

CONSOLIDATED VERSION

VERSION CONSOLIDÉE



Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and application programming requirements

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2017 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 Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and definitions clause of IEC publications issued between 2002 and 2015. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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 une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et définitions des publications IEC parues entre 2002 et 2015. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

CONSOLIDATED VERSION

VERSION CONSOLIDÉE



Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and application programming requirements

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.110; 25.040.01

ISBN 978-2-8322-8012-6

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.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016+AMD1:2017 CSV

REDLINE VERSION

VERSION REDLINE



Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and application programming requirements

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

CONTENTS

FOREWORD	5
INTRODUCTION	7
1 Scope	9
2 Normative references	12
3 Terms, definitions and abbreviations	13
3.1 Terms	13
3.2 Terms and definitions	13
3.3 Abbreviations	31
4 Conformance to the IEC 61511-1:2016	32
5 Management of functional safety	32
5.1 Objective	32
5.2 Requirements	33
5.2.1 General	33
5.2.2 Organization and resources	33
5.2.3 Risk evaluation and risk management	33
5.2.4 Safety planning	33
5.2.5 Implementing and monitoring	34
5.2.6 Assessment, auditing and revisions	34
5.2.7 SIS configuration management	37
6 Safety life-cycle requirements	37
6.1 Objectives	37
6.2 Requirements	38
6.3 Application program SIS safety life-cycle requirements	40
7 Verification	43
7.1 Objective	43
7.2 Requirements	43
8 Process H&RA	45
8.1 Objectives	45
8.2 Requirements	45
9 Allocation of safety functions to protection layers	46
9.1 Objectives	46
9.2 Requirements of the allocation process	46
9.3 Requirements on the basic process control system as a protection layer	49
9.4 Requirements for preventing common cause, common mode and dependent failures	50
10 SIS safety requirements specification (SRS)	50
10.1 Objective	50
10.2 General requirements	50
10.3 SIS safety requirements	51
11 SIS design and engineering	53
11.1 Objective	53
11.2 General requirements	53
11.3 Requirements for system behaviour on detection of a fault	54
11.4 Hardware fault tolerance	55
11.5 Requirements for selection of devices	56

11.5.1	Objectives	56
11.5.2	General requirements	56
11.5.3	Requirements for the selection of devices based on prior use	56
11.5.4	Requirements for selection of FPL programmable devices (e.g., field devices) based on prior use	57
11.5.5	Requirements for selection of LVL programmable devices based on prior use	58
11.5.6	Requirements for selection of FVL programmable devices	59
11.6	Field devices	59
11.7	Interfaces	59
11.7.1	General	59
11.7.2	Operator interface requirements	59
11.7.3	Maintenance/engineering interface requirements	60
11.7.4	Communication interface requirements	60
11.8	Maintenance or testing design requirements	61
11.9	Quantification of random failure	61
12	SIS application program development	63
12.1	Objective	63
12.2	General requirements	63
12.3	Application program design	64
12.4	Application program implementation	65
12.5	Requirements for application program verification (review and testing)	66
12.6	Requirements for application program methodology and tools	67
13	Factory acceptance test (FAT)	68
13.1	Objective	68
13.2	Recommendations	68
14	SIS installation and commissioning	69
14.1	Objectives	69
14.2	Requirements	69
15	SIS safety validation	70
15.1	Objective	70
15.2	Requirements	70
16	SIS operation and maintenance	73
16.1	Objectives	73
16.2	Requirements	73
16.3	Proof testing and inspection	75
16.3.1	Proof testing	75
16.3.2	Inspection	76
16.3.3	Documentation of proof tests and inspection	76
17	SIS modification	76
17.1	Objectives	76
17.2	Requirements	77
18	SIS decommissioning	77
18.1	Objectives	77
18.2	Requirements	78
19	Information and documentation requirements	78
19.1	Objectives	78
19.2	Requirements	78

Bibliography	80
Figure 1 – Overall framework of the IEC 61511 series	8
Figure 2 – Relationship between IEC 61511 and IEC 61508	10
Figure 3 – Detailed relationship between IEC 61511 and IEC 61508	11
Figure 4 – Relationship between safety instrumented functions and other functions	12
Figure 5 – Programmable electronic system (PES): structure and terminology	24
Figure 6 – Example of SIS architectures comprising three SIS subsystems	26
Figure 7 – SIS safety life-cycle phases and FSA stages	38
Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle	41
Figure 9 – Typical protection layers and risk reduction means	49
Table 1 – Abbreviations used in IEC 61511	31
Table 2 – SIS safety life-cycle overview (1 of 2)	39
Table 3 – Application program safety life-cycle: overview (1 of 2)	42
Table 4 – Safety integrity requirements: PFD_{avg}	47
Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF	47
Table 6 – Minimum HFT requirements according to SIL	55

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016+AMD1:2017 CSV

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: Framework, definitions, system, hardware and application programming requirements

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.

DISCLAIMER

This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 61511-1 bears the edition number 2.1. It consists of the second edition (2016-02) [documents 65A/777/FDIS and 65A/784/RVD], its corrigendum 1 (2016-09) and its amendment 1 (2017-08) [documents 65A/844/FDIS and 65A/848/RVD]. The technical content is identical to the base edition and its amendment.

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition constitutes a technical revision and includes the following significant technical changes with respect to the previous edition:

- references and requirements to software replaced with references and requirements to application programming;
- functional safety assessment requirements provided with more detail to improve management of functional safety.
- management of change requirement added;
- security risk assessment requirements added;.
- requirements expanded on the basic process control system as a protection layer;
- requirements for hardware fault tolerance modified and should be reviewed carefully to understand user/integrator options.

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

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 the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site 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 and performance levels.

The IEC 61511 series addresses the application of SISs for the process industries. The IEC 61511 series also addresses a process Hazard and Risk Assessment (H&RA) to be carried out to enable the specification for SISs to be derived. Other safety systems' contributions are only considered with respect to the performance requirements for the SIS. The SIS includes all devices necessary to carry out each SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application: SIS safety life-cycle and safety integrity levels (SILs).

The IEC 61511 series addresses SISs which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of the IEC 61511 series should be applied to ensure the functional safety requirements are met. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. 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 principles. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. However in some instances this is not possible or not practical. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, and programmable electronic). To facilitate this approach, the IEC 61511 series:

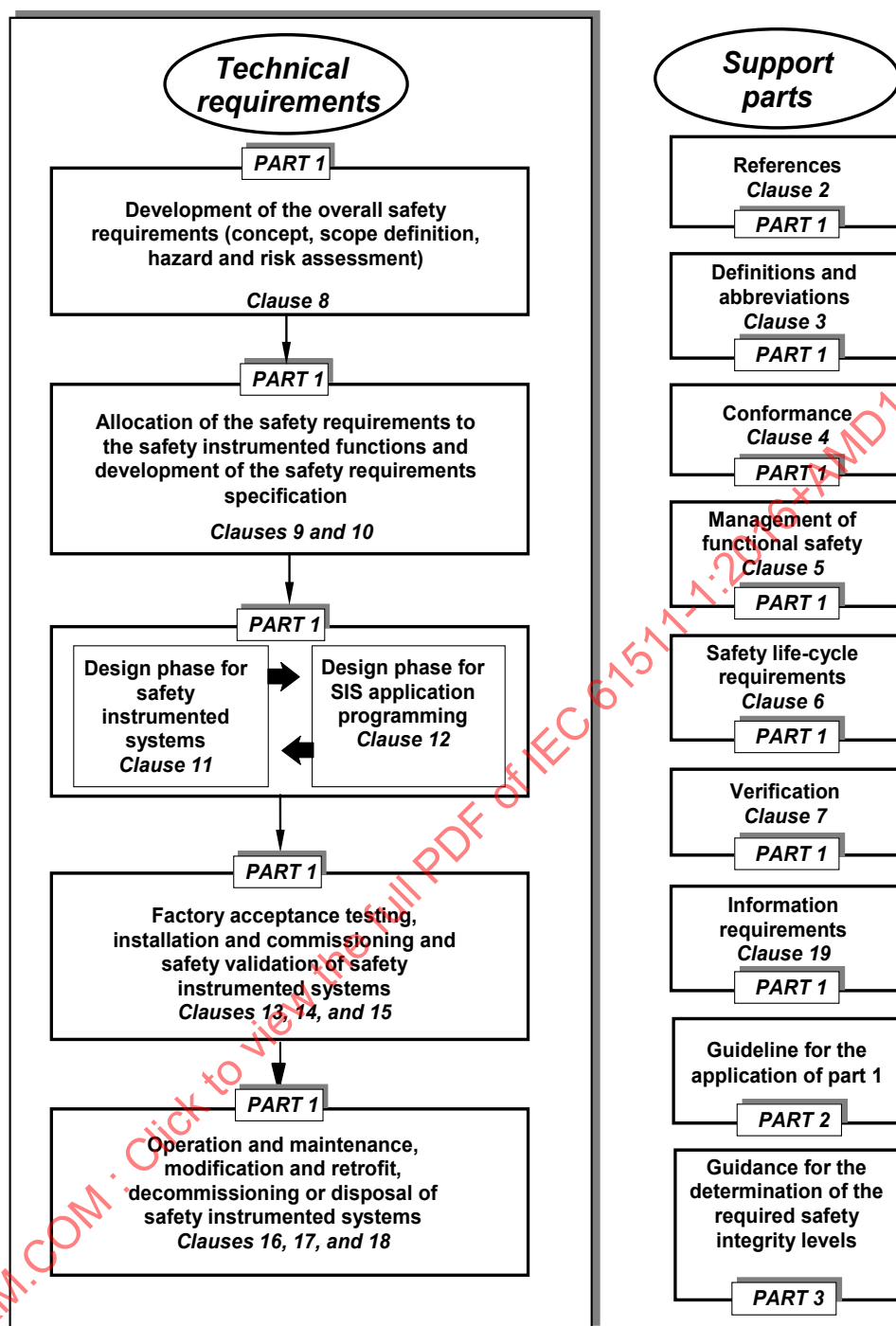
- addresses that a H&RA is carried out to identify the overall safety requirements;
- addresses that an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented means of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

The IEC 61511 series on SIS for the process industry:

- addresses all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (e.g., of underlying principles, terminology, and information) within the process industries. This should have both safety and economic benefits. Figure 1 below shows an overall framework of the IEC 61511 series.

In jurisdictions where the governing authorities (e.g., national, federal, state, province, county, city) have established process safety design, process safety management, or other regulations, these take precedence over the requirements defined in the IEC 61511 series.



IEC

Figure 1 – Overall framework of the IEC 61511 series

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

Part 1: Framework, definitions, system, hardware and application programming requirements

1 Scope

This part of IEC 61511 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve or maintain a safe state of the process. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010.

In particular, IEC 61511-1:

- a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (e.g., designers, suppliers, owner/operating company, contractor). This responsibility will be assigned to different parties according to safety planning, project planning and management, and national regulations;
- b) applies when devices that meets the requirements of the IEC 61508 series published in 2010, or IEC 61511-1:2016 [11.5], is integrated into an overall system that is to be used for a process sector application. It does not apply to manufacturers wishing to claim that devices are suitable for use in SISs for the process sector (see IEC 61508-2:2010 and IEC 61508-3:2010);
- c) defines the relationship between IEC 61511 and IEC 61508 (see Figures 2 and 3);
- d) applies when application programs are developed for systems having limited variability language or when using fixed programming language devices, but does not apply to manufacturers, SIS designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3:2010);
- e) applies to a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;

NOTE 1 Within the process sector some applications may have additional requirements that have to be satisfied.
- f) outlines the relationship between SIFs and other instrumented functions (see Figure 4);
- g) results in the identification of the functional requirements and safety integrity requirements for the SIF taking into account the risk reduction achieved by other methods;
- h) specifies life-cycle requirements for system architecture and hardware configuration, application programming, and system integration;
- i) specifies requirements for application programming for users and integrators of SISs.
- j) applies when functional safety is achieved using one or more SIFs for the protection of personnel, protection of the general public or protection of the environment;
- k) may be applied in non-safety applications for example asset protection;
- l) defines requirements for implementing SIFs as a part of the overall arrangements for achieving functional safety;
- m) uses a SIS safety life-cycle (see Figure 7) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the SIS;

- n) specifies that a H&RA is to be carried out to define the safety functional requirements and safety integrity levels (SIL) of each SIF;

NOTE 2 Figure 9 presents an overview of risk reduction means.

- o) establishes numerical targets for average probability of failure on demand (in demand mode) and average frequency of dangerous failures (in demand mode or continuous mode) for each SIL;
- p) specifies minimum requirements for hardware fault tolerance (HFT);
- q) specifies measures and techniques required for achieving the specified SIL;
- r) defines a maximum level of functional safety performance (SIL 4) which can be achieved for a SIF implemented according to IEC 61511-1;
- s) defines a minimum level of functional safety performance (SIL 1) below which IEC 61511-1 does not apply;
- t) provides a framework for establishing the SIL but does not specify the SIL required for specific applications (which should be established based on knowledge of the particular application and on the overall targeted risk reduction);
- u) specifies requirements for all parts of the SIS from sensor to final element(s);
- v) defines the information that is needed during the SIS safety life-cycle;
- w) specifies that the design of the SIS takes into account human factors;
- x) does not place any direct requirements on the individual operator or maintenance person:

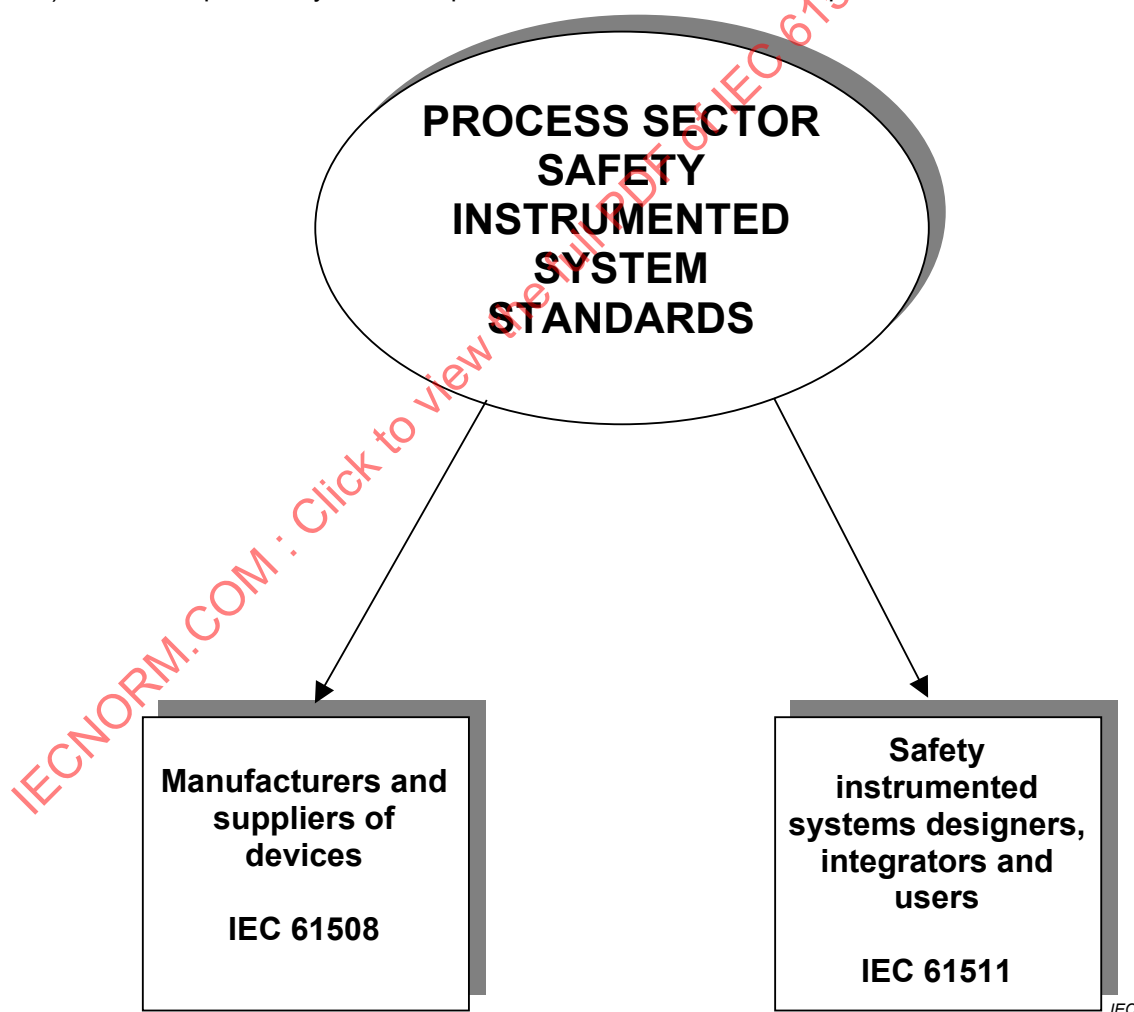


Figure 2 – Relationship between IEC 61511 and IEC 61508

NOTE 3 IEC 61508 is also used by safety instrumented designers, integrators and users where directed in IEC 61511.

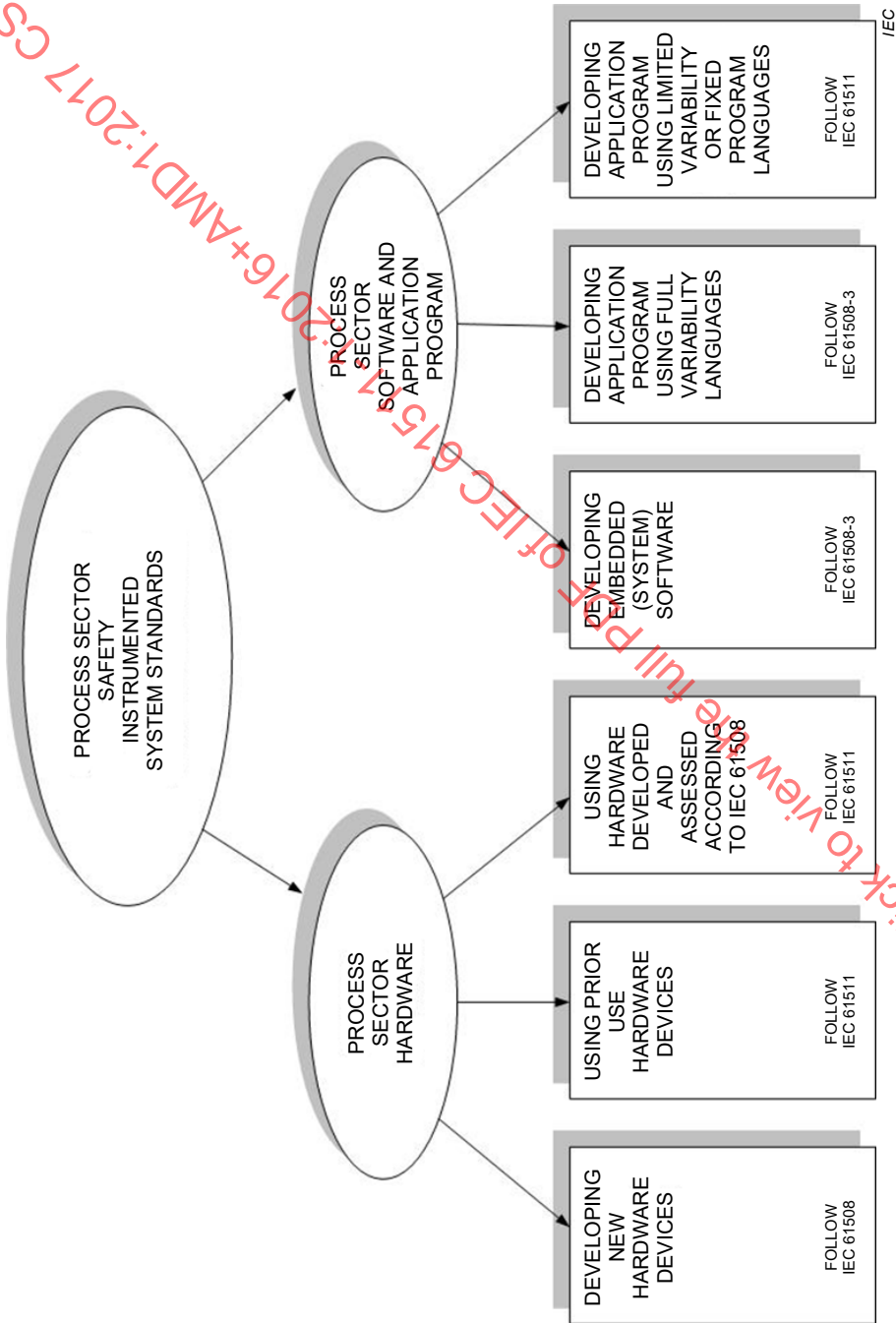
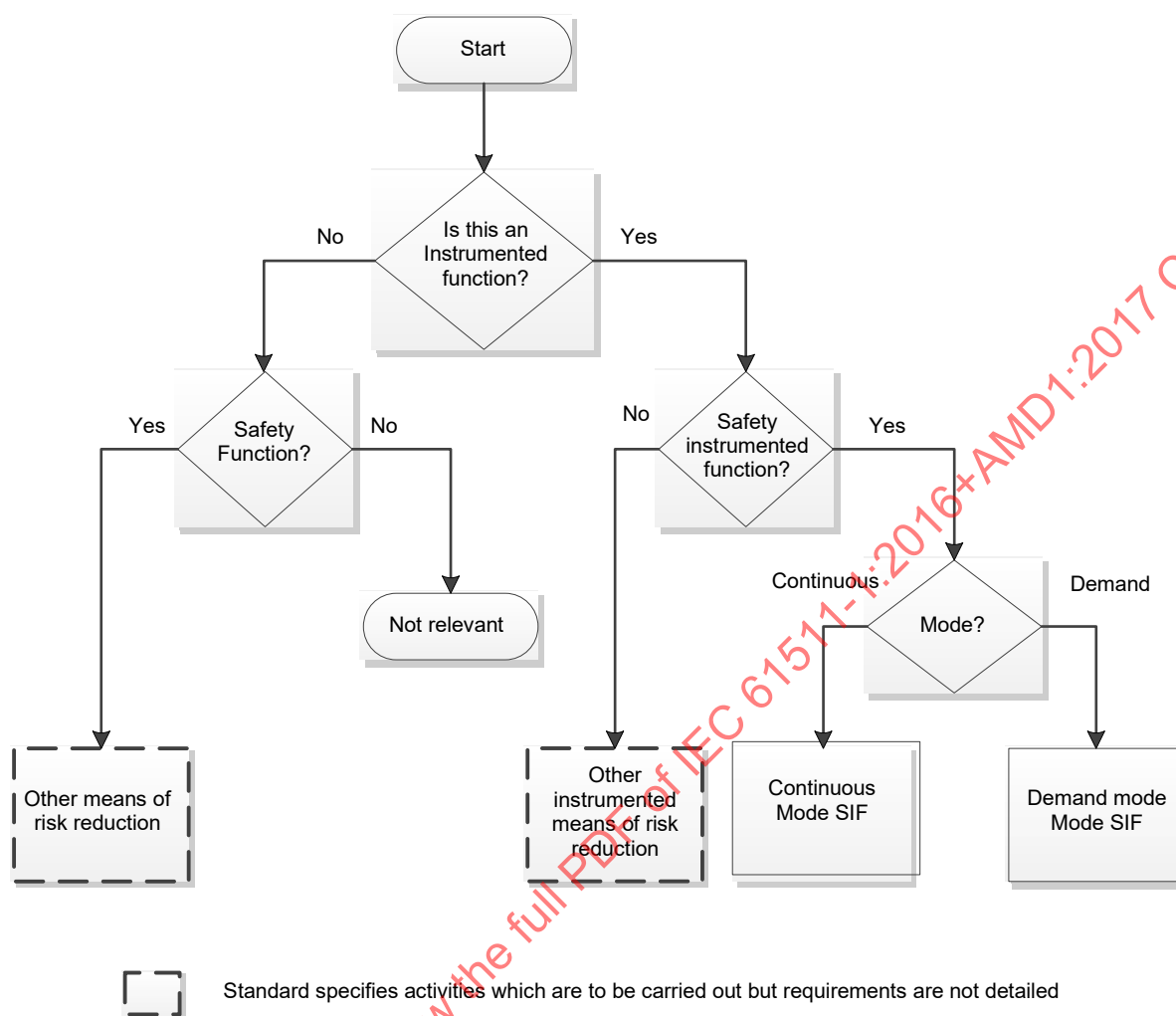


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

NOTE 4 Subclause 7.2.2 in IEC 61511-1:2016 and A.7.2.2 in IEC 61511-2:2016 contain guidance on handling integration of sub-systems that comply with other standards (such as machinery , burner, etc.).



IEC

Figure 4 – Relationship between safety instrumented functions and other functions

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 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General Requirements*

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*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

3 Terms, definitions and abbreviations

3.1 Terms

Terms are listed alphabetically in 3.2.

3.2 Terms and definitions

For the purposes of this document, the following definitions apply.

In some cases these definitions differ from the definitions of the same terms in IEC 61508-4:2010. In some cases this is due to the terminology used in the process sector. In other cases these definitions have been aligned with other relevant definitive references (e.g., IEC 60050 the International Electrotechnical Vocabulary, ISO/IEC Guide 51:2013). However, unless otherwise stated, there is no difference in the technical meaning between these definitions and the definitions of the same terms in IEC 61508-4:2010.

3.2.1

architecture configuration

specific configuration of hardware and software components in a system

Note 1 to entry: In the IEC 61511 series this can mean, for example, arrangement of SIS subsystems, the internal structure of a SIS subsystem or the internal structure of SIS application programs.

3.2.2

asset protection

function allocated to a system and designed for the purpose of preventing loss or damage to assets

3.2.3

basic process control system BPCS

system which responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any SIF

Note 1 to entry: A BPCS includes all of the devices necessary to ensure that the process operates in the desired manner.

Note 2 to entry: A BPCS typically may implement various functions such as process control functions, monitoring, and alarms.

3.2.4

bypass

action or facility to prevent all or parts of the SIS functionality from being executed

Note 1 to entry: Examples of bypassing include:

- the input signal is blocked from the trip logic while still presenting the input parameters and alarm to the operator;
- the output signal from the trip logic to a final element is held in the normal state preventing final element operation;
- a physical bypass line is provided around the final element;
- preselected input state (e.g., on/off input) or set is forced by means of an engineering tool (e.g., in the application program).

Note 2 to entry: Other terms are also used to refer to bypassing, such as override, defeat, disable, force, or inhibit or muting.

3.2.5

channel

device or group of devices that independently perform(s) a specified function

Note 1 to entry: The devices within a channel could include input/output (I/O) devices, logic solvers, sensors, and final elements.

Note 2 to entry: A dual channel (i.e., a two-channel) configuration is one with two channels that independently perform the same function. Channels may be identical or diverse.

Note 3 to entry: The term can be used to describe a complete system or a portion of a system (e.g., sensors or final elements).

Note 4 to entry: Channel describes SIS hardware architectural features often used to meet hardware fault tolerance requirements.

3.2.6 common cause

3.2.6.1

common cause failures, pl

concurrent failures of different devices, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: All the failures due to a common cause do not necessarily occur exactly at the same time and this may allow time to detect the occurrence of the common cause before a SIF is actually failed.

Note 2 to entry: Common cause failures can also lead to common mode failures.

Note 3 to entry: The potential for common cause failures reduces the effect of system redundancy or fault tolerance (e.g., increases the probability of failure of two or more channels in a multiple channel system).

Note 4 to entry: Common cause failures are dependent failures. They may be due to external events (e.g., temperature, humidity, overvoltage, fire, and corrosion), systematic fault (e.g., design, assembly or installation errors, bugs), human error (e.g., misuse), etc.

Note 5 to entry: By extension, a common cause failure (in singular form) is a failure belonging to a set of concurrent failures (plural form) according to 3.2.6.1 definition.

3.2.6.2

common mode failures, pl

concurrent failures of different devices characterized by the same failure mode (i.e., identical faults)

Note 1 to entry: Common mode failures may have different causes.

Note 2 to entry: Common mode failures can also be the result of common cause failures (3.2.6.1).

Note 3 to entry: The potential for common mode failures reduces the effectiveness of system redundancy and fault tolerance (e.g., failure of two or more channels in the same way, causing the same erroneous result).

Note 4 to entry: By extension, a common mode failure (in singular form) is a failure belonging to a set of concurrent failures (plural form) according to 3.2.6.2 definition.

3.2.7

compensating measure

temporary implementation of planned and documented methods for managing risks during any period of maintenance or process operation when it is known that the performance of the SIS is degraded

3.2.8

component

one of the parts of a system, SIS subsystem, or device performing a specified function

Note 1 to entry: Component may also include software.

3.2.9 configuration management

discipline of identifying the components and the arrangements of those components of an evolving system for the purposes of controlling changes to those components, and maintaining continuity of the system and traceability of any changes throughout the life-cycle

3.2.9.1 conservative approach

cautious way of doing analysis and calculations

Note 1 to entry: In the safety field, each time an analysis, assumptions, or calculation has to be done (about models, input data, computations, etc.) it can be chosen in order to be sure to produce pessimistic results.

3.2.10 control system

system which responds to input signals from the process and/or from an operator and generates output signals causing the process to operate in the desired manner

Note 1 to entry: The control system includes sensors and final elements and may be either a BPCS or a SIS or a combination of the two.

3.2.11 dangerous failure

failure which impedes or disables a given safety action

Note 1 to entry: A failure is "dangerous" only with regard to a given SIF.

Note 2 to entry: When fault tolerance is implemented, a dangerous failure can lead to either:

- a degraded SIF where the safety action is available, but there is either a higher PFD ~~(demand mode of operation)~~ or a higher likelihood of initiating a hazardous event ~~(continuous mode of operation)~~ or a PFH, or
- a disabled SIF where the safety action is completely disabled ~~(demand mode of operation)~~ or the hazardous event has been induced ~~(continuous mode of operation)~~.

Note 3 to entry: When no fault tolerance is implemented, all dangerous failures lead to a disabled SIF.

3.2.12 dependent failure

failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it

Note 1 to entry: Two events A and B are dependent if the probability of occurrence of A and B, $P(A \text{ and } B)$, is greater than $P(A) \times P(B)$.

Note 2 to entry: See 9.4.2 and IEC 61511-3:2016, Annex J for consideration of dependent failures between protection layers.

Note 3 to entry: Dependent failures include common cause.

3.2.13 detected revealed overt

relating to hardware and software failures or faults which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods

Note 1 to entry: There are some differences in the use of these terms:

- Overt is used for failures or faults which announce themselves when they occur (e.g., due to the change of state). The repair of such failures can begin as soon as they have occurred.
- Detected is used for failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, operator intervention like physical inspection and manual tests). The repair of such failures can begin only after they have been revealed. See Note 2 for the specific use of this term in IEC 61511.

- Revealed is used for failures or faults that become evident due to being overt or as a result of being detected.

Note 2 to entry: In IEC 61511 and except when the context suggests another meaning, the term *dangerous detected failures/faults* is related to dangerous failures detected by diagnostic tests.

Note 3 to entry: When the detection is very fast (e.g., by diagnostic tests) then the detected failures or faults can be considered to be overt failures or faults.

When the detection is not very fast (e.g., by proof tests) the detected failures or faults cannot be considered to be overt failures or faults when addressing safety integrity levels.

Note 4 to entry: A dangerous revealed failure can only be treated as a safe failure if effective measures, automatic or manual, are taken in a short enough time to maintain process safety.

3.2.14 device

hardware, with or without software, capable of performing a specified function

Note 1 to entry: Examples are sensors, logic solvers, final elements, operator interfaces, and field wiring.

3.2.14.1 field device

SIS or BPCS device connected directly to the process or located in close proximity to the process

Note 1 to entry: Examples are sensors, final elements and manual switches.

3.2.15 diagnostics

frequent (in relation to the process safety time) automatic test to reveal faults

3.2.15.1 diagnostics coverage

DC

fraction of dangerous failures rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof tests

Note 1 to entry: Diagnostics coverage is typically applied to SIS devices or SIS subsystems. E.g., the diagnostics coverage is typically determined for a sensor, final element or a logic solver.

Note 2 to entry: For safety applications the diagnostics coverage is typically applied to dangerous failures of SIS devices or SIS subsystems. For example, the diagnostics coverage for the dangerous failures of a device is $DC = \lambda_{DD} / \lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate. For a SIS subsystem with internal redundancy, DC is time dependant: $DC(t) = \lambda_{DD}(t) / \lambda_{DT}(t)$.

Note 3 to entry: When the diagnostics coverage (DC) and the total dangerous failure rate (λ_{DT}) are given, the detected (λ_{DD}) and undetected dangerous failures rates (λ_{DU}) can be computed as follows:

$$\lambda_{DD} = DC \times \lambda_{DT} \text{ and } \lambda_{DU} = (1-DC) \times \lambda_{DT}.$$

3.2.16 diversity

different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical means, different programming techniques, or different design approaches.

3.2.17 error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.2.18

failure

loss of ability to perform as required

Note 1 to entry: A failure of a device is an event that results in a fault state of that device.

Note 2 to entry: When the loss of ability is caused by a latent fault, the failure occurs when a particular set of circumstances is encountered.

Note 3 to entry: Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

Note 4 to entry: Failures are either random or systematic (~~see 3.2.61 and 3.2.83~~ see 3.2.59 and 3.2.81).

[SOURCE: IEC 60050-192:2015, 192-03-01, modified – Notes to entry have been changed]

3.2.18.1

failure mode

manner in which failure occurs

Note 1 to entry: A failure mode may be defined by the function lost or the state transition that occurred.

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.2.19

fault

inability to perform as required, due to an internal state

Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life-cycle, such as specification, design, manufacture or maintenance.

Note 2 to entry: A fault of a device results in a failure when a particular set of circumstances is encountered.

[SOURCE: IEC 60050-192:2015, 192-04-01, modified – Some notes to entry have been changed, others have been deleted]

3.2.20

fault avoidance

use of techniques and procedures which aim to avoid the introduction of faults during any phase of the SIS safety life-cycle

3.2.20.1

fault exclusion

elimination from further consideration of faults due to improbable failure modes

Note 1 to entry: Further information about fault exclusion can be found in ISO 13849-1 and ISO 13849-2. After those standards fault exclusion can be based on

- the technical improbability of occurrence of some faults,
- generally accepted technical experience, independent of the considered application;
- technical requirements related to the application and the specific hazard.

Note 2 to entry: Failure modes, identified in the devices performing the safety function, can be excluded because their related dangerous failure rate(s) are very low compared to the target failure measure for the safety function under consideration. That is, the sum of the dangerous failure rates of all serial devices on which fault exclusion is being claimed, generally cannot exceed more than 1 % of the target failure measure.

3.2.21

fault tolerance

ability of a functional item to continue to perform a required function in the presence of faults or errors

3.2.22 final element

part of the BPCS or SIS that implements the physical action necessary to achieve or maintain a safe state

Note 1 to entry: Examples are valves, switch gear, and motors, including their auxiliary elements (such as solenoid valve and actuator used to operate a valve).

3.2.23 functional safety

part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers

3.2.24 functional safety assessment FSA

investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers

3.2.25 functional safety audit

systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

Note 1 to entry: A functional safety audit may be carried out as part of a FSA.

3.2.26 hardware safety integrity

part of the safety integrity of the SIS relating to random hardware failures in a dangerous mode of failure

Note 1 to entry: The two failure measures that are relevant in this context are the average frequency of dangerous failure ~~(continuous mode of operation)~~ and the average probability of failure on demand ~~(demand mode of operation)~~.

Note 2 to entry: See 3.2.82.

Note 3 to entry: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.27 harm

injury or damage to the health of people, or damage to property or to the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.2.27.1 harmful event

hazardous event which has caused harm

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property, or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred. A hazardous event which has caused harm is termed a harmful event.

3.2.28 hazard

potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (e.g., fire and explosion) and also those that have a long-term effect on a person's health (e.g., release of a toxic substance or radioactivity).

[SOURCE: ISO/IEC Guide 51:2014, 3.2, modified – Note 1 to entry has been added]

3.2.28.1

hazardous event

event that can cause harm

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

[SOURCE: ISO/IEC Guide 51:2014: 3.3, modified – see Note 1]

3.2.28.2

hazardous situation

circumstance in which people, property or the environment are exposed to one or more hazards

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.2.29

human error

intended or unintended human action or inaction that produces an inappropriate result

Note 1 to entry: Mistakes, slips, and lapses are examples of human errors.

Note 2 to entry: This excludes malicious action.

3.2.30

impact analysis

activity of determining the effect that a change to a function or component will have to other functions or components in the system as well as in other systems

3.2.31

independent organization

organization that is separate and distinct, by management and other resources, from the organizations responsible for the activities that take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation

3.2.32

independent person

person who is separate and distinct from the activities which take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation and does not have direct responsibility for those activities

3.2.33

input function

function which monitors the process and its associated equipment in order to provide input information for the logic solver

Note 1 to entry: An input function could be a manual function.

3.2.34

instrument

apparatus used in performing an action (typically found in instrumented systems)

3.2.34.1

instrumented system

system composed of sensors (e.g., pressure, flow, temperature transmitters), logic solvers (e.g., programmable controllers, distributed control systems, discrete controllers), and final elements (e.g., control valves, motor control circuits)

Note 1 to entry: Instrumented systems perform instrumented functions including control, monitoring, alarm and protective functions. Instrumented systems can be SIS (see 3.2.67) or BPCS (see 3.2.3).

3.2.35 **logic function**

function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions)

Note 1 to entry: Logic functions provide the transformation from one or more input functions to one or more output functions.

Note 2 to entry: For further guidance, see IEC 61131-3:2012 and IEC 60617-12:1997.

3.2.36 **logic solver**

part of either a BPCS or SIS that performs one or more logic function(s)

Note 1 to entry: In IEC 61511 the following terms for logic solvers are used:

- electrical logic systems for electro-mechanical technology;
- electronic logic systems for electronic technology;
- PE logic system for programmable electronic systems.

Note 2 to entry: Examples are: electrical systems, electronic systems, programmable electronic systems, pneumatic systems, and hydraulic systems. Sensors and final elements are not part of the logic solver.

3.2.36.1 **safety configured PE logic solver**

general purpose industrial grade PE logic solver which is specifically configured for use in safety applications

Note 1 to entry: Further guidance can be found in 11.5.

3.2.37 **maintenance/engineering interface**

hardware and software provided to allow proper SIS maintenance or modification

Note 1 to entry: Maintenance/engineering interface can include instructions and diagnostics which may be found in software, programming terminals with appropriate communication protocols, diagnostic tools, indicators, bypass devices, test devices, and calibration devices.

3.2.37.1 **mean repair time** **MRT**

expected overall repair time

Note 1 to entry: MRT encompasses the times (b), (c) and (d) of the times for MTTR (see 3.2.37.2).

3.2.37.2 **mean time to restoration** **MTTR**

expected time to achieve restoration

Note 1 to entry: MTTR encompasses:

- the time to detect the failure (a);
- the time spent before starting the repair (b);
- the effective time to repair (c);
- the time before the component is put back into operation (d).

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

3.2.37.3 **maximum permitted repair time** **MPRT**

maximum duration allowed to repair a fault after it has been detected

Note 1 to entry: The MRT may be used as MPRT but the MPRT may be defined without regards to the MRT:

- A MPRT smaller than the MRT can be chosen to decrease the probability of hazardous event.
- A MPRT greater than the MRT can be chosen if the probability of hazardous event can be relaxed.

Note 2 to entry: When a MPRT has been defined it can be used in place of the MRT for calculating the probability of random hardware failures.

3.2.38

mitigation

action that reduces the consequence(s) of a hazardous event

Note 1 to entry: Examples include emergency depressurization or closing ventilation dampers on detection or confirmed fire or gas leak or initiation of deluge on confirmed fire detection.

3.2.39

mode of operation (of a SIF)

way in which a SIF operates which may be either low demand mode, high demand mode or continuous mode

- a) **low demand mode:** mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year.
- b) **high demand mode:** mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year.
- c) **continuous mode:** mode of operation where the SIF retains the process in a safe state as part of normal operation.

3.2.39.1

demand mode SIF

SIF operating in low demand mode (3.2.39 a)) or high demand mode (3.2.39 b))

Note 1 to entry: In the event of a dangerous failure of the SIF, a hazardous event can only occur

- if the failure is undetected and a demand occurs before the next proof test;
- if the failure is detected by the diagnostic tests but the related process and its associated equipment has not been moved to a safe state before a demand occurs.

Note 2 to entry: In high demand mode, it will normally be appropriate to use the continuous mode criteria.

Note 3 to entry: The safety integrity levels for SIF operating in demand mode are defined in Tables 4 and 5.

3.2.39.2

continuous mode SIF

SIF operating in continuous mode (3.2.39 c))

Note 1 to entry: In the event of a dangerous failure of the SIF a hazardous event will occur without further failure unless action is taken to prevent it within the process safety time.

Note 2 to entry: Continuous mode covers those SIF which implement continuous control to maintain functional safety.

Note 3 to entry: The safety integrity levels for SIF operating in continuous mode are defined in Table 5.

3.2.40

module

self-contained part of a SIS application program (can be internal to a program or a set of programs) that performs a specified function (e.g., final element start/stop/test sequence, an application specific sequence within a SIF)

Note 1 to entry: In the context of IEC 61131-3:2012, a software module is a function or function block.

Note 2 to entry: Most modules have repetitive usage within an application program.

3.2.41

MooN

SIS, or part thereof, made up of “ N ” independent channels, which are so connected, that “ M ” channels are sufficient to perform the SIF

3.2.42

necessary risk reduction

risk reduction to be achieved by the SIS(s) and/or other protection layers to ensure that the tolerable risk is not exceeded

3.2.43

non-programmable system (NP) system

system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software)

Note 1 to entry: Examples would include hard-wired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

3.2.44

operating environment

conditions inherent to the installation of a device that potentially affects its functionality and safety integrity, such as:

- external environment, e.g. , winterization needs, hazