alarme reflète la philosophie de gestion d'alarme du site. Les fonctionnalités mises en œuvre incluent:

- les alarmes pour lesquelles le crédit de réduction de risque est pris dans le LOPA ont la priorité la plus élevée. Il convient que ces alarmes (300 WTHA et 400 LSHA) soient vérifiées à la même fréquence que le SIS, c'est-à-dire deux fois par an;
- les alarmes de prédéclenchement qui déclenchent l'action de l'opérateur avant l'action du SIS ont la priorité la plus élevée;
- l'utilisation des caractéristiques de l'interface opérateur du BPCS qui permettent de distinguer les différents niveaux de priorité d'alarmes;
- l'utilisation des alarmes de prédéclenchement et de déclenchement pour aider à définir les exigences de réponse de l'opérateur;
- les alarmes de diagnostic du SIS qui sont affichées sur un graphique distinct dans le HMF.

F.18.9.3 Réponse de l'opérateur

L'aptitude de l'opérateur à répondre aux alarmes déclenchées par l'IHM exige les mises en œuvre suivantes:

- utilisation de l'enregistrement par séquence d'événements (SOE): le temps de balayage normal du BPCS fournit une véritable fonctionnalité de première alarme;
- utilisation d'alarmes de prédéclenchement: l'opérateur peut engager une action corrective avant qu'une fuite ne se produise (par exemple, ajout d'arrêt court pour éviter une réaction de fuite). Dans ces cas-là, les alarmes de prédéclenchement sont fournies. L'alarme de

prédéclenchement et les réglages de déclenchement prennent en considération les dynamiques du processus et la réponse du capteur.

F.18.9.4 Facteurs humains

Les "facteurs humains" font référence aux paramètres de conception de l'interface qui peuvent affecter l'aptitude de l'opérateur à identifier les informations sur une alarme et son état et à y répondre de manière efficace. Les facteurs de conception mis en œuvre incluent:

- utilisation cohérente de couleurs, éclairages, types, formes et tailles d'interrupteurs, emplacement des interrupteurs, etc.;
- utilisation d'un cache-interrupteur sur l'interrupteur d'arrêt de l'opérateur (500 PB) afin de réduire le risque d'exploitation accidentelle;
- exploitation mécanique des interrupteurs d'arrêt de l'opérateur (tirer pour réinitialiser).

F.18.10 Séparation

F.18.10.1 Généralités

Le Paragraphe F.18.10 décrit la séparation intrinsèque à la conception de chaque SIF.

La séparation a pour but de réduire les défaillances de cause commune et de faciliter la résolution des problèmes liés à la sécurité qui peuvent survenir en raison de changements accidentels. Ces types de problèmes pourraient rendre le SIS et le BPCS indisponibles au même moment. Afin de les résoudre, des approches de conception en cohérence avec la formation de l'installation et l'expérience acquise par la réussite de l'utilisation préalable sont mises en œuvre.

F.18.10.2 Sources de puissance

Il convient de mettre en œuvre la séparation de la puissance d'E/S du SIS des circuits de puissance non-SIS en utilisant un transformateur de distribution séparé pour les circuits de dérivation du panneau de puissance de l'instrument du SIS. Cette mise en œuvre apporte une défense contre les défaillances de cause commune relatives aux problèmes de mise à la terre. La distribution de la source de puissance du SIS est ensuite séparée pour garantir que les sources de puissance redondantes [c'est-à-dire l'alimentation en puissance normale et sans coupure (UPS)] sont routées en étant physiquement séparées et que les circuits de dérivation sont divisés pour traiter les entrées, solveurs logiques, alimentation(s) de puissance E/S, sorties à charge et sorties de diagnostic.

Les systèmes de coffres séparés (par exemple conduits, chemins de câbles, gaines et goulottes) ne sont pas exigés car les problèmes de compatibilité électromagnétique (EMC) sont résolus de manière cohérente avec les bonnes pratiques en matière d'ingénierie pour:

- les niveaux d'énergie d'application maximale (480 V et moins);
- la spécification et l'espacement des câbles/coffres/équipements;
- la séparation des conducteurs de puissance et des signaux des instruments (soit 4-20 mA) en différents câbles;
- l'identification unique (c'est-à-dire un codage de couleur) de l'équipement du SIS;
- la protection des points de connexion aux bornes du SIS;
- le programme d'installation informatisé de câblage identifiant chaque conducteur, câble, coffre et point de connexion.

F.19 Défaillances de cause commune et défaillances systématiques

F.19.1 Généralités

Les Paragraphes F.19.2 à F.19.19 ci-dessous définissent la conception permettant de résoudre les problèmes liés aux défaillances de cause commune et aux défaillances systématiques.

Les techniques de conception mises en œuvre pour éviter les défaillances de cause commune comprennent la séparation, la redondance, la diversité et la revue par les pairs.

Les techniques utilisées pour éviter les erreurs systématiques comprennent la revue par les pairs, l'utilisation d'approches de conception avec des rapports d'utilisations préalables positifs, la diversité et la comparaison de diagnostics.

F.19.2 Diversité

La diversité est atteinte grâce à l'utilisation de différents équipements (SIS et solveurs logiques BPCS), des conceptions différentes pour la réalisation d'une fonction commune (programme d'application du SIS et duplication du BPCS), ainsi que de différents programmes d'application imbriqués et les programmeurs.

F.19.3 Erreurs de spécification

Des erreurs de spécification (par exemple une plage de températures ambiantes erronée, des paramètres incorrects [par exemple 0 °C à la place de 0 °F] ou une métallurgie inappropriée pour un groupe d'instruments) ont été identifiées et corrigées grâce à l'utilisation de la revue par les pairs par du personnel habitué au sujet traité.

F.19.4 Erreurs de conception du matériel

Les erreurs de conception du matériel ont été résolues par l'utilisation d'équipement de SIS satisfaisant aux critères d'utilisation préalable de l'évaluation IEC 61508, des données de conformité de l'IEC 61508 ou de l'analyse d'approbation de l'installation. La conception est conforme aux meilleures pratiques d'entreprise et comprend un manuel de sécurité pour chaque appareil certifié, un manuel d'application pour les appareils non certifiés, ainsi que la revue par les pairs.

F.19.5 Erreurs de conception du logiciel

L'équipement PE a été choisi en fonction de l'utilisation préalable et de l'évaluation selon l'IEC 61508 ou de la conformité à l'IEC 61508. Le programme d'application du BPCS a été utilisé pour "dupliquer" le programme d'application du SIS, procurant donc les avantages des différents logiciels intégrés.

Afin de réduire les défaillances systématiques dues aux erreurs du logiciel intégré, une comparaison entre les deux capteurs de pression et une limite minimale et maximale ont été configurées à la fois dans le SIS et le BPCS.

Les erreurs systématiques de commande du programme d'application ont été résolues par la mise en œuvre de plusieurs des techniques et des mesures listées, y compris:

- un langage de variabilité limitée pour toutes les programmations d'application, sauf si une programmation à variabilité figée était disponible (les transmetteurs basés sur PE ou les commandes de l'opérateur basées sur PE, par exemple);
- un schéma de documentation logique (voir la Figure 11) qui pourrait être interprété par toutes les personnes concernées, et offrant une documentation explicite relative au processus intégrée dans la documentation du programme d'application;

- une revue par les pairs et des outils de simulation ont été utilisés pour réduire le nombre d'erreurs de conception du programme d'application;
- "la duplication" pour surveiller en permanence les performances du programme d'application et assurer la diversité de programmation;
- les exigences du manuel de sécurité des fabricants.

F.19.6 Contraintes environnementales

La conception de l'installation ne tient pas compte des séismes ou des accidents d'avion, mais elle est spécifiée pour résister à un ouragan de niveau 5. Les conditions environnementales auxquelles le SIS sera exposé qui ont été prises en compte sont:

- la température;
- l'humidité;
- les contaminants;
- les vibrations;
- la mise à la terre;
- le conditionnement de la ligne d'alimentation;
- La compatibilité électromagnétique (CEM).

F.19.7 Température

Les appareils de SIS, tels que les duplications logiques, les modules d'E/S, les capteurs et les éléments terminaux subissent des dommages liés aux températures extrêmes. Les décisions de conception relatives à la température mises en œuvre lors de la conception comprennent:

- les températures d'exploitation telles que spécifiées par les fabricants;
- l'emplacement de l'équipement dans des zones où les plages de températures restent comprises dans les spécifications des fabricants;
- la protection contre les intempéries et le contrôle de la température pour les équipements d'extérieur;
- selon le cas, il convient d'utiliser des collecteurs de condensats ou des drains, voire d'assécher l'air de l'instrument pour réduire les défaillances potentielles dues à la formation de glace;
- des câbles chauffants, lorsque cela est exigé.

F.19.8 Humidité

Il convient de maintenir l'humidité relative selon les exigences des fabricants (généralement inférieure à 90 % pour les systèmes électroniques). Pour réduire les effets préjudiciables de forts taux d'humidité (par exemple vapeur, extérieur), il convient de protéger les assemblages électroniques en appliquant des revêtements enrobant ou en utilisant des "lubrifiants de contact" antihumidité afin d'assurer une connexion étanche au gaz entre les connecteurs.

F.19.9 Contaminants

Afin de prévenir toute contamination potentielle, il convient de remplir les conditions suivantes:

- une ventilation adéquate et une protection contre la poussière de l'environnement immédiat;
- lorsque les atmosphères corrosives constituent un problème, l'installation de filtres ou de matériaux absorbants est dispensée pour le système CVC et une purge (air) est mise en œuvre pour tous les autres équipements;

- pour l'électronique montée de terrain, l'utilisation de coffrets purgés et/ou de revêtement enrobant ainsi qu'une forme quelconque de protection sur les connecteurs.

F.19.10 Vibration

L'immeuble est secoué par des vibrations. Pour contrer ce problème, tous les appareils enfichables de SIS (par exemple les relais "glaçon", ou les cartes d'E/S) sont fournis avec un mécanisme de verrouillage positif. Le coffret du solveur logique du SIS utilise des montages d'isolation de vibration afin de minimiser la transmission de vibrations du coffret au solveur logique.

F.19.11 Mise à la terre

La mise à la terre a été conçue pour faciliter l'utilisation de technologies électroniques programmables par la mise en œuvre:

- résistance du système de mise à la terre inférieure à 5 ohms;
- utilisation du système Ufer (surface) de mise à la terre;
- acier de construction électriquement continu;
- mise à niveau du "cône de protection" en acier de construction avec des conducteurs de cuivre où ils sont exigés.

F.19.12 Conditionnement de la ligne d'alimentation

Le conditionnement de la ligne d'alimentation a été conçu pour protéger le SIS des anomalies de la ligne d'alimentation telles que les défaillances électriques, la foudre, les fléchissements, les creux de tension, les ondes de choc et les pics.

La protection contre la foudre est garantie par la mise en œuvre des appareils de protection qui sont:

- coordonnés à la capacité de résistance (par exemple court-circuit, surcharge) des appareils protégés;
- localisés pour protéger chaque appareil du SIS ainsi que le cône de protection.

Le réseau de distribution d'énergie existant comporte un résidu harmonique. Le réseau de distribution d'énergie du SIS a été conçu pour fournir une protection contre les harmoniques.

La protection contre la surcharge et le court-circuit du SIS a été assurée par les fonctionnalités suivantes:

- fusibles individuels pour chacun des circuits d'E/S afin de limiter les effets d'une défaillance dans ce circuit;
- coordination du fusible de dérivation avec les circuits alimentant la dérivation pour minimiser la possibilité de voir une partie majeure de la structure d'E/S désactivée par une défaillance de niveau faible.

F.19.13 Compatibilité électromagnétique (CEM)

Les systèmes électroniques et électroniques programmables utilisent des signaux de niveau faible, des circuits numériques, des microprocesseurs, des puces de mémoire, etc., différents et sensibles aux bruits électriques comme les interférences électromagnétiques (IEM) par exemple. Les interférences électromagnétiques générées par les systèmes de communication personnels (les radios portables bidirectionnelles, les stations radio fixes, les téléphones cellulaires, les ordinateurs personnels, les modems sans fil et les appareils d'entraînement à fréquence variable, par exemple) ont été évaluées au cours de la conception. Le SIS a été conçu pour résoudre ce problème par la mise en œuvre des fonctionnalités suivantes:

a) des enveloppes électroniques assurent la protection du SIS contre les sources de bruits externes (à l'extérieur du coffret);

b) la conception du coffre et des câbles assure la protection du SIS contre les sources de bruits internes (à l'intérieur du coffret);

c) des filtres de bruit ont été installés où cela est exigé.

Les techniques supplémentaires de réduction des interférences électromagnétiques comprennent:

1) des enveloppes métalliques;

2) des barrières métalliques;

3) le blindage des câbles et des fils;

4) le câblage par paires torsadées;

5) la mise à la terre correcte;

6) la localisation correcte de l'appareil;

7) le cheminement des fils à distance de la source d'interférence électromagnétique;

8) la séparation.

Les critères de sélection d'un équipement du SIS exigent que l'équipement soit en mesure de résister à des niveaux d'interférences électromagnétiques généralement présents dans un environnement industriel. Cela a été possible grâce à:

- la spécification d'un équipement conçu, fabriqué et soumis à l'essai conformément aux normes applicables (l'IEC 61131, TUV, par exemple);
- l'installation de l'équipement conformément aux lignes directrices d'installation des fabricants.

F.19.14 Sources utilitaires

L'électricité et l'air de l'instrument sont des utilitaires clés au service du SIS. Le contenu et la qualité de leur conception sont directement relatifs à leur disponibilité au service du SIS. La conception mise à part, il a été pris pour hypothèse au cours de l'analyse préliminaire des risques (APR) que des pièces ou l'ensemble de ces utilitaires ne seraient pas disponibles.

L'entreprise de distribution et le personnel de l'installation (par exemple, centrale électrique, autre processus d'exploitation) ont été consultés pour évaluer la disponibilité des sources utilitaires existantes. D'après ces informations, les sources utilitaires ont été conçues avec des fonctionnalités visant à optimiser la disponibilité, y compris:

- L'air de l'instrument
  - l'utilisation d'une qualité de l'air de l'instrument propre et sèche;
  - une capacité de puissance pneumatique suffisante fournie aux appareils de commande terminaux afin de leur assurer un temps d'exploitation adéquat;
  - les évents bénéficient d'une protection contre le blocage, la poussière, les insectes et le gel;
  - la longueur et le diamètre de la puissance pneumatique et de la tubulure de signal sont établis de manière à assurer des performances satisfaisantes.
- Electricité
  - une source d'alimentation redondante a été utilisée pour le solveur logique du SIS, les entrées, l'IHM et les sorties de diagnostic;
  - un délai sous protection de tension (30 cycles) pour les charges motrices a été fourni;
  - la source d'alimentation de secours possède la même qualité de l'énergie que la source principale;

- des sources d'alimentation de secours (par exemple, ASI) localisées de manière à pouvoir assurer la maintenance de chacune sans affecter les performances des autres;
- le SIS a été conçu avec un démarrage permissif qui exige la disponibilité de l'ensemble des circuits électriques du SIS.

F.19.15 Capteurs

Des prises séparées sont utilisées pour chaque capteur afin de minimiser les défaillances de cause commune.

F.19.16 Traitement de la corrosion ou de l'encrassement

Ce processus a limité le potentiel d'atteinte des conditions du processus anormales menant à la corrosion. Il s'agit également d'un processus de lot, qui facilite le nettoyage entre chaque exécution de processus. Aucune exigence conceptuelle particulière n'a été mise en œuvre.

F.19.17 Maintenance

L'organisation de la maintenance a participé à la planification, la vérification et l'approbation de la conception. Une attention toute particulière a été portée à la conception car elle est relative à l'étalonnage, aux exigences de formation, à la dérivation et aux essais.

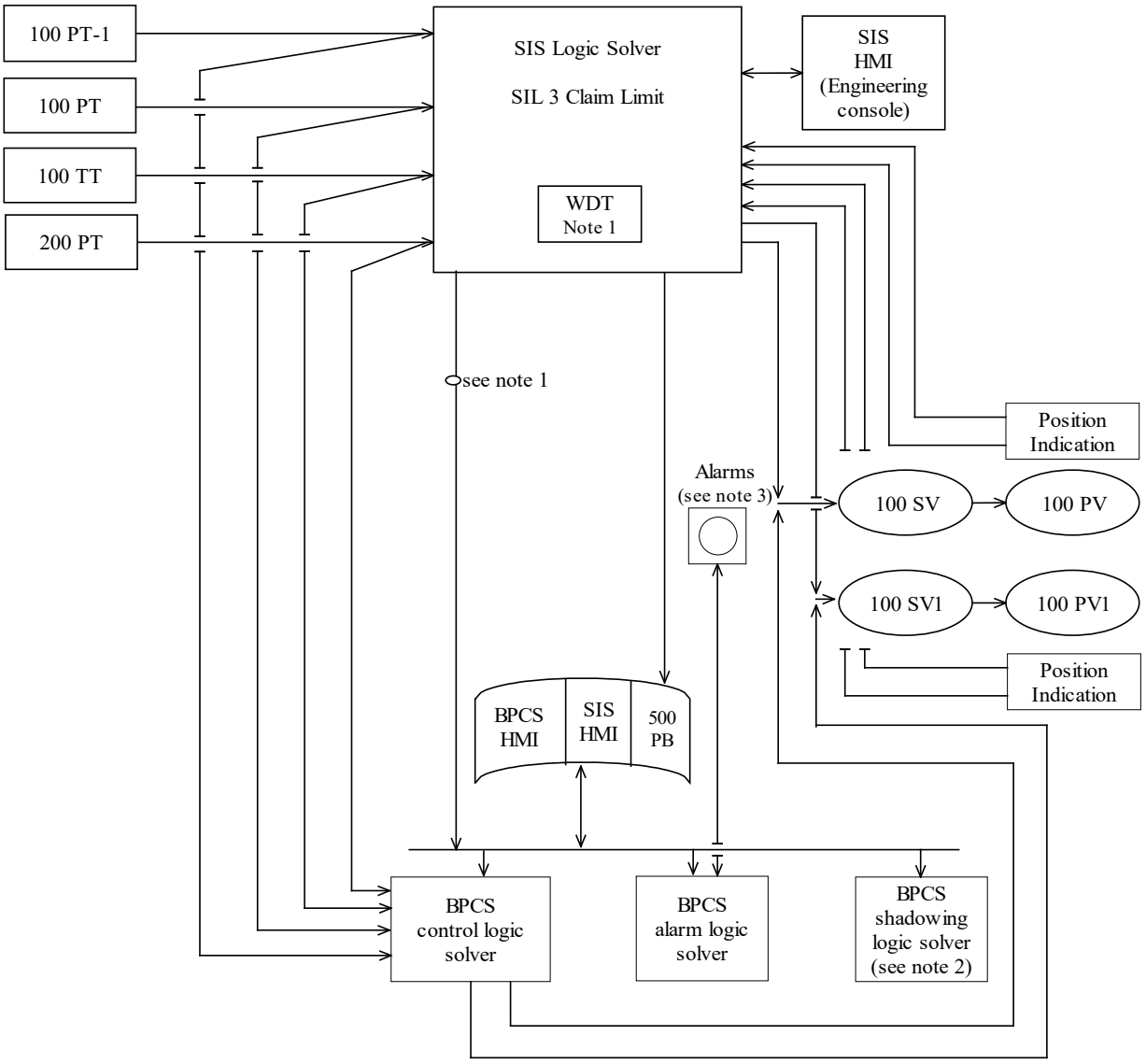
F.19.18 Susceptibilité à la mauvaise manipulation

L'organisation opérationnelle a participé à la planification, la vérification et l'approbation de la conception. Une attention toute particulière a été portée à la conception, car il s'agit de simplifier les procédures de fonctionnement, de limiter les exigences d'intervention des opérateurs lors du cycle de production, de disposer de modes de fonctionnement appropriés pour assurer la terminaison des lots à des intervalles clés, de soumettre le programme d'application à l'essai pour s'assurer qu'il satisfasse à tous les besoins de processus et de confirmer que les problèmes liés à la gestion d'alarme/l'IHM ont été résolus avec succès.

F.19.19 Architecture du SIS

Les éléments suivants décrivent l'architecture du SIS. La Figure F.12 présente l'architecture du SIS. Le Paragraphe F.19.19 a pour objet de présenter l'architecture du SIS, ainsi que ses relations avec les influences extérieures (BPCS, IHM, capteurs et éléments terminaux, par exemple).

Le BPCS communique avec le SIS par une autoroute de données. Toutefois, les exigences de sécurité exigent que les changements de point de consigne du SIS et les changements de configurations du SIS puissent être effectués uniquement à partir de la console d'ingénierie du SIS dédiée. Il convient de connecter la console d'ingénierie du SIS directement au SIS depuis la salle de commande à chaque changement des points de consigne ou de la configuration du SIS.



Note #1 - Communication link to the SIS HMI is supplemented with a communication WDT ensuring SIS HMI is functional during the operational cycle.
Note #2 - Shadowing of SIS application software.
Note #3 - Weigh cell & level alarms (300 WTA & 400 LSA [see figure 11]).

Project #	Revision #	Revision	RVSD	CHKD	APPD	Date

Project # YYYY Date:
Drawn: S. Bulk _____
Checked: V. May _____
R. Brown _____
Approved: W. Burk _____
DWG# XXXXX1

IEC

Anglais	Français
SIS logic solver	Solveur logique du SIS
SIL 3 claim limit	Limite de demande SIL 3
SIS HMI (engineering console)	IHM SIS (console d'ingénierie)
WDT Note 1	WDT Note 1
See Note 1	Voir Note 1

Anglais	Français
Position indication	Indication de position
Alarms (see Note 3)	Alarmes (voir Note 3)
BPCS HMI	IHM BPCS
SIS HMI	IHM SIS
BPCS control logic solver	Solveur logique de commande BPCS
BPCS alarm logic solver	Solveur logique d'alarme BPCS
BPCS shadowing logic solver (see Note 2)	Solveur logique de duplication BPCS (voir Note 2)
Note 1 Communication link to the SIS HMI is supplemented with a communication WDT ensuring SIS HMI is functional during the operational cycle.	Note 1 Le lien de communication vers l'IHM SIS est complété par un WDT de communication pour assurer le fonctionnement de l'IHM SIS pendant le cycle opérationnel.
Note 2 Shadowing of SIS application software.	Note 2 Duplication du logiciel d'application du SIS.
Note 3 Weigh cell & level alarms (300 WTA & 400 LSA [see Figure 11]).	Note 3 Cellule de poids et niveaux d'alarmes (300 WTA et 400 LSA [voir Figure 11]).
Project #	N° de projet
Revision #	N° de révision
Revision	Révision
Date	Date
Drawn:	Dessiné par:
Checked:	Vérifié par:
Approved:	Approuvé par:

Figure F.12 – SIS pour le réacteur VCM

F.20 Fonctionnalités de conception du programme d'application du SIS

La documentation du programme d'application contient des commentaires suffisamment détaillés pour expliquer la fonction de chaque symbole et de chaque SIF, et la relation qui lie chaque symbole à sa SIF. Les commentaires sont suffisamment complets pour aider les ingénieurs et le personnel de maintenance à comprendre les fonctions du programme d'application et à naviguer dans le programme d'application.

F.21 Pratiques de câblage

De bonnes pratiques de câblages sont essentielles pour parvenir à la disponibilité du SIS désirée. Voici une liste des pratiques de câblage mises en œuvre dans ce SIS:

- Les circuits ne partagent pas de conducteurs neutres ou retours communs en courant continu afin de minimiser:
  - la possibilité d'interruption accidentelle si un ou des circuit(s) si un conducteur neutre ou commun est soulevé ou ouvert;
  - le potentiel de boucles de terre et les erreurs de câblage;
  - des circuits de dérivation additionnels (10 % de rechange et 20 % d'espace) sont fournis.
- Les caractéristiques de fusibles d'E/S comprennent:
  - l'utilisation de circuits d'E/S individuellement à fusible individuel pour mieux isoler les défaillances et minimiser le potentiel des effets de cause commune;
  - l'utilisation d'E/S de type isolé;
  - l'utilisation de fusibles externes (c'est-à-dire extérieurs aux fusibles d'E/S PLC) où ils sont exigés et lorsque le retrait d'une carte peut être minimisé;

  - l'utilisation de blocs de jonction de support de fusible (avec un support de fusible intégral/levier de déconnexion) comme moyen de déconnexion à des fins de maintenance.
- L'utilisation de verre transparent résistant CEM afin d'assurer un accès visuel aux informations de diagnostic (lumières d'E/S, par exemple).
- Des lumières internes (c'est-à-dire à l'intérieur du coffret de solveur logique SIS) et un réceptacle de verrou pivotant pour le SIS afin de pouvoir éliminer les appareils inductifs raccordés.
- Les raccordements du SIS sont identifiés lorsqu'ils sont localisés près de terminaux non-SIS.
- Le câblage par paires torsadées a été utilisé pour minimiser le bruit magnétique ou de cause commune où cela est exigé.

F.22 Sécurité

Les mesures de sécurité prises conformément à la conception du SIS conservent l'intégrité de sécurité en prévenant les modifications non autorisées ou accidentelles de toute fonction ou tout appareil du SIS y compris le solveur logique, la logique d'application, les interfaces utilisateur, les capteurs et les éléments terminaux. Pour ces appareils (les appareils d'interface) pour lesquels le contrôle de l'accès physique est plus difficile, il convient de mettre en œuvre l'utilisation de procédures administratives.

Quelques approches de sécurité de base mises en œuvre sont énumérées ci-après:

- l'approbation écrite et les raisons pour lesquelles l'accès est demandé;
- l'approbation écrite et l'identification des personnes demandant l'accès;
- la définition de la formation et/ou du niveau de connaissance du système exigé(es) avant de permettre l'accès;
- la définition des personnes devant avoir accès au système, sous quelles conditions, et pour quel type de travail à effectuer. Cela comprend les procédures nécessaires au contrôle de l'utilisation de dérivations de maintenance.

Les caractéristiques du SIS qui facilitent le contrôle d'accès. Les exemples de telles fonctions de conception incluent:

- l'identification claire des appareils du SIS à l'aide de couleurs distinctives;
- la séparation physique de l'équipement du SIS et BPCS (ce qui facilite la sécurisation des enveloppes associées avec des clés de verrouillage);
- l'utilisation de technologies variées (ce qui exigerait généralement une interface de maintenance différente).

L'utilisation du SIS basé sur PES a créé des soucis de sécurité supplémentaires dus à la facilité relative avec laquelle il est possible d'effectuer des changements dans la logique d'application. Pour ces systèmes, des fonctionnalités supplémentaires ont été mises en œuvre, y compris:

- l'accès restreint à l'interface de maintenance/d'ingénierie;
- l'établissement de règles/procédures administratives qui définissent les conditions sous lesquelles l'interface de maintenance peut être connectée au système au cours d'une opération normale;
- l'utilisation d'un logiciel de vérification de virus et de procédures de gestion des programmes et des fichiers appropriées de la console d'ingénierie pour aider à éviter la corruption de la logique imbriquée et/ou d'application;

- l'utilisation d'un logiciel utilitaire du SIS qui suit les révisions de la logique d'application et permet de savoir (post-factum) à quel moment un changement a été opéré, par qui et quels ont été les changements apportés;
- pas de connexion externe du SIS ou BPCS à internet ou aux lignes téléphoniques.

F.23 Etape F.5: Installation, mise en service et validation du SIS

Tableau F.17 – Cycle de vie de sécurité du SIS – Zone 5

Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigences Article ou paragraphe de l'IEC 61511-1:2016**	**Entrées**	**Sorties**
IEC 61 511-1:2016 Figure F.7, zone 5	Installation, mise en service et validation du SIS	Intégrer et soumettre à l'essai le SIS Valider que le SIS satisfait, en tous points, aux exigences de sécurité, en termes de SIF et d'intégrité de sécurité exigées	12.3, 14, 15	Conception du SIS Plan d'essai d'intégration du SIS Exigences concernant la sécurité du SIS Plan de validation de sécurité du SIS	SIS fonctionnant entièrement en conformité avec les résultats des essais d'intégration du SIS, prévus à la conception du SIS Résultats des activités d'installation, de mise en service et de validation

Le Tableau F.17 donne les objectifs, les entrées, les sorties et les références aux articles et paragraphes connexes pour l'installation, la mise en service et la validation du SIS.

F.24 Installation

L'installation du SIS a commencé avec la disponibilité de conception, des locaux de fonction, d'équipement du processus, des utilitaires (par exemple, électrique) et de l'équipement d'instrumentation. L'installation s'est achevée avec la transition (c'est-à-dire le roulement) du SIS du mode construction à opérations. Cette transition a reflété l'acceptation par le mode opérations. Dès lors, la mise en service a été démarrée (voir Article F.24).

Les fonctions d'inspection des achats et des réceptions en entreprise étaient considérées comme permettant de garantir que les appareils SIS spécifiés étaient reçus dans le bon ordre, avec la documentation appropriée à leur utilisation conformément à 11.5 de l'IEC 61511-1:2016 . Le stockage temporaire est conforme au manuel de sécurité du fabricant pour chaque appareil, et inclut une maintenance préventive nécessaire de l'équipement.

Il est à noter qu'une procédure visant à retourner au mode installation était disponible, que des corrections aux problèmes rencontrés par le mode opérations pourraient être mises en œuvre. Cette transition a créé un déséquilibre entre les états de fin/acceptation différents de l'équipement adjacent (c'est-à-dire état installation contre opérations). Au cours de ce projet, un marqueur blanc a été utilisé pour l'état opérations et un marqueur vert pour l'état construction.

Chaque instrument a été identifié avec son propre numéro d'étiquette. Le SIS a bénéficié des caractéristiques d'identification supplémentaires suivantes:

- toute l'instrumentation du SIS a reçu une identification visuelle (par exemple, peinte en rouge) de son statut en tant qu'appareil du SIS;
- le coffret du SIS a reçu une plaque signalétique référençant les numéros de dessin du SIS;

- les IHM SIS ont été identifiées (identification de plateau logicielle) en tant qu'appareils liés au SIS;
- chaque appareil SIF a été identifié avec une étiquette portant son numéro de dessin de ligne et son numéro SIF.

La construction n'avait aucun lien avec l'installation du programme d'application. Le programme d'application a été développé, soumis à l'essai et vérifié au cours de la conception, et a été introduit dans le SIS au moment de la mise en service.

Les activités de vérification de la construction précédant la transition vers le mode opérations comprennent:

- la "limitation" du câblage installé pour assurer la mise à la terre et l'interconnexion du SIS correctes;
- la mise sous tension des commandes (garantissant ainsi l'absence de court-circuit ou de surcharges) y compris les E/S;
- "surélévation" (par exemple, activation "jog" courte) de chaque moteur et de chaque valve garantissant l'exécution de l'opération dans la direction correcte;
- la garantie de fonctionnalité de tous les utilitaires (par exemple, les pneumatiques);
- la "lecture croisée" pour vérifier que l'installation est complète, sûre et correcte;
- la mise à disposition d'une documentation complète et de construction du SIS.

Les opérations ont participé aux activités de vérification ci-dessus afin que le mode opérations:

- comprenne les limites de la batterie et la localisation des appareils du SIS;
- comprenne la localisation des utilitaires et de leurs appareils critiques, par exemple, la protection contre la déconnexion, la surcharge ou le court-circuit (par exemple, les fusibles ou les disjoncteurs);
- puisse fournir les détails nécessaires au plan de mise en service (voir l'Article F.25);
- la maintenance s'est familiarisée avec l'installation du SIS en travaillant sous la supervision de construction, afin de procéder aux activités de vérification du SIS sélectionnées, traitées dans le présent document ("limitation" du SIS, par exemple).

L'installation terminée a été vérifiée et approuvée par une équipe d'inspection composée de personnel des états de construction, d'opérations et de conception. Une fois terminé, l'équipement a été marqué pour signifier l'acceptation du mode opérations et le propriétaire (c'est-à-dire le responsable de l'équipement).

F.25 Mise en service

Le terme "mise en service" fait référence à la période qui commence à la fin de la transition (c'est-à-dire du mode construction au mode opérations) et se termine par la vérification que la mise en service du SIS a abouti et peut passer au mode validation (voir l'Article F.27). Dans cet exemple, la mise en service du SIS a démarré immédiatement après la mise en service du BPCS.

La mise en service du SIS inclut la vérification de l'identification, l'ordonnancement, la planification, l'organisation, la supervision et la documentation du système matériel du SIS, ainsi que la vérification des systèmes d'exploitation (c'est-à-dire, les logiciels intégrés).

Dans la mise en service de cet exemple, il est également fait référence au SIS avec le terme "vérification" qui reflète mieux l'activité majeure mise en œuvre au cours de la mise en service. La vérification est une procédure étape par étape qui garantit que:

- toute la connectivité du SIS est correcte (y compris la mise à la terre);
- tous les utilitaires (par exemple, électrique ou pneumatique) fonctionnent correctement;
- tous les appareils du SIS (par exemple, capteurs, solveur(s) logique(s), éléments terminaux, IHM, stations d'ingénierie, systèmes de communication) sont sous tension et fonctionnent correctement;
- les paramètres des capteurs sont corrects.

Les appareils avec des langages de programmation fixés (FPL) (par exemple, les transmetteurs intelligents) ont été vérifiés à ce moment. La station d'ingénierie du solveur logique de PE et sa fonction "force" ont été utilisées au cours de cette vérification. L'équipe de maintenance de l'installation a constitué une équipe clé de cette activité, avec le soutien de la construction et de la conception, lorsque cela est nécessaire. Les équipes d'opérations ont approuvé la mise en service et l'ont déclarée terminée et satisfaisante avant de procéder à la validation.

F.26 Documentation

Il convient de mettre à la disposition du personnel la documentation nécessaire. En conséquence, une vérification a été menée afin de s'assurer que l'ensemble de la documentation était disponible et correct avant de procéder à la validation.

La liste finale des documents approuvés comprend:

- la documentation relative à l'analyse de danger et de risque (Simulations (Tableau F.4), HAZOP (Tableau F.5));
- le classement du risque tolérable (Tableau F.8);
- la documentation relative à l'affectation de risque aux couches de sécurité – détermination du SIL de chaque SIF (LOPA);
- la procédure d'essai pour chaque SIF (voir l'Article F.27);
- spécification des exigences de sécurité, y compris:
  - les schémas P&I;
  - les schémas logiques;
  - l'impression du programme d'application;
  - les manuels de sécurité;
  - l'évaluation de la justification de sécurité corporelle;
  - la documentation relative à la méthode de justification de sélection de l'équipement;
  - les instructions d'installation du fabricant;
  - la documentation relative au matériel du SIS/au programme d'application/à l'installation/à la maintenance;
  - la justification de la capabilité systématique;
  - les calculs de vérification du SIL (c'est-à-dire la PFD_{avg}) pour la SIF, y compris les schémas architecturaux.

F.27 Validation

Le terme "validation" fait référence à la période qui commence après la fin de la mise en service et se termine avec la conclusion certifiant que le SIS satisfait aux exigences de fonctionnalités définies dans le SRS.

La validation du SIS a commencé après la mise en service du SIS et la validation du BPCS.

La validation du SIS inclut l'identification, l'ordonnancement, la planification, l'organisation, la supervision et la documentation d'un certain nombre d'activités. Ces activités liées au SIS comprennent:

- la mise en route du système matériel du SIS;
- la mise en route des systèmes d'exploitation (c'est-à-dire, les logiciels intégrés) du SIS;
- mise en route du programme d'application;
- le démarrage du SIS (approbation de l'essai d'acceptation et transition vers la production, c'est-à-dire la division des opérations).

Au cours de la validation de cet exemple, le SIS a été divisé en "mise en route" et "démarrage" pour mieux refléter les activités majeures mises en œuvre dans la validation.

La mise en route est une procédure étape par étape qui s'assure de la fonctionnalité correcte du SIS en utilisant des matériaux de processus non dangereux (par exemple, de l'eau à la place d'un liquide dangereux) tout en exécutant le processus comme s'il fabriquait un produit fini. A cet égard, le programme d'application du solveur logique du SIS a été installé (voir l'Article F.23) et soumis à l'essai (voir l'Article F.27) minutieusement pour chacun de ses modes de fonctionnement (démarrage, exécution, arrêt, par exemple). Le personnel de production a joué un rôle clé au cours de la validation, avec le soutien des équipes de maintenance et de conception. A l'issue de la finalisation réussie et de l'approbation des opérations de mise en route, le SIS a effectué la transition vers le démarrage.

Le démarrage est une activité qui exige la production sûre d'un produit de qualité par les opérations, à un taux de productivité prédéfini. Au cours de cette procédure, les appareils du SIS ont été vérifiés pour garantir leur fonctionnalité correcte et leur capacité à effectuer les fonctions de sécurité, telles qu'établies au cours de la mise en route. Une fois cette vérification terminée avec succès, les résultats ont été documentés et l'approbation des opérations finalisée. La validation de ce projet de SIS a été terminée.

F.28 Essais

La plupart des essais exigés présentés à l'Article F.28 ont été effectués au cours de la validation initiale du SIS. Les procédures d'essais décrites ci-dessous sont également utilisées pour les essais périodiques et l'inspection décrits à l'Article F.29, Etape 6.

La procédure d'essai a été écrite par le concepteur du SIS. La procédure a inclus la reconnaissance du potentiel pour les incidents liés à la sécurité comme le résultat des essais sur la SIF. Ainsi, la procédure d'essai expliquait clairement la manière de procéder aux essais en toute sécurité, ainsi que la quantité/qualité de l'équipement et du personnel exigé.

Les activités suivantes ont été incluses dans les essais:

- essais d'appareil;
- essais en atelier et étalonnage;
- simulation;
- la logique a subi les essais séparément;
- essais automatiques;
- essais manuels;
- documentations des conditions "tel quel" et "en l'état";
- procédure par étape détaillée.

Certaines fonctionnalités principales ont subi des essais au-delà du réglage de déclenchement et des appareils de commande terminaux. Les diagnostics, tels que la perte

de signal, ont subi des essais, que le diagnostic ait généré des alarmes ou qu'il ait mené le processus à un état de sécurité. Le verrouillage de la SIF et la logique de réinitialisation ont été soumis à l'essai, y compris la position de l'appareil de commande terminal sur réinitialisation. La position de réinitialisation a été documentée et soumise à l'essai.

L'interaction du SIS avec le BPCS a été soumise à l'essai. Les indications de la SIF envoyées au BPCS ont été soumises à l'essai ainsi que toutes les actions prises relativement à ces indications. La duplication du BPCS sur la logique du SIS a été soumise à l'essai indépendamment, de manière à prouver le bon fonctionnement des deux systèmes.

Voici une procédure générale pour les essais de la SIF:

- Mettre les autres SIF qu'il convient de désactiver en dérivation pour ne soumettre à l'essai que la SIF ciblée.
- Simuler des conditions normales de fonctionnement:
  - simuler les signaux des instruments dans les conditions normales de fonctionnement;
  - mettre les appareils de commande terminaux ciblés sur la position de fonctionnement normal;
  - mettre les contrôleurs et les autres appareils sur le mode de fonctionnement normal.
- Soumettre la SIF à l'essai:
  - enregistrer le point de déclenchement réel de la SIF;
  - vérifier l'alarme de la SIF et les actions sur les appareils de commande terminaux;
  - vérifier que la SIF BPCS a relié les actions.
- Effacer la condition de la SIF:
  - vérifier que les actions de la SIF restent en état de sécurité.
- Réinitialiser la SIF:
  - vérifier que les actions de la SIF se réinitialisent à l'état désigné.

La procédure d'exemple prend pour hypothèse que les instruments ont été soumis à l'essai en atelier et étalonnés. La procédure d'exemple a été écrite pour soumettre à l'essai toutes les fonctions du SIS en même temps, plutôt qu'à une procédure individuelle pour chaque SIF. La procédure vérifie d'abord les fonctions principales du SIS et les appareils de commande terminaux. Chacune des actions d'essai listées suivantes soumet une SIF à l'essai sans soumettre à l'essai à nouveau les appareils de commande terminaux. Chaque action d'essai comprend une procédure d'essai au cas où un transmetteur serait remplacé ou un réglage de déclenchement modifié.

La validation réussie de la phase d'essais tient principalement au personnel d'exploitation d'installation et de maintenance impliqué qui a assuré la compréhension limpide de tous les aspects du processus, du BPCS et du SIS. Personnel inclus:

- opérateur de salle de commande qualifié;
- techniciens d'instruments et électriques qualifiés.

Le Tableau F.18 ci-dessous énumère les types d'instruments et quelques procédures d'essais utilisées.

Tableau F.18 – Liste des types d'instruments et des procédures d'essais utilisées

PRESSION	
Connexions normales	Fournir des drains/évents et soumettre à l'essai des connexions de pression en aval de la valve de sectionnement principale.
Joints du diaphragme à distance	Il convient de fournir les valves d'isolation et les anneaux d'étalonnage pour les soumettre à l'essai en ligne. Prendre en compte l'élévation relative aux prises et la gravité spécifique du tube capillaire rempli de fluide lors de la validation de l'étalonnage.
TEMPERATURE	
Thermocouple	Une vérification de continuité peut être menée sur l'appareil pour déterminer l'opérabilité seulement. Vérifier la sortie mV à une température connue par rapport à une courbe normalisée.
Détecteurs de températures à résistance (RTD)	La résistance peut être mesurée pour vérifier l'opérabilité d'un appareil. Vérifier la résistance à une température connue par rapport au tableau de normes d'étalonnage.
Systèmes pleins	Retirer l'appareil de détection et le placer dans le bain de température.
Interrupteur bimétallique	Retirer l'appareil de détection et le placer dans le bain de température.

La procédure suivante est un exemple pour la validation des fonctions du SIS, y compris les alarmes de diagnostic. Cet exemple n'inclut pas les essais des fonctions du BPCS. L'essai (ou le remplacement) de tout appareil du SIS (par exemple, capteur, solveur logique, élément terminal) est recommandé par le fabricant. Cela peut ne pas être spécifié dans cette procédure d'exemple mais, par hypothèse, être mis en œuvre séparément. Voir l'ISA-TR84.00.03:2012, *Mechanical Integrity of Safety Instrumented Systems (SIS).* Pour des exemples de procédures d'essai, voir la section relative aux essais périodiques du manuel de sécurité du fabricant. Une procédure d'essai complète peut également comprendre des essais sur:

- les actions du BPCS sur l'activation de la fonction de sécurité, telles que la commutation en mode manuel des contrôleurs;
- les fonctions de verrouillage de la duplication du BPCS;
- les alarmes BPCS des diagnostics du système de sécurité;
- les alarmes BPCS affectées en tant que couches de sécurité dans le LOPA.

Un exemple de procédure de contrôle de verrouillage du réacteur R1 est présenté ci-dessous:

NOMEX® est cité dans la procédure ci-dessous. [1]

[1] NOMEX® est un exemple de produit approprié disponible sur le marché. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que la l'IEC approuve our recommande l'emploi exclusif du produit ainsi désigné.

Titre:	Réacteur R1 Procédures de vérification de verrouillage	Préparé par: Révisé par:	DATE: DATE:
Région:		Approbation technique:	DATE:
PSM critique:	Oui	Approuvé par:	DATE:

☐ COPIE DE FICHIER ☐ COPIE TERRAIN

Résumé de l'essai

A. Capteurs/commutateurs soumis à l'essai:

Etiquette	Zéro	Portée	Unités	Normal	Normal mA	Alarme	Alarme mA	Déclencher	Déclencher mA	Tolérance
100PT	0	200	PSIG	100	12	115	13,2	125	14	± 2 PSIG
100PT1	0	200	PSIG	100	12	115	13,2	125	14	± 2 PSIG
100TT	0	250	Deg F	125	12	180	15,52	200	16,8	± 2 Deg F
200PT	0	20	PSIG	2,5	6	5	8	10	12	± 1 PSIG

B. Appareils de commande terminaux soumis à l'essai:

Etiquette	Position
100PV	Ouvert
100PV1	Ouvert

C. Résultats de l'essai:
Vérification une:

_____ Tous les appareils ont réussi l'essai.

_____ Des actions correctrices ont été exigées pour réussir l'essai.

Date à laquelle la procédure de vérification a été terminée: _____.

D. Sécurité et santé

- Equipement de protection spécial comme exigé par la procédure de zone (par exemple, lunettes de sécurité, casque, chaussures de sécurité)

E. Equipement de protection spécial

- NOMEX® comme exigé pour la protection flash.

F. Conditions précédant l'essai et verrouillage

- Il convient de dé-inventorier et verrouiller le réacteur, en utilisant une procédure de verrouillage, étiquetage et essai.
- Il convient de désactiver les systèmes d'extinction d'urgence.

- Il convient de placer des barrières où elles sont exigées.
- Il convient de terminer la communication (par exemple, signes, mémos, ordonnancement, planification).

G. Permis

- Permis de rupture de ligne pour chaque transmetteur.

H. Equipement spécial

- Un simulateur en cours.
- Un communicateur portatif du transmetteur.

I. Epreuves de référence

- Numéro de P&ID:
- Numéro de feuille logique:
- Numéro de dessin E&I:

J. Main-d'œuvre

- Opérateur de salle de commande qualifié
- Techniciens d'instruments et électriques qualifiés

Chaque procédure d'essai de verrouillage a ses propres considérations de sécurité. Il convient de modifier le texte suivant pour satisfaire aux exigences d'application spécifiques.

Etalonnage et inspection

A. Instrument étalonné ou étalonnage vérifié.

Instruments étalonnés selon les procédures de maintenance.

Etiquette	Description	Déclencher	Tel quel	Initiales	Date
100PT	Pression du réacteur au nord				
100PT1	Pression du réacteur au sud				
100TT	Température du réacteur				
200PT	Pression du sceau du réacteur				

B. Instruments et appareils de commande terminaux inspectés:

Installations de terrain inspectées pour des problèmes de connexions de câblage, tubage, filtres, jauges, solénoïdes, isolation et processus.

Etiquette	Description	Tel quel	En l'état	Initiales	Date
100PT	Pression du réacteur au nord				
100PT1	Pression du réacteur au sud				
100TT	Température du réacteur				
200PT	Pression du sceau du réacteur				
100PV	Vanne d'évent du réacteur au nord				
100PV1	Vanne d'évent du réacteur au sud				

Procédures d'essai de verrouillage

Heure à laquelle la procédure de vérification a commencé: _____Date: _____

Procédure à effectuer par:

Titre	Signature	Date
Opérateur de salle de commande		
Technicien E&I		
Technicien E&I		
Chef d'équipe d'opération		

Configuration générale de la procédure de vérification du verrouillage

Technicien E&I:

A. Simuler les conditions de fonctionnement normal.

_____ Supprimer tous les verrouillages BPCS sur 100PV et 100PV1.
_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 1.

Procédure de vérification de verrouillage pour le PB d'extinction du SIS du réacteur

Fréquence d'essai:	6 mois
Objectif de l'essai:	Un arrêt du système de sécurité du réacteur manuel ouvre les vannes de commande de la pression du réacteur 100PV et 100PV1. Soumettre aussi à l'essai les diagnostics d'appareil de commande terminaux.

A. Supprimer le verrouillage. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 n'est pas allumé.

B. Simuler des conditions normales. (Opérateur de salle de commande)

_____ Vérifier que l'alarme de diagnostic fermé de la vanne de l'évent du réacteur EA18 n'est pas allumée.

_____ Depuis le BPCS, fermer la vanne de l'évent du réacteur 100PV.

_____ Depuis le BPCS, fermer la vanne de l'évent du réacteur 100PV1.

_____ Mettre l'ensemble des contrôleurs du BPCS en position de fonctionnement normal.

_____ Mettre l'ensemble des contrôleurs du BPCS en mode de fonctionnement normal.

_____ Mettre l'ensemble des moteurs et des vannes du BPCS en mode normal.

C. Vérifier sur le terrain les conditions normales. (Opérateur de terrain)

_____ Vérifier sur le terrain que la vanne de l'évent du réacteur 100PV est fermée.

_____ Vérifier sur le terrain que la vanne de l'évent du réacteur 100PV1 est fermée.

D. Soumettre l'alarme de diagnostic à l'essai. (Technicien E&I)

_____ Déconnecter le signal du commutateur de position fermée de la vanne de l'évent du réacteur 100LSC.

_____ Vérifier que l'alarme de diagnostic fermé de la vanne de l'évent du réacteur EA18 est allumée.

_____ Reconnecter le signal du commutateur de position fermée de la vanne de l'évent du réacteur 100LSC.

_____ Vérifier que l'alarme de diagnostic fermé de la vanne de l'évent du réacteur EA18 n'est pas allumée.

_____ Déconnecter le signal du commutateur de position fermée de la vanne de l'évent du réacteur 100LSC1.

_____ Vérifier que l'alarme de diagnostic fermé de la vanne de l'évent du réacteur EA18 est allumée.

_____ Reconnecter le signal du commutateur de position fermée de la vanne de l'évent du réacteur 100LSC1.

_____ Vérifier que l'alarme de diagnostic fermé de la vanne de l'évent du réacteur EA18 n'est pas allumée.

E. Soumettre le verrouillage à l'essai. (Opérateur de salle de commande)

_____ Eteindre le système de sécurité du réacteur en appuyant sur le bouton-poussoir d'arrêt 500 PB.

F. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 n'est pas allumé.

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de diagnostic ouvert de la vanne de l'évent du réacteur EA17 n'est pas allumée.

_____ Depuis le BPCS, vérifier que la vanne de l'évent du réacteur 100PV est ouverte.

_____ Depuis le BPCS, vérifier que la vanne de l'évent du réacteur 100PV1 est ouverte.

_____ Vérifier que tous les contrôleurs BPCS sont configurés sur une position de sécurité.

_____ Vérifier que tous les contrôleurs BPCS sont configurés sur un mode sûr.

_____ Vérifier que l'ensemble des moteurs et des vannes du BPCS sont en mode sûr.

G. Vérifier sur le terrain les conditions normales. (Opérateur de terrain)

_____ Vérifier sur le terrain que la vanne de l'évent du réacteur 100PV est ouverte.

_____ Vérifier sur le terrain que la vanne de l'évent du réacteur 100PV1 est ouverte.

H. Soumettre l'alarme de diagnostic à l'essai. (Technicien E&I)

_____ Déconnecter le signal du commutateur de position de la vanne de l'évent du réacteur 100LSO.

_____ Vérifier que l'alarme de diagnostic ouvert de la vanne de l'évent du réacteur EA17 est allumée.

_____ Reconnecter le signal du commutateur de position de la vanne de l'évent du réacteur 100LSO.

_____ Vérifier que l'alarme de diagnostic ouvert de la vanne de l'évent du réacteur EA17 n'est pas allumée.

_____ Déconnecter le signal du commutateur de position de la vanne de l'évent du réacteur 100LSO1.

_____ Vérifier que l'alarme de diagnostic ouvert de la vanne de l'évent du réacteur EA17 est allumée.

_____ Reconnecter le signal du commutateur de position de la vanne de l'évent du réacteur 100LSO1.

_____ Vérifier que l'alarme de diagnostic ouvert de la vanne de l'évent du réacteur EA17 n'est pas allumée.

I. Supprimer le verrouillage. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 n'est pas allumé.

_____ Vérifier que l'alarme de diagnostic ouvert de la vanne de l'évent du réacteur EA17 n'est pas allumée.

J. Vérifier sur le terrain les conditions de réinitialisation. (Opérateur de terrain)

_____ Vérifier sur le terrain que la vanne de l'évent du réacteur 100PV est ouverte.

_____ Vérifier sur le terrain que la vanne de l'évent du réacteur 100PV1 est ouverte.

K. Vérifier les conditions de réinitialisation. (Opérateur de salle de commande)

_____ Depuis le BPCS, vérifier que la vanne de l'évent du réacteur 100PV est ouverte.

_____ Depuis le BPCS, vérifier que la vanne de l'évent du réacteur 100PV1 est ouverte.

_____ Vérifier que tous les contrôleurs BPCS sont configurés sur une position de sécurité.

_____ Vérifier que tous les contrôleurs BPCS sont configurés sur un mode sûr.

_____ Vérifier que l'ensemble des moteurs et des vannes du BPCS sont en mode sûr.

Procédure de vérification de verrouillage pour la pression du réacteur, 100PT

SIF	S1, S2
Nom de l'événement:	Surpression du réacteur
Classification de l'événement:	SIL 2
Fréquence d'essai:	6 mois
Objectif de l'essai:	Une pression élevée du réacteur ouvre les vannes de commande de la pression du réacteur 100PV et 100PV1.

A. Exécuter les diagnostics (Technicien E&I)

_____ Connecter au transmetteur de pression du réacteur 100PT en utilisant un communicateur portatif et exécuter les diagnostics du transmetteur.

_____ Vérifier qu'il n'y a pas d'erreur de diagnostic.

B. Simuler des conditions normales. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

C. Soumettre le verrouillage à l'essai. (Technicien E&I)

_____ Déconnecter le transmetteur de pression du réacteur 100PT du système de sécurité.

D. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

E. Simuler les conditions normales. (Technicien E&I)

_____ Connecter un simulateur au transmetteur de pression du réacteur 100PT.

_____ Simuler 100 PSI (12 mA) sur le transmetteur de pression du réacteur 100PT.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 2.

F. Simuler les conditions normales. (Opérateur de salle de commande)

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 n'est pas allumée.

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

G. Soumettre le verrouillage à l'essai (Technicien E&I)

_____ Augmenter lentement le signal simulé sur le transmetteur de pression du réacteur de 100PT à 125 PSI (14 mA).

_____ Enregistrer le réglage auquel le verrouillage s'est déclenché: _____

H. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

I. Supprimer le verrouillage. (Technicien E&I)

_____ Diminuer lentement le signal simulé sur le transmetteur de pression du réacteur de 100PT à 100 PSI (12 mA).

J. Vérifier les conditions de réinitialisation. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 n'est pas allumée.

K. Revenir aux conditions courantes. (Technicien E&I)

_____ Retirer le simulateur du transmetteur de pression du réacteur 100PT.

_____ Reconnecter le transmetteur de pression du réacteur 100PT au système de sécurité.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 2.

L. Vérifier les conditions courantes. (Opérateur de salle de commande)

_____ Vérifier que le transmetteur de pression du réacteur 100PT affiche la pression du réacteur réelle.

Procédure de vérification de verrouillage pour la pression du réacteur, 100PT1

SIF	S2
Nom de l'événement:	Surpression du réacteur
Classification de l'événement:	SIL 2
Fréquence d'essai:	6 mois
Objectif de l'essai:	Une pression élevée du réacteur ouvre les vannes de commande de la pression du réacteur 100PV et 100PV1.

A. Exécuter les diagnostics (Technicien E&I)

_____ Connecter au transmetteur de pression du réacteur 100PT1 en utilisant un communicateur portatif et exécuter les diagnostics du transmetteur.

_____ Vérifier l'absence d'erreur de diagnostic.

B. Simuler des conditions normales. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

C. Soumettre le verrouillage à l'essai. (Technicien E&I)

_____ Déconnecter le transmetteur de pression du réacteur 100PT1 du système de sécurité.

D. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

E. Simuler les conditions normales. (Technicien E&I)

_____ Connecter un simulateur au transmetteur de pression du réacteur 100PT1.

_____ Simuler 100 PSI (12 mA) sur le transmetteur de pression du réacteur 100PT1.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 3.

F. Simuler les conditions normales. (Opérateur de salle de commande)

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 n'est pas allumée.

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

G. Soumettre le verrouillage à l'essai (Technicien E&I)

_____ Augmenter lentement le signal simulé sur le transmetteur de pression du réacteur de 100PT1 à 125 PSI (14 mA).

_____ Enregistrer le réglage auquel le verrouillage s'est déclenché: _____

H. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

F. Supprimer le verrouillage. (Technicien E&I)

_____ Diminuer lentement le signal simulé sur le transmetteur de pression du réacteur de 100PT1 à 100 PSI (12 mA).

J. Vérifier les conditions de réinitialisation. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 n'est pas allumée.

K. Revenir aux conditions courantes. (Technicien E&I)

_____ Retirer le simulateur du transmetteur de pression du réacteur 100PT1.

_____ Reconnecter le transmetteur de pression du réacteur 100PT1 au système de sécurité.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 3.

L. Vérifier les conditions courantes. (Opérateur de salle de commande)

_____ Vérifier que le transmetteur de pression du réacteur 100PT1 affiche la pression du réacteur réelle.

Procédure de vérification de verrouillage pour la température du réacteur, 100TT

SIF	S1
Nom de l'événement:	Surpression du réacteur
Classification de l'événement:	SIL 2
Fréquence d'essai:	12 mois
Objectif de l'essai:	Une température élevée du réacteur ouvre les vannes de commande de la pression du réacteur 100PV et 100PV1.

A. Exécuter les diagnostics (Technicien E&I)

_____ Connecter au transmetteur de pression du réacteur 100TT en utilisant un communicateur portatif et exécuter les diagnostics du transmetteur.

_____ Vérifier l'absence d'erreur de diagnostic.

B. Simuler des conditions normales. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

C. Soumettre le verrouillage à l'essai. (Technicien E&I)

_____ Déconnecter le transmetteur de température du réacteur 100TT du système de sécurité.

D. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

E. Simuler les conditions normales. (Technicien E&I)

_____ Connecter un simulateur au transmetteur de température du réacteur 100TT.

_____ Simuler 125 °F (12 mA) sur le transmetteur de température du réacteur 100TT.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 4.

F. Simuler les conditions normales. (Opérateur de salle de commande)

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 n'est pas allumée.

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

G. Soumettre le verrouillage à l'essai (Technicien E&I)

_____ Augmenter lentement le signal simulé sur le transmetteur de température du réacteur de 100TT à 200 °F (16,8 mA).

_____ Enregistrer le réglage auquel le verrouillage s'est déclenché: _____

H. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

F. Supprimer le verrouillage. (Technicien E&I)

_____ Diminuer lentement le signal simulé sur le transmetteur de température du réacteur de 100TT à 125 °F (12 mA).

J. Vérifier les conditions de réinitialisation. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 n'est pas allumée.

K. Revenir aux conditions courantes. (Technicien E&I)

_____ Retirer le simulateur du transmetteur de température du réacteur 100TT.

_____ Reconnecter le transmetteur de température du réacteur 100TT au système de sécurité.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 4.

L. Vérifier les conditions courantes. (Opérateur de salle de commande)

_____ Vérifier que le transmetteur de température du réacteur 100TT affiche la température du réacteur réelle.

Procédure de vérification de verrouillage pour la pression du sceau du réacteur, 200PT

SIF	S3
Nom de l'événement:	Surpression du sceau du réacteur
Classification de l'événement:	SIL 2
Fréquence d'essai:	6 mois
Objectif de l'essai:	Une pression élevée du sceau ouvre les vannes de commande de la pression du réacteur 100PV et 100PV1.

A. Exécuter les diagnostics (Technicien E&I)

_____ Connecter au transmetteur de pression du réacteur 200PT en utilisant un communicateur portatif et exécuter les diagnostics du transmetteur.

_____ Vérifier l'absence d'erreur de diagnostic.

B. Simuler des conditions normales. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

C. Soumettre le verrouillage à l'essai. (Technicien E&I)

_____ Déconnecter le transmetteur de pression du réacteur 200PT du système de sécurité.

D. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

E. Simuler les conditions normales. (Technicien E&I)

_____ Connecter un simulateur au transmetteur de pression du sceau du réacteur 200PT.

_____ Simuler 2,5 PSI (6 mA) sur le transmetteur de pression du sceau du réacteur 200PT.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 5.

F. Simuler les conditions normales. (Opérateur de salle de commande)

_____ Vérifier que l'alarme de diagnostic du transmetteur du système de sécurité du réacteur EA014 n'est pas allumée.

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

G. Soumettre le verrouillage à l'essai (Technicien E&I)

_____ Augmenter lentement le signal simulé sur le transmetteur de pression du sceau du réacteur de 200PT à 10 PSI (12 mA).

_____ Enregistrer le réglage auquel le verrouillage s'est déclenché: _____

H. Vérifier les actions de verrouillage. (Opérateur de salle de commande)

_____ Vérifier que le voyant inactif du système de sécurité du réacteur EA011 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 est allumée.

_____ Vérifier que le système de sécurité du réacteur ne se réinitialisera pas quand le bouton de réinitialisation PB000 est activé.

F. Supprimer le verrouillage. (Technicien E&I)

_____ Diminuer lentement le signal simulé sur le transmetteur de pression du sceau du réacteur de 200PT à 2,5 PSI (6 mA).

J. Vérifier les conditions de réinitialisation. (Opérateur de salle de commande)

_____ Pour réinitialiser le système de sécurité du réacteur, appuyer sur le bouton de réinitialisation PB000.

_____ Vérifier que le voyant actif du système de sécurité du réacteur EA010 est allumé.

_____ Vérifier que l'alarme de déclenchement du transmetteur du système de sécurité du réacteur EA012 n'est pas allumée.

K. Revenir aux conditions courantes. (Technicien E&I)

_____ Retirer le simulateur du transmetteur de pression du sceau du réacteur 200PT.

_____ Reconnecter le transmetteur de pression du sceau du réacteur 200PT au système de sécurité.

_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 5.

L. Vérifier les conditions courantes. (Opérateur de salle de commande)

_____ Vérifier que le transmetteur de pression du sceau du réacteur 200PT affiche la pression du sceau du réacteur réelle.

Fin générale de la procédure de vérification du verrouillage

Technicien E&I:

A. Remettre tous les autres verrouillages en service.

_____ Remettre en service tous les verrouillages BPCS sur 100PV et 100PV1.
_____ Mettre à jour la feuille de contrôle de dérivation pour la dérivation n° 1

Essai et inspection terminés par:

Titre	Signature	Date
Opérateur de salle de commande		
Opérateur de salle de commande		
Technicien E&I		
Technicien E&I		
Chef d'équipe d'opération		

Heure à laquelle la procédure de vérification a été terminée: _____Date: _____

Documentation et inspection post-essai

A. Vérifier que tous les changements de la procédure ont été revus avec la direction et ont été approuvés.
B. Si un appareil a échoué, quelle action correctrice a été exigée:

_____
_____
_____
_____
_____
_____

Ajouter les signatures sur la copie du fichier et sur le fichier avec les enregistrements d'essai du système de sécurité. Le Tableau F.19 présente la manière dont une feuille de contrôle de dérivation/simulation de la procédure de verrouillage peut être documentée.

Tableau F.19 – Feuille de contrôle de dérivation/simulation de la procédure de vérification de verrouillage

N° de dérivation	Boucle	Emplacement	Méthode	Etape installée	Initiales	Etape retirée	Initiales
1	DCS	DCS	Drapeau	1.1		7.1	
2	100PT	Transmetteur	Simulateur	3.4		3.10	
3	100PT 1	Transmetteur	Simulateur	4.4		4.10	
4	100TT	Transmetteur	Simulateur	5.4		5.10	
5	200PT	Transmetteur	Simulateur	6.4		6.10	
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
18							
20							

F.29 Etape F.6: Fonctionnement et maintenance du SIS

Tableau F.20 – Cycle de vie de sécurité du SIS – Zone 6

Phase ou activité du cycle de vie de sécurité		Objectifs	Exigences Article ou paragraphe de l'IEC 61511-1:2016	Entrées	Sorties
IEC 61511-1:2016 Figure F.7, zone 6	Fonctionnement et maintenance du SIS	Assurer que la sécurité fonctionnelle du SIS est conservée pendant le fonctionnement et la maintenance	16	Exigences du SIS Conception du SIS Plan pour le fonctionnement et la maintenance du SIS	Résultats des activités de fonctionnement et de maintenance

La formation du personnel d'exploitation, de la maintenance et d'autres personnels de soutien au fonctionnement du BPCS et du SIS a été réalisée avant de mettre les systèmes en mode opérationnel et est mise à jour à chaque fois qu'un changement est effectué sur l'un des deux systèmes.

Les nouveaux éléments à prendre en compte concernant la formation du personnel d'exploitation et de maintenance du SIS comprennent:

- la terminologie (par exemple, SIS, SIF, PFD_{avg}, SIL, couche de protection);
- l'analyse de danger et de risque;
- l'architecture, par exemple, IHM (SIS et BPCS), interfaces du SIS (par exemple, lecture seule du lien BPCS);
- les exigences de documentation (par exemple, la fréquence des sollicitations placées sur les procédures/méthodes/techniques SIF/SIS, les essais périodiques et les inspections, les résultats d'essais, les identifiants d'équipement jusqu'au niveau de révision, les personnes/départements/organismes responsables);
- les procédures de dérivation;
- les essais de la fréquence pour SIF/SIS;
- la description fonctionnelle du SIS.

Un journal de déclenchement du SIS a été développé pour les opérations et la maintenance afin d'enregistrer les sollicitations et les défaillances du SIS. Voir le Tableau F.21 ci-dessous.

Des déclenchements parasites de la SIF sont inclus dans ce journal mais ne sont pas considérés en tant que sollicitations sur le SIS.

Tableau F.21 – Journal de déclenchement du SIS

Date	SIF	Sollicitation/Parasite	Cause du déclenchement	N° du rapport d'incident	Enregistré par
18/05/2008	S-2	Sollicitation	Erreur de l'opérateur – réacteur surchargé	Rapport d'incident sérieux n° 18	L. Soft
03/08/2008	S-3	Parasite	Défaillance du transmetteur 200PT	Aucune	J. Doe
28/02/2009	S-1	Sollicitation	Défaillance de la boucle de commande de refroidissement	Rapport d'incident sérieux n° 43	T. Rex

Un système de suivi a été mis en place pour identifier les problèmes récurrents avec les appareils du SIS lors de leur détection pendant les essais. Les résultats sont consignés tel que le montre le Tableau F.22 ci-dessous.

Tableau F.22 – Journal des défaillances de l'appareil du SIS

Date	Appareil	Défaillance en/hors sécurité	Description de la défaillance	Enregistré par
21/03/2007	100TT	Sûr	Pas étalonné	T. Rex
18/05/2008	100PV	Pas sûr	Sortie de vanne coincée – ne s'ouvre pas	L. Soft
03/08/2008	100PV	Pas sûr	Sortie de vanne coincée – ne s'ouvre pas	J. Doe
28/02/2009	100PV	Pas sûr	Sortie de vanne coincée – ne s'ouvre pas	T. Rex

Comme indiqué au Tableau F.20, la valve d'évent 100PV est souvent confrontée à des problèmes. Après la troisième défaillance, une analyse des causes de défaillances initiales a

déterminé que la valve était défectueuse. La valve a été remplacée et aucune défaillance n'a été constatée depuis.

Une documentation de la logique de commande et de sécurité actuellement mise en œuvre dans le BPCS et le SIS est disponible à tout moment. Tout changement est documenté au moment où il est mis en œuvre. Une version papier de la documentation, qui décrit entièrement les systèmes et leurs fonctions, sert de référence.

Un programme d'audit exigeant l'examen de la documentation du système comme partie intégrante du processus cyclique de revue du danger a été mis en œuvre. Un rapport consignant les résultats de l'audit est publié et toutes les recommandations de l'audit sont signalées pour être suivies (trimestriellement) jusqu'à la mise en place complète. L'audit inclut:

- la revue de tous les changements apportés depuis la dernière revue, et la vérification du statut de la documentation correcte;
- la revue de tous les problèmes liés à l'équipement ou la logique associés au SIS depuis la dernière revue, afin de vérifier si des problèmes qui pourraient dégrader à l'avenir les fonctions du système se développent;
- la revue de la compréhension des fonctions et de l'exploitation du système par le personnel d'exploitation;
- la revue du journal de sollicitation du SIS pour valider les hypothèses du taux de sollicitation utilisé dans le LOPA;
- la revue des résultats de l'essai de la SIF pour valider les hypothèses du taux de défaillances de l'appareil utilisé dans le calcul de la PFD_{avg}.

La liste ci-après présente le support documentaire qui sera inclus dans l'audit. Cette documentation sera à la disposition du personnel d'exploitation et tenue à jour.

– la documentation relative à l'analyse de danger et de risque (simulations (Tableau I.4), HAZOP (Tableau F.5));
– le classement du risque tolérable utilisé (c'est-à-dire le Tableau F.8);
– la documentation relative à l'affectation de risque aux couches de sécurité – détermination du SIL de chaque SIF (LOPA) (c'est-à-dire le Tableau F.9);
– les schémas P&I (c'est-à-dire la Figure F.3 et la Figure F.10);
– le schéma du système SIF (c'est-à-dire la Figure F.12);
– l'impression du programme d'application (diagrammes à contacts) (c'est-à-dire la Figure F.11 (feuilles 1 à 5));
– manuels de sécurité;
– documentation du matériel du SIS/du programme d'application/de l'installation/de la maintenance (Tableau F.20, zone 6, par exemple);
– documentation de la capabilité systématique;
– calculs de vérification du SIL (c'est-à-dire la PFD_{avg}) pour la SIF, y compris les schémas architecturaux (c'est-à-dire la Figure F.4, la Figure F.5, la Figure F.6, la Figure F.7, la Figure F.8, et la Figure F.9);
– procédure d'essai pour chaque SIF;
– sollicitations de processus sur chaque SIF (c'est-à-dire le Tableau F.12);
– données de défaillance pour les appareils SIF (c'est-à-dire Tableau F.13).

Des essais et une inspection périodique du SIS sont menés à la fréquence spécifiée par les calculs de PFD_{avg} (c'est-à-dire, tous les six mois). Les couches de protection identifiées dans le LOPA sont également soumises à l'essai à la même fréquence, tous les six mois.

Les opérations conservent les enregistrements qui démontrent que les essais périodiques et les inspections ont été réalisés comme cela est exigé. Il convient que ces enregistrements incluent au moins les informations suivantes:

a) la description des essais et des inspections effectuées;

b) les dates des essais et des inspections;

c) le nom des personnes qui ont effectué les essais et les inspections;

d) le numéro de série ou tout autre identifiant unique du système soumis à l'essai (par exemple, numéro de ligne, numéro d'étiquette, numéro d'équipement et numéro de la SIF);

e) les résultats des essais et de l'inspection (par exemple, conditions "tel quel" et "en l'état");

f) le programme d'application actuellement en fonctionnement dans le solveur logique du SIS.

F.30 Etape F.7: Modification du SIS

Tableau F.23 – Cycle de vie de sécurité du SIS – Zone 7

Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigences** **Article ou paragraphe de l'IEC 61511-1: —**	**Entrées**	**Sorties**
Figure F.2, zone 7	Modification du SIS	Faire des corrections, des améliorations ou des adaptations au SIS, en s'assurant que le SIL exigé est obtenu et maintenu	17	Exigences concernant la sécurité du SIS révisées	Résultats des modifications du SIS

Le Tableau F.23 donne les objectifs, les entrées, les sorties et les références aux articles et paragraphes connexes pour la modification du SIS.

L'installation a une gestion fonctionnelle du processus de changements en place, conformément à l'OSHA 29 CFR 1910.119. Toute modification du SIS exigera une nouvelle entrée dans le cycle de vie de sécurité du SIS, à l'étape appropriée.

F.31 Etape F.8: Déclassement du SIS

Les principaux appareils de déclassement sont décrits au Tableau F.24.

Tableau F.24 – Cycle de vie de sécurité d'un SIS – Zone 8

Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigences** **Article ou paragraphe de l'IEC 61511-1:2016**	**Entrées**	**Sorties**
IEC 61511-1:2016 Figure F.2, zone 8	Déclassement	Assurer la revue, l'organisation sectorielle ad hoc, mais aussi assurer que la SIF reste appropriée	18	Exigences de sécurité et informations de processus conformes à la construction	SIF déclarée hors service

L'installation a de l'expérience en matière de déclassement des processus dangereux et comprend la nécessité de procéder à une analyse de danger et de risque, ainsi qu'à une analyse technique suivie d'une planification de déclassement. Une fois terminés, la (ou les) autorisation(s) indiquée(s) et l'ordonnancement précèdent le début du déclassement.

F.32 Etape F.9: Vérification du SIS

La vérification (Tableau F.25) est une opération menée tout au long du cycle de vie du SIS.

Tableau F.25 – Cycle de vie de sécurité du SIS – Zone 9

Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigence** **Article ou paragraphe de l'IEC 61511-1:2016**	**Entrées**	**Sorties**
IEC 61511-1:2016 Figure F.2, zone 9	Vérification du SIS	Soumettre à l'essai et évaluer les sorties d'une phase donnée, pour assurer la véracité et la cohérence par rapport aux produits et aux normes donnés comme entrées à cette phase	7, 12.5	Plan de vérification du SIS, pour chaque phase	Résultats de la vérification du SIS, pour chaque phase

Le personnel d'ingénierie, d'opérations et de maintenance coordonne la planification de la vérification afin que chaque service puisse atteindre ses objectifs.

L'ingénierie a utilisé la vérification pour garantir:

- le matériel, le programme d'application et la conception du système sont corrects et cohérents avec la SRS;
- les opérations sont impliquées dans une sélection d'activités de vérification (le développement du programme d'application, les affichages de l'IHM, par exemple) dès les prémices, de telle sorte que l'approbation finale n'apporte aucune surprise (retouches importantes, délais, par exemple);
- la maintenance a l'occasion pratique de gérer des appareils/sous-systèmes/systèmes du SIS, afin de se familiariser avec la documentation, la localisation du matériel, les fonctionnalités du programme d'application, tout en facilitant la vérification.

Les opérations ont utilisé les activités de vérification:

- pour s'assurer que le projet est conforme à la planification et dans les délais indiqués;
- tel que stipulé dans les instructions d'exploitation consignées par écrit.

La maintenance a utilisé la vérification pour:

- habituer le personnel au processus;
- identifier les zones où de nouvelles formations ou de nouveaux outils sont exigés;
- identifier les procédures d'installations non conformes aux pratiques de l'installation;
- développer les procédures de maintenance.

F.33 Etape F.10: Gestion de la sécurité fonctionnelle et de la FSA du SIS

Tableau F.26 – Cycle de vie de sécurité du SIS – Zone 10

Phase ou activité du cycle de vie de sécurité		**Objectifs**	**Exigence** **Article ou paragraphe de l'IEC 61511-1: —**	**Entrées**	**Sorties**
Figure F.2, zone 10	Gestion de la sécurité fonctionnelle et de la FSA du SIS	Pour s'assurer que toutes les étapes du cycle de vie de sécurité du SIS sont prises en compte de manière adéquate, et pour enquêter et parvenir à une conclusion sur la sécurité fonctionnelle obtenue par le SIS	5	Planification pour la FSA du SIS Exigence concernant la sécurité du SIS	Résultats de la FSA du SIS

F.34 Gestion de la sécurité fonctionnelle

F.34.1 Généralités

La gestion de la sécurité fonctionnelle (Tableau F.26) dans cette entreprise est mise en œuvre dans le cadre du programme de gestion de la sécurité des processus (PSM). Les normes extensives de l'entreprise traitent tous les aspects du PSM tels que l'intégrité mécanique, l'assurance qualité et la formation. Ces normes exigent que la mise en œuvre d'un nouveau projet dans les usines de l'entreprise soit conforme aux exigences de l'IEC 61511, le cas échéant.

F.34.2 Compétences du personnel

La gestion doit s'assurer que les personnes responsables de mener et de revoir chacune des activités du cycle de vie de sécurité du SIS soient compétentes dans leur domaine d'opération. Pour ce faire, mettre en œuvre l'approche présentée dans l'IEC 61511-1:2016 , 12.5.2. Les éléments de qualification suivants ont été passés en revue:

- expérience et formation;
- connaissance d'ingénierie du processus;
- connaissance d'ingénierie de la technologie SIS;
- connaissance d'ingénierie de sécurité (par exemple, les normes de sécurité fonctionnelle de l'entreprise);
- compétences en gestion et en leadership;
- la compréhension de la conséquence potentielle d'un événement.

De plus, le personnel d'exploitation et de la maintenance a été formé sur les dangers associés au processus, ainsi que sur le fonctionnement du BPCS et du SIS avant le démarrage.

F.35 Evaluation de la sécurité fonctionnelle

Une FSA (également appelée revue de sécurité préalable au démarrage) a été menée avant le démarrage du processus. Voir l'IEC 61511-1:2016 5.2.6.1. L'objectif général de la FSA était de s'assurer que le SIS opérerait conformément aux exigences définies par le SRS afin que le SIS puisse passer en toute sécurité de la phase d'installation à la phase de production.

La FSA n'est pas lancée avant que toutes les activités de vérification soient terminées et approuvées.

Une FSA continue sera menée périodiquement, conformément à la description donnée à l'Article F.29, Etape 6.

Annexe G
(informative)

Lignes directrices relatives au développement de pratiques de programmation d'application

G.1 Objectif de ces lignes directrices

Dans le secteur des industries de transformation, le choix des appareils programmables électroniques (voir l'IEC 61511-1:2016 , 11.5 et 11.6) s'appuiera sur un appareil conforme à l'IEC 61508 ("automate de sécurité", par exemple) auquel sera associé un manuel de sécurité ou qui sera sélectionné sur la base d'une épreuve par une utilisation préalable.

La présente Annexe G donne des exemples de considérations (appelées "attributs génériques de programmation sûre d'applications") qu'il convient de satisfaire selon le cas, soit dans le manuel de sécurité fourni par le fabricant soit en tant que manuel de programmation spécifique au projet. Il s'agit de maintenir la conception du programme d'application dans le domaine d'application de la présente norme et de contribuer à obtenir l'intégrité systématique de sécurité prévue du programme d'application.

NOTE Auparavant, la présente annexe était l'Annexe A.

G.2 Attributs génériques de programmation sûre d'applications

La présente annexe décrit les attributs génériques ou indépendants du langage d'une programmation sûre d'applications. Les attributs ont été définis dans un cadre hiérarchique à trois niveaux. Les quatre attributs de niveau supérieur sont:

Fiabilité: La fiabilité représente les performances prévisibles et constantes du programme d'application dans les conditions spécifiées dans la base de conception. Cet attribut de niveau supérieur est important pour la sécurité, car il réduit la probabilité d'erreurs susceptibles de provoquer des dysfonctionnements dans le programme d'application lors de la mise en œuvre.

Robustesse: La robustesse est la capacité du programme d'application à fonctionner de manière acceptable en cas d'événements ou de conditions du processus anormaux. Cet attribut de niveau supérieur est important pour la sécurité, car il améliore les capacités du programme d'application à prendre en compte les conditions d'exception, à récupérer suite à des défaillances internes et à éviter la propagation des erreurs issues de circonstances inhabituelles (elles peuvent ne pas avoir été toutes bien définies dans la base de conception).

Traçabilité: La traçabilité fait référence à la faisabilité de la revue et de l'identification des processus de développement et de l'origine de la bibliothèque et du programme d'application, c'est-à-dire qu'il peut être montré que le programme d'application fourni est le produit d'un processus de mise en œuvre défini et discipliné. La traçabilité inclut également le fait de pouvoir associer le programme d'application à des documents de conception de niveau supérieur. Cet attribut de niveau supérieur est important pour la sécurité, car il facilite la vérification, la validation et d'autres aspects de l'assurance qualité du programme d'application.

Maintenabilité: La maintenabilité est le moyen par lequel le programme d'application réduit la probabilité d'introduire des erreurs lors des changements apportés après la mise en service. Cet attribut de niveau supérieur est important pour la sécurité, car il réduit la probabilité de mauvais fonctionnement suite à la présence d'erreurs lors de la maintenance adaptative, corrective ou perfective du programme d'application.

G.3 Fiabilité

G.3.1 Généralités

Dans le contexte du programme d'application, la fiabilité est (1) la probabilité d'une exécution réussie sur un intervalle de temps défini et dans des conditions définies ou (2) la probabilité d'une exécution réussie sur sollicitation. Le fait que le programme d'application s'exécute jusqu'à son terme est le résultat de son bon comportement par rapport à la mémoire du système et à la logique du programme d'application. Le fait que le programme d'application produise des sorties en respectant le temps de réponse requis dépend de la manière dont l'automaticien comprend les constructions du langage et les caractéristiques de l'environnement d'exécution. Les attributs intermédiaires de fiabilité définis sont donc:

- la prévisibilité de l'utilisation de la mémoire: Il y a une forte probabilité que le programme d'application ne soit pas à l'origine de l'accès du solveur logique à des emplacements de mémoire non prévus ou non admis;
- la prévisibilité du flux de contrôle: Il y a une forte probabilité que le solveur logique exécute les instructions selon les séquences prévues par le programmeur;
- la prévisibilité du planning: Il y a une forte probabilité que le programme d'application qui s'exécute dans l'environnement d'exécution défini satisfasse aux contraintes de temps de réponse et de capacité; la prévisibilité du résultat mathématique ou logique: il y a une forte probabilité que le programme d'application qui s'exécute dans l'environnement d'exécution défini donne le résultat mathématique ou logique attendu par l'automaticien.

G.3.2 Prévisibilité de l'utilisation de la mémoire

G.3.2.1 Réduction de l'allocation dynamique de mémoire

L'allocation dynamique de mémoire est utilisée dans les programmes d'application pour revendiquer (allouer) temporairement de la mémoire, si nécessaire, pendant l'exécution et pour libérer la mémoire (également pendant l'exécution) pour d'autres utilisations quand elle n'est plus nécessaire. Le problème pour la sécurité est que, quand la mémoire est allouée de manière dynamique dans un système en temps réel, le programme d'application peut ensuite ne pas en libérer tout ou partie. Cela peut se produire car:

- le programme d'application s'alloue de la mémoire, mais ne la libère pas dans le cadre des chemins d'exécution normaux, ou
- un programme d'application qui s'est temporairement alloué de la mémoire est interrompu dans son exécution avant d'exécuter l'instruction de libération de la mémoire.

L'une ou l'autre de ces situations provoquera la perte finale de toute la mémoire utilisable et une perte de toutes les fonctions du système de sécurité. Il convient donc de réduire l'allocation dynamique de mémoire dans les systèmes numériques de sécurité.

Si l'allocation dynamique de mémoire est inévitable, l'IEC 61508-3 s'applique: il convient alors que le programme d'application inclue des dispositions pour garantir que:

- toute la mémoire allouée de manière dynamique pendant un cycle d'exécution spécifique est libérée à la fin de ce cycle; et
- la possibilité d'interruption de l'exécution entre le point où la mémoire est allouée de manière dynamique et le moment où elle est libérée est réduite (voire totalement éliminée). Il convient en outre que des dispositions dans le programme d'application détectent toute situation dans laquelle la mémoire allouée de manière dynamique n'a pas été libérée et de libérer cette mémoire.

La présente norme décourage donc l'utilisation de l'adressage indirect. L'IEC 61508-3 s'applique aux programmes d'application qui utilisent l'adressage indirect.

G.3.2.2 Réduction de la permutation et de la pagination de mémoire

La pagination de mémoire consiste à utiliser une partie de la mémoire pour stocker les zones de la mémoire principale utilisées de façon peu fréquente. Quand un programme d'application en fonctionnement a besoin de ces zones de données, le solveur logique les amène à être lus par une partie de la mémoire et à être rechargés dans une autre partie de la mémoire. Le processus de permutation consiste à utiliser une partie de la mémoire pour y stocker l'image mémoire d'un processus inactif dans son ensemble (y compris ses zones de données, par exemple la zone de pile et la zone tri).

Quand arrive le moment d'exécuter le processus, l'image est chargée depuis une partie de la mémoire dans la mémoire principale pour que le solveur logique l'utilise. En tout cas, l'utilisation spécifique de la mémoire et la portion du stockage utilisée pour la permutation sont indéterminées.

Ces capacités ne sont pas adaptées aux systèmes de sécurité, car ces indéterminations dans l'utilisation de la mémoire et du stockage peuvent, à leur tour, provoquer des retards significatifs dans le temps de réponse et utiliser des fonctions complexes déclenchées sur interruption pour réaliser les transferts de mémoire.

Si un solveur logique qui utilise la pagination de mémoire ou un processus de permutation est utilisé dans un SIS, il convient que cette fonctionnalité soit désactivée au niveau du solveur logique. Il convient que la mémoire principale soit suffisante pour l'ensemble des données et des programmes d'application. Si ces fonctionnalités n'ont pas été désactivées, l'IEC 61508-3 s'applique, et il convient que des dispositions dans le programme d'application garantissent la présence de toutes les fonctions critiques et de toutes leurs zones de données dans la mémoire principale pendant toute la période d'exécution. Ces dispositions dans le programme d'application incluent les appels du CPU ("brochage"), les directives de l'outil de programmation d'application et les processus du solveur logique.

G.3.3 Prévisibilité du flux de contrôle

G.3.3.1 Généralités

Le flux de contrôle définit l'ordre d'exécution des instructions d'un programme d'application. Un flux de contrôle prévisible permet une évaluation non ambiguë de la façon dont le programme s'exécutera dans des conditions spécifiées.

Les attributs de base liés sont:

- la maximisation de la structure;
- la réduction de la complexité du flux de contrôle;
- l'initialisation des variables avant utilisation;
- les points d'entrée et de sortie uniques pour les sous-programmes;
- la réduction des ambiguïtés de l'interface;
- l'utilisation du typage des données;
- la comptabilité de la précision;
- l'ordre de priorité des opérateurs arithmétiques, logiques et fonctionnels;
- la non-utilisation des fonctions ou procédures avec effets secondaires;
- la séparation de l'assignation et de l'évaluation;
- la gestion correcte de l'instrumentation du programme;
- le contrôle de la taille de la bibliothèque de classe;
- la réduction de l'utilisation des liaisons dynamiques;
- le contrôle de la surcharge d'opérateur.

G.3.3.2 Maximisation de la structure

Il convient d'éviter un programme d'application avec des instructions de contrôle d'exécution GOTO ou équivalent, provoquant un décalage non structuré de l'exécution d'une branche du programme d'application à une autre. Le problème de sécurité est que le comportement du temps d'exécution est difficile à tracer et à comprendre. Les instructions GOTO peuvent provoquer des effets secondaires indésirables, car elles interrompent l'exécution d'un segment particulier du programme d'application sans assurance que la suite de l'exécution satisfera à toutes les conditions à l'origine de l'entrée dans ce segment. Des normes qui découragent ou interdisent de telles pratiques de programmation d'application sont en place depuis plus de deux décennies. La structure est optimisée par l'élimination des instructions GOTO et l'utilisation d'un programme d'application structuré en blocs approprié. Les constructions case, if..then..else, do until et do while permettent la création de branches avec un retour défini et sans introduire l'incertitude du flux de contrôle associé aux instructions GOTO ou équivalentes.

G.3.3.3 Réduction de la complexité du flux de contrôle

Une indication de la complexité du flux de contrôle est le nombre de niveaux d'imbrication pour la création de branches ou de boucles. Une trop grande complexité rend plus difficile la prévision du flux d'un programme d'application et empêche la revue et la maintenance. Un problème de sécurité spécifique est que le flux de contrôle peut être imprévisible quand des combinaisons non anticipées de paramètres surviennent. Un niveau excessif d'imbrication peut généralement être évité par l'utilisation de fonctions ou de sous-routines à la place de branches en ligne. Il convient de définir une limite spécifique d'imbrication dans le cadre des lignes directrices du projet ou de la programmation organisationnelle afin de régler les problèmes de sécurité

L'IEC 61511 limite donc les couches dans l'architecture du programme d'application à 2 couches:

- types;
- verrouillages.

L'IEC 61508-3 s'applique aux programmes d'application dont le nombre de niveaux d'imbrication est supérieur à cette limite définie.

G.3.3.4 Initialisation des variables avant utilisation

Quand des variables ne sont pas initialisées à une valeur connue au début d'un cycle d'exécution, la sécurité est compromise, car elles peuvent contenir des valeurs "incorrectes" (des restes de l'utilisation préalable de cette zone de données). La prévisibilité de l'exécution exige que les zones de stockage de la mémoire mises de côté pour les données de processus soient définies sur des valeurs connues avant de pouvoir y accéder (qu'elles soient définies et utilisées). Le résultat spécifique de l'utilisation de valeurs initiales inconnues d'une variable dépend de la façon dont cette variable est utilisée dans le programme d'application. L'IEC 61508-3 s'applique aux programmes d'application qui utilisent des variables non initialisées.

G.3.3.5 Points d'entrée et de sortie uniques pour les sous-programmes

La présence de plusieurs points d'entrée et de sortie dans les sous-programmes introduit des incertitudes dans le flux de contrôle similaires à celles provoquées par les instructions GOTO.

La prévisibilité du flux d'exécution est améliorée en présence d'une seule entrée et d'une seule sortie pour chaque programme d'application. Parce que la prévisibilité du flux d'exécution est une caractéristique importante pour la sécurité, il n'est pas souhaitable d'avoir plusieurs points d'entrée et de sortie dans les sous-routines ou dans les fonctions, même si le langage les prend en charge. L'IEC 61508-3 s'applique aux programmes d'application comportant plusieurs points d'entrée et de sortie.

G.3.3.6 Réduction des ambiguïtés de l'interface

Les erreurs d'interface incluent les décalages dans les listes d'arguments lors de l'appel d'autres sous-programmes, de la communication avec d'autres tâches ou de la transmission de messages entre les objets. Un exemple d'erreur de ce type est l'inversion de l'ordre des arguments lors de l'appel d'une sous-routine. Une précédente recherche sur les défaillances du programme d'application a montré que cette catégorie d'erreurs est relativement significative. Des pratiques de programmation d'application qui peuvent réduire ou éliminer les erreurs d'interface incluent:

- l'organisation des arguments de manière à alterner des types de données différents (ce qui réduit le risque de placer deux arguments adjacents dans un ordre incorrect);
- l'utilisation de la notation nommée au lieu de la notation d'ordre ou de position pour les langages qui prennent en charge une telle notation;
- les essais de validité des arguments d'entrée au début du sous-programme.

Il convient que des préconditions et que des postconditions adéquates soient spécifiées pour les routines. Une précondition est une assurance que toutes les variables locales sont initialisées et que toutes les variables d'entrée satisfont aux vérifications de vraisemblance appropriées. Une postcondition est une assurance que toutes les variables de sortie satisfont aux vérifications de vraisemblance appropriées.

G.3.3.7 Utilisation du typage des données (structures de données)

L'utilisation de structures de données différentes de celles prévues pour un programme d'application peut provoquer des défaillances, lesquelles, si elles se produisent dans une condition d'exception, peuvent avoir des effets particulièrement néfastes sur la sécurité. Ce problème peut être résolu par la déclaration des types de données. A l'origine, le principal avantage de la déclaration des types de données était de permettre aux compilateurs de réserver la bonne quantité de mémoire. Le typage des données est toutefois utile pour améliorer la définition des interfaces, mais aussi pour augmenter la lisibilité (pour les revues), le temps de compilation et la vérification d'exécution. Ces utilisations à l'origine secondaires ont fini par devenir les principaux moteurs du typage des données et ont conduit à l'utilisation de typages forts, dans lesquels des déclarations supplémentaires, pour au moins une plage valide, sont exigées. Les problèmes de sécurité associés au typage des données incluent:

- La limitation de l'utilisation de types anonymes (par exemple, entier général ou virgule flottante sans limite supérieure et inférieure) dans des langages de type fort.
- La vérification que les limites des types de données ne sont pas excessivement contraintes afin que des messages d'erreur ou des exceptions parasites ne soient pas générés (ce qui est un problème dans des langages de type fort).
- La réduction des conversions de type et l'élimination des conversions de type implicites ou automatisées (dans des affectations et des opérations de pointeur, par exemple).
- Le fait d'éviter des opérations en mode mixte. Si de telles opérations sont nécessaires, il convient qu'elles soient clairement identifiées et décrites avec des commentaires prédominants dans le programme d'application.
- La vérification que les expressions qui impliquent des évaluations arithmétiques ou des opérations relationnelles ont un seul type de données, ou le bon jeu de types de données pour lequel les difficultés de conversion sont réduites.

La limitation de l'utilisation de références indirectes pour les exemples d'index de matrices, les pointeurs ou l'accès des objets à des situations dans lesquelles il n'y a aucune autre alternative raisonnable et l'exécution de la validation sur des données adressées indirectement avant la configuration ou l'utilisation pour garantir l'exactitude des emplacements accédés. Les pointeurs de type fort, les index de matrices et les types d'accès réduisent la possibilité de référencer des emplacements non valides.

G.3.4 Comptabilité de la précision

G.3.4.1 Généralités

Il convient que la mise en œuvre du programme d'application assure une précision et une pertinence adéquates pour l'application de sécurité prévue. Cela s'applique à la mesure des propriétés physiques et à l'arithmétique en virgule flottante dans le programme d'application. Des problèmes de sécurité surviennent quand la précision déclarée des variables en virgule flottante n'est pas prise en charge par l'analyse, en particulier quand de petites différences entre les grandes valeurs sont utilisées (par exemple, quand le taux de calcul du changement de la différence entre les valeurs en cours et précédentes, le calcul des écarts ou l'exécution d'opérations de filtrage telles que les moyennes mouvantes).

G.3.4.2 Ordre de priorité des opérateurs arithmétiques, logiques et fonctionnels

L'ordre par défaut de priorité des opérations arithmétiques, logiques et autres varie en fonction des langages. Les développeurs ou les réviseurs peuvent émettre des hypothèses de priorité incorrectes. Il convient donc d'utiliser les mécanismes pour garantir un énoncé clair de l'ordre d'évaluation des opérations.

G.3.4.3 Non-utilisation de fonctions ou procédures avec effets secondaires

Un effet secondaire est un changement apporté à une variable non renvoyée par cette fonction qui persiste une fois la fonction terminée. Cela inclut les changements aux fichiers, registres matériels, etc. Un exemple d'effet secondaire serait un changement dans une variable globale absente de la liste des paramètres. Les effets secondaires peuvent conduire à des problèmes avec les dépendances non planifiées et peuvent provoquer des bogues difficiles à identifier.

G.3.4.4 Séparation de l'assignation et de l'évaluation

Il convient que les énoncés d'affectation soient séparés des expressions d'évaluation. La séparation peut être enfreinte quand les sous-programmes sont utilisés dans le cadre de l'évaluation. Par exemple, une fonction de filtrage peut être utilisée dans le cadre d'une évaluation à la place de la simple valeur du capteur. Un attribut relatif est la réduction de l'utilisation des variables globales, comme décrit ci-dessous.

G.3.4.5 Gestion correcte des fonctions auxiliaires du programme d'application

L'instrumentation du programme d'application collecte et sort certaines valeurs d'état interne d'un programme d'application lors de l'exécution, et permet au développeur de vérifier si des aspects particuliers de la spécification ont été correctement mis en œuvre. Les problèmes relatifs à la sécurité spécifiques sont:

La réduction des perturbations d'exécution: Les fonctions auxiliaires qui interfèrent avec le flux d'exécution normal ne sont pas souhaitables dans les applications de sécurité. Par exemple, une "écriture" étendue ou d'autres instructions de sortie peuvent donner lieu à l'exécution d'une quantité significative de programmes d'application de bibliothèque associée aux valeurs de sorties. Un moyen moins intrusif peut être d'écrire ces valeurs dans des emplacements de mémoire externe, où ils pourront être traités plus tard. Cela peut aussi vouloir dire l'écriture des données dans un format binaire pour le traitement de format hors ligne (c'est-à-dire, la conversion en valeurs numériques et en texte lisible par l'homme). Pour réduire les différences de comportement entre l'essai et le fonctionnement normal, il peut être souhaitable de conserver certaines fonctions auxiliaires du programme d'application dans l'environnement réel.

Le maintien de la visibilité des fonctions auxiliaires dans le programme d'application d'exécution: Certains outils du programme d'application modifient les fichiers objets (ou exécutables) générés par le solveur logique afin d'insérer les fonctions auxiliaires. Cela n'est généralement pas acceptable dans un système de sécurité, car l'impact de ces changements

n'est pas visible dans le programme d'application et leur effet sur l'exécution ne peut pas être passé en revue.

La conformité aux lignes directrices relatives aux fonctions auxiliaires du programme d'application: La revue est facilitée (et la sécurité est donc améliorée) si les pratiques des fonctions auxiliaires sont décrites dans les traités d'ingénierie spécifiques au projet. Il convient que des lignes directrices identifient les types de mécanismes de sortie qui doivent être utilisés et dans quelles conditions il convient de ne pas les utiliser. Par exemple, une mesure mentionnée ci-dessus pour réduire l'interférence d'exécution est en contradiction avec les attributs d'abstraction de données et de confinement d'erreur décrits plus loin dans l'Annexe G.

G.3.4.6 Contrôle de la taille de la bibliothèque de classe

Il est important de contrôler la taille de la bibliothèque de classe pour éviter qu'un système devienne ingérable ou présente des performances très dégradées parce qu'il comporte trop de classes et d'objets. La sécurité est améliorée si les lignes directrices spécifiques au projet limitent le nombre de classes et d'objets, et si le programme d'application réel est conforme à ces lignes directrices.

G.3.4.7 Réduction de l'utilisation des liaisons dynamiques

La liaison dénote l'association d'un nom avec une classe. Les liaisons dynamiques permettent à l'association nom/classe d'être différée jusqu'à ce que l'objet désigné par le nom soit créé au moment de l'exécution. L'imprévisibilité de l'association nom/classe crée donc des problèmes de sécurité. Cela réduit également la prévisibilité du comportement d'exécution d'un programme orienté objet, et cela complique le débogage, la compréhension et le traçage. La restriction ou l'élimination des liaisons dynamiques est souhaitable pour les applications de sécurité critiques. L'IEC 61508-3 s'applique aux programmes d'application qui utilisent les liaisons dynamiques.

G.3.4.8 Contrôle de la surcharge d'opérateur

Le polymorphisme (surcharge d'opérateur) peut améliorer la lisibilité et réduire la complexité, en permettant l'utilisation d'un seul comportement de sous-programme, d'opérateur ou d'objet pour des types de données différents. Toutefois, cela peut également être problématique du point de vue de la prévisibilité. En effet, la façon dont un solveur logique reliera le programme d'application pour différents polymorphismes (la manière dont une opération de multiplication dans une matrice multidimensionnelle pourrait être reliée à des scalaires ou à des matrices unidimensionnelles, par exemple) n'est pas claire.

Des lignes directrices sur l'utilisation de la surcharge d'opérateur dans un manuel de normes de programmation d'application organisationnelle ou spécifique au projet sont donc souhaitables pour les applications relatives à la sécurité, et pour vérifier que le programme d'application est conforme à la présente norme.

G.3.5 Prévisibilité du planning

G.3.5.1 Généralités

La prévisibilité temporelle est cruciale dans un système de sécurité utilisé dans le contrôle en temps réel. Les attributs de base relatifs à la programmation orientée objet pertinents pour cet attribut intermédiaire sont par ailleurs décrits:

- le contrôle de la taille de la bibliothèque de classe;
- la réduction de l'utilisation des liaisons dynamiques;
- le contrôle de la surcharge d'opérateur.

Deux attributs de base supplémentaires relatifs au temps présentés dans les paragraphes suivants sont:

– la réduction de l'utilisation de l'attribution des tâches;
– la réduction de l'utilisation du traitement déclenché par interruption.

G.3.5.2 Réduction de l'utilisation de l'attribution des tâches

Bien que l'attribution des tâches fournisse un modèle attractif pour le traitement concomitant, son utilisation n'est pas souhaitable dans les applications de sécurité critiques pour les raisons suivantes:

- La séquence d'exécution est incertaine quand plusieurs alternatives d'appel attendent d'être exécutées car il n'est pas toujours clair de savoir quel appel sera sélectionné.
- L'attribution des tâches permet aux erreurs temporelles critiques, par exemple les états de concurrence et les interblocages, de se développer. Ces différences sont difficiles à déboguer.

L'attribution des tâches doit être évitée dans les systèmes de sécurité sauf en cas de justification impérative.

G.3.5.3 Réduction de l'utilisation du traitement déclenché par interruption

L'utilisation du traitement déclenché par interruption pour gérer l'acceptation et le traitement des entrées d'installation et d'opérateur peut réduire le temps moyen de réponse, mais conduit généralement à des temps de réponse maximaux non déterministes. Le traitement déclenché par interruption a été impliqué dans certains accidents.

Les normes et documents de références relatifs à la sécurité d'un système numérique découragent ou interdisent généralement son utilisation (IEC 60880:2006). Le fait d'éviter le traitement déclenché par interruption facilite l'analyse de la synchronisation et du comportement d'exécution. Cela évite en outre le non-déterminisme du temps de réponse inhérent au traitement déclenché par interruption.

G.4 Prévisibilité du résultat mathématique ou logique

La prévisibilité du résultat mathématique ou logique signifie que les résultats obtenus à la fin de l'exécution du niveau le plus faible du programme d'application en cours d'examen sont ceux prévus et attendus par le programmeur qui a écrit le programme d'application. Le terme "logique" est destiné à étendre le terme "résultats" au cas où le programme d'application manipule des données booléennes et lorsqu'il générera un résultat booléen. Il convient donc qu'un programme d'application de sécurité soit strictement statique. L'IEC 61508-3:2010 s'applique aux programmes d'application qui utilisent des mémoires à bascule de façon explicite ou implicite.

Une forte utilisation des verrouillages modifie la prévisibilité des résultats et augmente la complexité de la démonstration d'indépendance entre les structures de programme d'application. Il convient que les SIF ne soient pas verrouillées entre elles.

Il convient que l'utilisation de temporisateurs soit limitée et pas mise en cascade ou verrouillée.

G.5 Robustesse

G.5.1 Généralités

La robustesse fait référence à la capacité du programme d'application à poursuivre son exécution dans des conditions anormales ou non anticipées. Un synonyme de robustesse est

pérennité. La robustesse est un attribut important pour un système de sécurité. En effet, des événements non anticipés peuvent se produire pendant un accident ou une excursion, et la capacité du programme d'application à poursuivre la surveillance et la commande d'un système est vitale dans de telles circonstances.

Les attributs intermédiaires de robustesse sont:

- le contrôle de l'utilisation de la diversité;
- le contrôle de l'utilisation de la gestion des exceptions;
- la vérification de l'entrée et de la sortie.

G.5.2 Contrôle de l'utilisation de la diversité

G.5.2.1 Généralités

La décision d'utiliser différentes mises en œuvre du programme d'application est une fonction au niveau de la conception, qui est donc en dehors du domaine d'application des présentes lignes directrices. Toutefois, si de la diversité est souhaitée dans la conception ou les exigences, il convient qu'elle soit contrôlée dans son application. Le principal problème lié à l'utilisation de la diversité dans le programme d'application est la possibilité que des défaillances en mode commun du programme d'application puissent provoquer une défaillance des systèmes de sécurité entraînant une perte de la fonction de sécurité.

La possibilité de défaillances en mode commun entre des routines de programme d'application développées de façon indépendante n'est pas facile à éliminer. Toute spécification partagée peut conduire à des défaillances en mode commun. Le même problème existe dans le développement de données d'essai pour vérifier le programme d'application, les personnes qui réalisent les essais pouvant omettre les mêmes cas non nominaux ou inhabituels que les développeurs. De plus, pour utiliser l'approche grâce à laquelle les sorties de plusieurs versions du programme d'application peuvent être comparées en temps réel (ou pour pouvoir comparer les résultats intermédiaires), les conceptions des équipes indépendantes peuvent être spécifiées de manière excessive. De telles spécifications communes détaillées peuvent donner une faible diversité dans les programmes d'application. Cela se produit souvent dans les normes de programmation d'entreprise.

De plus, plusieurs versions du programme d'application écrites de façon indépendante à partir de la même spécification d'exigences sont uniquement efficaces contre les erreurs de programmation d'application (voire à un nombre d'erreurs limité). D'autre part, les preuves empiriques suggèrent que la plupart des problèmes de sécurité (et des erreurs détectées dans le programme d'application opérationnel) proviennent d'erreurs dans les exigences du programme d'application, et en particulier d'une mauvaise compréhension du fonctionnement exigé du programme d'application. Le programme d'application prévu pour assurer la redondance peut ne pas atteindre cet objectif, mais peut simplement multiplier les problèmes de mauvaise compréhension. Lors de la revue du programme d'application de sécurité critique, l'analyse de la diversité du programme d'application pour déterminer les défaillances en mode commun est importante.

Deux attributs de base sont distingués:

- contrôle de la diversité interne;
- contrôle de la diversité externe.

G.5.2.2 Contrôle de la diversité interne

Quand seule la diversité interne est utilisée, il convient que les interfaces de toutes les versions soient identiques. En d'autres termes, il convient que les paramètres ou les données des capteurs des procédures d'appel soient transmis de façon identique à toutes les versions; il convient en outre que les données de sortie de toutes les versions soient acceptées et utilisées par les autres parties du système. Il convient par contre que les opérations internes

et que le stockage des données locales se comportent différemment dans les instanciations ou les versions à plusieurs modules. La diversité interne est facilitée par une approche orientée objet, dans laquelle les mêmes messages et méthodes sont utilisés, mais où les représentations de données et les algorithmes internes diffèrent. Il convient que la diversité interne soit mise en œuvre conformément à la conception et aux lignes directrices spécifiques du projet. Il convient que ces lignes directrices s'adressent aux éléments suivants:

- Différents algorithmes: L'utilisation d'algorithmes, de conversions d'unités et de paramètres de processus différents (en cas d'appels ou si cela est admis dans les exigences ou la conception) réduit la possibilité qu'une défaillance survienne dans la conception ou la mise en œuvre.
- Validation des différentes données: L'utilisation d'autres schémas de validation des données du capteur (ou d'une autre entrée) et des données de sortie limite la possibilité de défaillance liée à la mise en œuvre du concepteur.
- Différentes routines de la gestion des exceptions: Cette mesure réduit la probabilité qu'une erreur dans le traitement ou la gestion des exceptions survienne en même temps dans plusieurs versions.
- Différents types de données, structures et affectations de stockage: Cette mesure réduit la possibilité que des interactions non anticipées entre le programme d'application d'objet généré par l'outil de programmation d'application et le solveur logique soient à l'origine d'un remplacement accidentel simultané des données ou du programme d'application sur plusieurs versions.
- Différentes bibliothèques et sous-routines: Eviter l'utilisation des mêmes sous-routines de programme d'application, routines de bibliothèque fournies par le compilateur et interfaces de programmation d'application fournies par le solveur logique. Cette mesure réduit la possibilité d'une défaillance simultanée en cas de problème dans ces routines.
- Ordre d'opération arithmétique différent: Le changement d'ordre des opérations arithmétiques dans les énoncés de conversion, arithmétiques et d'affectation à l'aide de propriétés commutatives, associatives et distributives réduit la possibilité de défaillances simultanées à cause de conditions de débordement non anticipées générées par les résultats intermédiaires ou de problèmes dans la précision numérique.
- Ordre d'opération d'entrée et de sortie différent: L'exécution d'opérations d'E/S dans différents ordres réduit la possibilité de défaillances simultanées liées à la temporisation (interblocage, par exemple) ou aux défaillances guidées par les données (c'est-à-dire, le plantage d'un programme d'application à cause d'une valeur de données particulière).

La limite de la diversité est le fait que, sur une plate-forme donnée, tous ces langages ne sont en fait qu'une représentation diverse des mêmes algorithmes. L'utilisation de la diversité des langages ne compense donc que la faiblesse de chaque langage avant la compilation. Le programme d'application peut donc être écrit dans deux langages différents afin d'en comparer les comportements.

G.5.2.3 Contrôle de la diversité externe

Quand la diversité externe est utilisée, la sécurité est améliorée si elle est mise en œuvre de façon disciplinée, conformément aux documents de conception. Il convient que les documents de conception reflètent la diversité imposée par les exigences, les analyses de danger et les sources similaires. La diversité externe est obtenue à l'aide de différentes interfaces dans les versions et peut être combinée à la diversité interne. La diversité externe est nécessaire quand des langages différents sont utilisés pour des versions différentes; elle peut aussi être utilisée pour obtenir des données de capteur via un autre canal. La diversité externe non contrôlée ou non spécifiée peut conduire à une prolifération d'interfaces, ce qui a un impact sur la sécurité à cause des difficultés de maintenance, d'essai, de vérification et de validation.

G.5.3 Contrôle de l'utilisation de la gestion des exceptions

G.5.3.1 Généralités

La gestion des exceptions traite des données d'entrée et des états système anormaux. Les dispositions de gestion des exceptions dans certains langages facilitent l'établissement d'un autre chemin d'exécution dans l'éventualité de conditions qui, bien qu'inattendues, résulteraient dans des états qui peuvent être définis à l'avance. Des problèmes peuvent toutefois survenir lors de la survenue et de la gestion des exceptions, car le flux d'exécution dans des conditions d'exception est souvent difficile à tracer.

Les attributs de base qui concernent la gestion des exceptions incluent:

- la gestion des exceptions en local;
- la préservation du flux de contrôle externe;
- la gestion des exceptions de façon uniforme.

G.5.3.2 Gestion des exceptions en local

La propagation des exceptions via différents niveaux d'un programme d'application peut provoquer une mauvaise interprétation de la nature exacte de l'exception là où la gestion des exceptions est mise en œuvre. Cette cause de défaillance système (avec des implications potentiellement sérieuses sur la sécurité) est évitée si les exceptions sont gérées en local.

G.5.3.3 Préservation du flux de contrôle externe

L'interruption du flux de contrôle externe à la routine dans laquelle l'exception est survenue crée une incertitude dans l'exécution qui suit la gestion des exceptions. La sécurité est améliorée par la préservation du flux de contrôle externe au module responsable de l'exception.

G.5.3.4 Gestion des exceptions de façon uniforme

Une utilisation imprudente de la gestion des exceptions peut se traduire par un traitement incohérent de la même condition d'exception dans des parties différentes du programme d'application. Dans le cas le plus défavorable, cela peut générer des exceptions qui ne sont pas gérées. Ces problèmes peuvent être évités par l'utilisation de lignes directrices sur l'utilisation d'exceptions dans le cadre des procédures des pratiques de programmation d'application pour l'organisation ou le projet spécifique. Rubriques à inclure dans ces lignes directrices:

- les exceptions générales et spécifiques au projet qui ont été définies et qui sont admises;
- le placement du programme d'application de gestion des exceptions;
- l'énumération de tous les effets secondaires prévus et la vérification qu'il n'y a pas d'autre effet secondaire;
- la vérification de l'intégrité des données d'état critiques pendant le traitement de l'exception.

Les critères qui permettent de distinguer quelles conditions il convient de gérer via des constructions de flux de contrôle dans le cadre d'un traitement normal par opposition à des conditions anormales, où l'utilisation de la gestion des exceptions est appropriée.

G.5.4 Vérification de l'entrée et de la sortie

G.5.4.1 Généralités

Les corruptions de données à cause d'une défaillance transitoire ou d'un résultat non valide peuvent avoir de sérieuses conséquences sur le traitement suivant s'il est admis qu'elles se propagent. Les attributs de base relatifs à la vérification des entrées et des sorties atténuent

les conséquences en contenant l'erreur. Les deux attributs de base décrits en G.5.4.2 et G.5.4.3 sont:

- la vérification des données d'entrée, et
- la vérification des données de sortie.

G.5.4.2 Vérification des données d'entrée

Les données d'entrées incluent des données d'une autre routine, des données de l'environnement externe et des données stockées dans la mémoire d'une itération précédente. Il convient que la validité des données d'entrée soit vérifiée avant le traitement. Ces vérifications réduisent la probabilité que des résultats incorrects ou que des données corrompues soient propagées. Au minimum, il convient que les valeurs des entrées soient vérifiées en fonction du type de données et de la plage acceptable. Si possible, il convient également d'effectuer des vérifications de vraisemblance sur les données. Il convient de prévoir des dispositions dans le programme d'application pour détecter les entrées non valides et pour faire passer le module à un état connu (c'est-à-dire, les valeurs valides précédentes ou les valeurs par défaut), comme défini dans la conception de niveau supérieur.

G.5.4.3 Vérification des données de sortie

Il convient de vérifier la validité des données de sortie – dans l'environnement externe, dans une autre routine ou stockées pour être utilisées dans une itération ultérieure. Au minimum, il convient que cette vérification de validité garantisse que les valeurs sont du type de données approprié et dans une plage acceptable. Il est plus souhaitable que la vraisemblance des valeurs soit aussi vérifiée. Il convient toutefois que ces vérifications de vraisemblance ne soient pas si restrictives qu'elles rejettent à tort des valeurs correctes. Il convient également que des dispositions de gestion des valeurs de sortie rejetées conformément à la conception soient présentes dans le programme d'application.

G.6 Traçabilité

G.6.1 Généralités

Comme indiqué précédemment dans la présente annexe, la traçabilité fait référence aux attributs du programme d'application de sécurité qui prennent en charge la vérification de l'exactitude et de l'exhaustivité par rapport à la conception du programme d'application. Les attributs intermédiaires de traçabilité sont:

- la lisibilité;
- le contrôle de l'utilisation des fonctions intégrées (G.6.2);
- le contrôle de l'utilisation des bibliothèques compilées (G.6.3).

La lisibilité étant également un attribut intermédiaire de la maintenabilité, elle est présentée en G.3.4.8. Les deux derniers attributs et leur pertinence eu égard à la sécurité sont présentés en G.6.2 et G.6.3.

G.6.2 Contrôle de l'utilisation des fonctions intégrées

Presque tous les langages incluent des fonctions intégrées pour les tâches de programmation fréquemment utilisées afin d'optimiser la productivité du programmeur. Toutefois, les limites de ces fonctions et la façon dont elles gèrent les exceptions peuvent ne pas être aussi bien connues que celles des constructions du langage de base. L'utilisation de ces fonctions crée donc des problèmes de sécurité.

Les problèmes sur l'utilisation des fonctions intégrées peuvent être adressés via des lignes directrices organisationnelles ou spécifiques au projet. Les cas d'essai de régression permettent l'établissement d'une conformité avec les résultats attendus des nouvelles versions de compilateurs et de bibliothèques d'exécution. Il convient donc de conserver les

cas d'essai, les procédures et les résultats des essais précédents pour les fonctions intégrées admissibles. Il convient également que les essais évaluent le comportement pour les conditions hors limites et marginales (des arguments négatifs sur une routine de racine carrée, des chaînes mal arrêtées pour une routine de copie de chaîne, etc.) dans l'environnement d'exécution spécifique.

G.6.3 Contrôle de l'utilisation des bibliothèques compilées

Les bibliothèques compilées sont des routines écrites et compilées par une entité autre que le groupe de développement. Les applications de bibliothèques compilées incluent les opérations d'entrée/de sortie, les pilotes d'appareils ou les opérations mathématiques qui ne sont pas définies dans le langage normalisé. De telles bibliothèques peuvent être fournies par les constructeurs d'outils de programmation d'application, des tiers ou d'autres départements de l'organisation de développement. Les inquiétudes en matière d'utilisation de ces bibliothèques sont similaires à celles relatives aux fonctions intégrées.

Les inquiétudes en matière d'utilisation de bibliothèques compilées peuvent être traitées en contrôlant l'utilisation des appels de fonction à ces bibliothèques via des lignes directrices organisationnelles ou spécifiques au projet.

Comme pour les fonctions intégrées, il convient de maintenir un jeu de cas d'essai, de procédures et de résultats. Il convient que les cas d'essai évaluent le comportement pour les conditions normales, hors limites et marginales dans l'environnement d'exécution spécifique. Il convient que les essais de régression soient effectués pour chaque nouvelle version de la bibliothèque compilée.

G.7 Maintenabilité

G.7.1 Généralités

La maintenabilité du programme d'application réduit la probabilité d'introduction d'erreurs lors des changements. Les attributs intermédiaires relatifs à la maintenabilité qui affectent la sécurité incluent:

- la lisibilité: les attributs du programme d'application qui facilitent la compréhension du programme d'application par le personnel de projet;
- l'abstraction des données: l'étendue du partitionnement et de la modularisation du programme d'application, de manière à réduire l'impact collatéral et la probabilité de survenue d'effets secondaires imprévus lors de l'apport de changements au programme d'application;
- la cohérence fonctionnelle: l'affectation appropriée de fonctions au niveau de la conception aux appareils du programme d'application dans le programme d'application (une procédure, une fonction);
- la malléabilité: la mesure dans laquelle les zones de changements potentiels sont isolées du reste du programme d'application;
- la portabilité: le principal impact de sécurité lié à l'évitement des fonctions non normalisées d'un langage.

G.7.2 Lisibilité

G.7.2.1 Généralités

La lisibilité permet au personnel de développement qualifié, autre que l'auteur, de comprendre le programme d'application. L'importance de la lisibilité pour la maintenabilité peut être vue à travers des études dans lesquelles la lecture manuelle du programme d'application (vérification théorique) s'est révélée plus efficace que des essais structurels ou fonctionnels pour rechercher des erreurs dans la programmation d'application. Une extrapolation raisonnable consiste à dire que la lisibilité améliorerait également l'identification

du programme d'application à modifier pendant une procédure de maintenance corrective ou adaptative, et réduirait la probabilité d'introduction de nouvelles erreurs au cours de cette maintenance.

Il n'existe aucune norme générale de lisibilité qui puisse être rendue obligatoire ou même recommandée. Des manuels de pratiques et des styles de programmation d'application organisationnels ou spécifiques au projet (ou des lignes directrices relatives) sont toutefois attendus pour les SIS. Les attributs de base suivants sont relatifs à la lisibilité.

- la conformité aux lignes directrices d'indentation;
- l'utilisation de noms d'identification descriptifs;
- les commentaires et la documentation interne;
- la limitation de la taille du sous-programme;
- la réduction de la programmation dans plusieurs langages;
- la réduction des constructions de programmation obscures ou subtiles;
- la réduction de la dispersion ou des appareils connexes;
- la réduction de l'utilisation des littéraux.

G.7.2.2 Conformité aux lignes directrices d'indentation

Une indentation appropriée facilite l'identification des déclarations, des flux de contrôle, des commentaires non exécutables et des autres appareils du programme d'application. Les lignes directrices d'indentation font généralement partie de normes ou d'un type de programmation organisationnel ou spécifique au projet. Les problèmes significatifs que doivent traiter les pratiques d'application sont la gestion des éléments suivants:

- les blocs de programmation (séquences d'énoncés liés par le début et la fin);
- les commentaires;
- les constructions de branche (par exemple, if...then...else, énoncés de cas, boucles, etc.);
- plusieurs niveaux d'imbrication (par exemple, une boucle do dans une boucle do);
- les déclarations de variable et de sous-routine;
- les directives de l'outil de programmation d'application;
- survenue et gestion des exceptions.

G.7.2.3 Utilisation de noms d'identification descriptifs

Les noms des variables, des procédures, des fonctions, des types de données, des constantes, des exceptions, des objets, des méthodes, des étiquettes et d'autres identifiants qui ne sont pas faciles à comprendre peuvent empêcher la revue et la maintenance. Les problèmes de sécurité découlant de certaines pratiques de dénomination peuvent être compensés quand les noms doivent être descriptifs, cohérents et traçables pour les documents de niveau supérieur (c'est-à-dire la conception du programme d'application). Les conventions de dénomination sont une partie importante du style de la programmation d'application et du manuel des pratiques.

Des exemples de facteurs à résoudre incluent:

- l'identification des données d'entrée de l'installation (par exemple, s'il convient que la variable fasse référence à un capteur ou s'il convient de l'appeler loop1_hot_leg_TC1);
- la façon dont il convient de nommer les variables de mise en boucle (par exemple, "i,j,k" ou titres plus longs);
- la redénomination locale des identifiants (par exemple, "moyen de procédure moyenne" renommé "moyen");

- la distinction entre les différentes catégories d'identifiants (par exemple, un suffixe sur tous les types de données avec un _T pour les distinguer des variables);
- les listes de mots réservés et de termes spécifiques au projet (par exemple, les restrictions sur l'utilisation des termes "alarme", "limite", etc.).

L'utilisation du même nom pour un autre objectif doit être évitée sauf s'il s'agit d'un avantage évident; s'il est utilisé, il convient qu'il soit accompagné de notations claires, cohérentes et pas ambiguës. L'utilisation de plusieurs occurrences du même nom peut être source de confusion. Un autre problème peut se produire si le langage prend en charge des unités précompilées. Une variable avec le même nom dans deux progiciels différents, dont l'un est utilisé par l'autre, peut être interprétée par l'outil de programmation d'application d'une autre manière que celle prévue par l'auteur du programme. Dans certains cas, le programmeur peut avoir omis la déclaration d'un nom dans un progiciel. Un autre progiciel peut donc conduire à utiliser une autre variable du même nom de façon totalement imprévue. Si le chemin d'exécution ou la branche en particulier n'est pas souvent rencontré, il est possible qu'une telle erreur ne soit pas découverte avant d'avoir provoqué une défaillance d'exécution.

L'utilisation de mots réservés pour des identifiants sélectionnés par les utilisateurs (dans les langages pour lesquels cette fonctionnalité est admise) n'est pas souhaitable.

G.7.2.4 Commentaires et documentation interne

Des commentaires incomplets, des formats incohérents et des commentaires non mis à jour pour refléter le programme d'application en cours empêchent la revue et posent des problèmes de sécurité. Ces problèmes peuvent être limités par l'utilisation de lignes directrices dans les normes de programmation d'application organisationnelles ou spécifiques au projet afin de contrôler les commentaires et la documentation interne (au programme d'application). Des exemples d'éléments, lors de leur incorporation, qu'il convient de placer dans la section de prologue incluent:

- l'objectif du sous-programme ou de l'unité et la façon d'y arriver;
- les fonctions et les exigences de performances, ainsi que les interfaces externes que le sous-programme ou que l'unité met en œuvre;
- les autres sous-programmes ou unités appelés et leurs dépendances;
- l'utilisation de variables globales et locales, mais aussi, si applicables, les emplacements de mémoire et de registre avec les instructions de maintenance spéciales;
- le département ou la section responsable de la programmation;
- la date de création de l'unité;
- la date de la dernière révision, le numéro de révision, le numéro de rapport de problème et le titre associé à la révision, le comportement de défaillance prévu et les informations relatives à tous les principaux segments du programme d'application;
- les entrées et les sorties, y compris les fichiers de données référencés dans l'article d'entrée d'exécution;
- les commentaires sur l'objectif, le domaine d'application et les limitations de chaque argument (pour les sous-programmes avec des arguments).

Des exemples similaires pour la documentation dans le programme d'application incluent:

– la référence à la documentation de conception de niveau supérieur dans les commentaires associés aux déclarations de type de données, de variable et de constante;
– l'objectif et les résultats attendus au début des branches et des blocs de programmation;
– des commentaires en lignes détaillés qui expliquent les constructions inhabituelles et les écarts par rapport aux pratiques de programmation.

G.7.2.5 Limitation de la taille du sous-programme

Certains documents recommandent des limites spécifiques sur le programme d'application de chaque sous-programme ou unité. Par exemple, une moyenne de 100 énoncés non extensibles et un maximum de plus de 200 énoncés de ce type ont été recommandés. Les problèmes liés à la taille des sous-programmes ont fait partie des motivations qui ont conduit à l'adoption de la programmation structurée. Des sous-programmes de petite taille (une ou deux pages) sont plus faciles à passer en revue que les plus longs. Il convient toutefois aussi que les limites de tailles admises prennent en compte la nature du programme et du langage. Dans les systèmes de commande et de sécurité des processus, il convient qu'un programme d'application donné gère fréquemment une multitude de quantités ressenties, leurs déclarations de données (avec les commentaires exigés) pouvant par elles-mêmes compter pour plusieurs pages. Le critère de cet attribut de base est donc que des lignes directrices sur la taille soient fournies plutôt qu'un seuil numérique universel.

G.7.2.6 Réduction de la programmation dans plusieurs langages

L'utilisation de plusieurs langages de programmation, par exemple, "diagramme fonctionnel séquentiel" pour les commandes séquentielles, "diagramme à contacts" pour la logique booléenne et "bloc fonctionnel" pour les fonctions plus sophistiquées (mise à l'échelle, moyennes, etc.) présente des difficultés pour les réviseurs et les agents de maintenance, ce qui pose des problèmes de sécurité. Quand cette pratique ne peut pas être évitée, les difficultés peuvent être réduites en plaçant le programme d'application dans un langage "étranger" à côté de la routine du langage dominante avec laquelle il est en interface (une directive d'outil de programmation d'application d'assemblage en ligne dans la routine de traitement des entrées associée à une interruption, par exemple) afin d'améliorer la lisibilité.

Si cette pratique ne peut pas être évitée, les difficultés peuvent être réduites par le placement du programme d'application dans un langage "étranger" imbriqué dans la routine du langage dominante avec laquelle il est en interface (du texte structuré imbriqué dans un bloc de fonction d'un diagramme de bloc fonctionnel, par exemple) afin d'améliorer la lisibilité.

G.7.2.7 Réduction des constructions de programmation obscures ou subtiles

Des constructions de programmation d'application obscures peuvent généralement être caractérisées comme l'utilisation de techniques indirectes afin de réduire la quantité de traitement de solveur logique ou de programmation d'application exigée pour obtenir un résultat. De telles pratiques de programmation d'application présentent des problèmes de revue et de maintenance, ce qui pose des problèmes de sécurité. Par exemple, le fait de déplacer un entier vers la gauche équivaut à multiplier sa valeur par deux. La première construction serait toutefois obscure si la conception appelait à doubler la valeur (c'est-à-dire qu'il serait préférable d'effectuer la multiplication). La deuxième construction serait obscure si la conception appelait à déplacer la valeur vers la gauche (c'est-à-dire qu'il serait préférable d'effectuer l'opération de déplacement dans le programme d'application plutôt que de multiplier par 2). Les commentaires appropriés peuvent minimiser l'impact des changements de programmation d'application obscurs ou légèrement obscurs (par exemple, l'addition d'une valeur à elle-même comme moyen de la doubler).

Il convient d'éviter l'inversion des états réels du capteur ou de l'actionneur en états logiques via les fonctions "NOT", ainsi que le multiplexage des booléens en entiers et en sorties de verrouillage.

G.7.2.8 Réduction de la dispersion ou des appareils relatifs

Si des appareils relatifs au programme d'application sont dispersés dans un programme, il doit être fait référence à plusieurs emplacements dans un programme d'application pendant la revue et la maintenance. La nature spécifique de la dispersion varie toutefois en fonction du langage. Par exemple, certains langages permettent de séparer les spécifications d'interface du corps du programme d'application, d'autres permettant le "prototypage" pour un objectif similaire. Pour les langages avec un typage des données fort, il peut être souhaitable de

centraliser toutes les déclarations de type dans un seul fichier (ou jeu de fichiers); pour les langages orientés objet, il peut être souhaitable de séparer les classes de base et les classes dérivées. La revue est facilitée et la sécurité est améliorée si des lignes directrices spécifiques au projet sont fournies sur l'emplacement des appareils relatifs dans le programme d'application.

G.7.2.9 Réduction de l'utilisation des littéraux

Les littéraux (c'est-à-dire un nombre réel ou une chaîne réelle dans le programme d'application) sont plus difficiles à identifier que les noms auxquels une valeur de constante est affectée au début du module. Les littéraux impactent la sécurité, car ils réduisent la lisibilité et compliquent la maintenabilité – en particulier s'ils sont associés à un paramètre de processus qui peut être affiné ou à un facteur de conversion qui peut être changé après le réétalonnage d'un instrument. Il est nettement plus facile de changer une valeur établie au début d'un fichier que de garantir que tous les littéraux associés à un tel paramètre ont été changés de manière complète et correcte dans tous les fichiers pertinents.

G.7.3 Abstraction des données

G.7.3.1 Généralités

L'abstraction des données est la combinaison de données et des exploitations admissibles de ces données dans une seule entité, ainsi que l'établissement d'une interface qui permet l'accès aux données, leur manipulation et leur stockage uniquement pour les exploitations admissibles. Il contribue de manière importante à la sécurité en réduisant ou en éliminant les effets secondaires potentiels de la modification des variables, soit pendant l'exécution, soit dans le cadre des activités de maintenance du programme d'application. Ce principe est associé aux attributs de base spécifiques suivants:

- la réduction de l'utilisation des variables globales;
- la réduction de la complexité de l'interface via la définition d'opérations admises.

G.7.3.2 Réduction de l'utilisation des variables globales

Il est souhaitable de limiter l'utilisation des variables globales dans les programmes relatifs à la sécurité à cause du potentiel de survenue d'effets secondaires indésirables. La lisibilité est améliorée si des variables sont définies et utilisées dans la même routine. Ces variables peuvent être mises à la disposition d'autres routines via des interfaces établies et contrôlées, ce qui réduit le risque d'interactions non prévues. Pour les mêmes raisons, il convient de contrôler ou d'éviter les dépendances entre les données stockées en interne des différentes routines.

Pour éviter tout problème potentiel de sécurité, il convient que les variables locales de programmes différents ne partagent pas le même emplacement de stockage.

Il convient d'éviter les variables globales qui peuvent être écrites depuis plusieurs instances logiques dans le programme d'application, à cause des effets secondaires indésirables potentiels.

G.7.3.3 Réduction de la complexité des interfaces

Les interfaces sont une cause fréquente de défaillances du programme d'application. Les interfaces complexes, qui sont difficiles à passer en revue et à maintenir, ne sont pas souhaitables dans les programmes relatifs à la sécurité. Les caractéristiques qui contribuent à la complexité incluent:

- un grand nombre d'arguments utilisés dans les routines d'appel;
- l'utilisation d'expressions concises quand différents modes ou options sont utilisés;

- un manque de restrictions et de limites faciles à comprendre sur l'utilisation des exploitations admises.

G.7.4 Cohérence fonctionnelle

G.7.4.1 Généralités

La cohérence fonctionnelle fait référence à une correspondance claire entre les fonctions d'un programme d'application et la structure de ses appareils. La cohérence fonctionnelle a un seul attribut de base.

G.7.4.2 Procédures et fonctions à un seul objectif

La revue et la maintenance sont facilitées lorsque chaque procédure, sous-programme ou fonction donné(e) ne met en œuvre qu'une tâche ou qu'un objectif spécifié(e) dans la conception du programme d'application.

Il convient que les sous-programmes, les fonctions ou les procédures qui effectuent plusieurs tâches soient séparés et écrits en tant que fonctions séparées. Une façon simple de soumettre une fonction à l'essai consiste à utiliser une fonction à objectif unique pour déterminer si la fonction peut être résumée en une phrase de la forme suivante:

"verbe + objet(s)"

L'IEC 61511 prévoit d'itérer les éléments types en tant que SIF pour être mis en œuvre dans un seul solveur logique.

G.7.4.3 Variables à un seul objectif

Il convient d'appliquer les principes des fonctions à un seul objectif aux variables. Il convient de n'utiliser une variable que pour un seul objectif.

G.7.5 Malléabilité

G.7.5.1 Généralités

La malléabilité est la capacité d'un programme d'application à accepter les changements dans les exigences fonctionnelles. La malléabilité étend l'abstraction des données avec pour motivation l'isolation des zones de changements potentiels. Afin de mettre en œuvre un système de programme d'application malléable, les éléments censés être constants et ceux censés être modifiés doivent être identifiés, et les éléments censés être modifiés doivent être isolés en zones facilement identifiables qui peuvent être altérées avec un minimum de changements collatéraux. La malléabilité a un seul attribut de base.

G.7.5.2 Isolation des fonctions altérables

La revue et la maintenance sont facilitées quand des fonctions qui peuvent être altérées sont isolées, de sorte que les changements qui leur sont apportés n'affectent pas d'autres données ou programmes d'application. Dans de nombreux cas, ces fonctions sont des fonctions relatives au matériel, qu'il convient de modifier quand la plate-forme change, quand le système change ou quand de nouveaux appareils sont utilisés pour remplacer de vieux appareils, par exemple un solveur logique plus puissant de la même ligne de produits d'un fabricant.

A un niveau plus large, l'isolation des fonctions altérables est un problème de conception relatif à l'abstraction des données. En tant que telle, une discussion détaillée est donc en dehors du domaine d'application de ces lignes directrices.

G.7.6 Portabilité

G.7.6.1 Généralités

Du point de vue de la sécurité, les avantages de la portabilité sont l'adhésion à des constructions de programmation normalisées qui donnent des résultats prévisibles et cohérents sur différentes plates-formes d'exploitation. Un programme d'application réutilisé ou converti pour s'exécuter sur une autre plate-forme sera donc plus facile à maintenir. Les attributs relatifs à la portabilité qui ont par ailleurs fait l'objet de discussions incluent:

- la réduction de l'utilisation des fonctions intégrées;
- la réduction de l'utilisation des bibliothèques compilées;
- la réduction des liaisons dynamiques;
- la réduction de l'attribution des tâches;
- la réduction des constructions (interruptions) asynchrones.

L'attribut de base unique relatif à la portabilité consiste à éviter l'utilisation de constructions non normalisées ou "améliorées" spécifiques à un outil de programmation d'application particulier ou à un outil de programmation d'application associé à la plate-forme d'exécution.

G.7.6.2 Isolation de constructions non normalisées

Quand des constructions non normalisées sont nécessaires, il convient de les identifier clairement en même temps que la justification, que les limitations et que les dépendances de version.

Bibliographie

[1] IEC 60880:2006, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

[2] IEC 61025:2006, *Analyse par arbre de panne (AAP)*

[3] IEC 61078:2006, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

[4] IEC 61131-3:2013, *Automates programmables – Partie 3: Langages de programmation*

[5] IEC 61165:2006, *Application des techniques de Markov*

[6] IEC 61506, *Mesure et commande dans les processus industriels – Documentation des logiciels d'application*

[7] IEC 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

[8] IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

[9] IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

[10] IEC 61508-6:2010, *Sécurité fonctionnelle des systèmesélectriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

[11] IEC 61882:2001, *Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application*

[12] IEC 62061:2005, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[13] IEC 62502:2010, *Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre d'événement (AAE)*

[14] IEC 62551:2012, *Techniques d'analyse de sûreté de fonctionnement – Techniques des réseaux de Petri*

[15] ISO 9000:2015, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

[16] ISO 10418:2003, *Industries du pétrole et du gaz naturel – Plates-formes de production en mer – Analyse, conception, installation et essais des systèmes essentiels de sécurité de surface*

[17] ISO TR 12489:2013, *Pétrole, pétrochimie et gaz naturel – Modélisation et calcul fiabilistes des systèmes de sécurité*

[18] ISO 17776:2000, *Industries du pétrole et du gaz naturel – Installations des plates-formes en mer – Lignes directrices relatives aux outils et techniques pour l'identification et l'évaluation des risques*

[19] ISO 31000:2009, *Management du risque – Principes et lignes directrices*

[20] API RP14C:2001(R2007), *Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms* (disponible en anglais seulement)

[21] ISA TR84.00.02:2002, *Part 1: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part1 Introduction* (disponible en anglais seulement; voir la version 2015 mise à jour ci-dessous)

[22] ISA TR84.00.02:2002, *Part 2: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 2 Determining the SIL of a SIF via Simplified Equations* (disponible en anglais seulement; voir la version 2015 mise à jour ci-dessous)

[23] ISA TR84.00.02:2002, *Part 3: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 3: Determining the SIL of a SIF via Fault Tree Analysis* (disponible en anglais seulement; voir la version 2015 mise à jour ci-dessous)

[24] ISA TR84.00.02:2002, *Part 4: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 4: Determining the SIL of a SIF via Markov Analysis* (disponible en anglais seulement; voir la version 2015 mise à jour ci-dessous)

[25] ISA TR84.00.02:2002, *Part 5: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 5: Determining the PFD of SIS Logic Solvers via Markov Analysis* (disponible en anglais seulement; voir la version 2015 mise à jour ci-dessous)

[26] ISA TR84.00.02:2015, *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions ISBN: 1-55617-802-6* (disponible en anglais seulement)

[27] ISA TR84.00.03:2012, *Mechanical Integrity of Safety Instrumented Systems (SIS)* (disponible en anglais seulement)

[28] ISA TR84.00.04:2015, *Part 1: Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)* (disponible en anglais seulement)

[29] ISA TR84.00.09: 2013, *Security Countermeasures Related To Safety Instrumented Systems (SIS)* (disponible en anglais seulement)

[30] NFPA 85:2015, *Boiler and combustions systems hazards code* (disponible en anglais seulement)

[31] CCPS/AICHE, *Human Factors Methods for Improving Performance in the Process Industries (1st edition), John Wiley & Sons (2007), ISBN 0 4701 1754 0* (disponible en anglais seulement)

[32] CCPS/AIChE, *Guidelines for Preventing Human Error in Process Safety (1st edition), John Wiley & Sons (2004), ISBN 08169 0461 8* (disponible en anglais seulement)

[33] CCPS/AIChE, *Guidelines for Chemical Process Quantitative Risk Analysis (second edition), New York: American Institute of Chemical Engineers (2000), 0 8169 0720 X* (disponible en anglais seulement)

[34] CCPS/AIChE*, Guidelines for Safe Automation of Process Applications, 1993* (disponible en anglais seulement)

[35] CCPS/AIChE, *Guidelines for Safe Storage and Handling of High Toxic Hazard Material* (disponible en anglais seulement)

[36] CCPS/AIChE, *Guidelines for Vapor Release Mitigation* (disponible en anglais seulement)

[37] CCPS/AIChE, *Guidelines for the Technical Management of Chemical Process Safety* (disponible en anglais seulement)

[38] CCPS/AIChE, *Layer of Protection Analysis, Simplified Process Risk Assessment, 2001* (disponible en anglais seulement)

[39] HSE*, Reducing Risk Protecting People, Health and Safety Executive, London (2001) ISBN No. 07176-2151-0* (disponible en anglais seulement)

[40] HSE, *Reducing error and influencing behavior, HSG48, Health and Safety Executive, London (2009), ISBN 978 0 7176 2452 2* (disponible en anglais seulement)

[41] NAMUR recommendation NE130:2011, *"Prior use"-Devices for Safety Instrumented Systems and simplified SIL Calculation* (disponible en anglais seulement*)*

[42] OSHA 29 CFR 1910.119:2013, *Process safety management of highly hazardous chemicals* (disponible en anglais seulement)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch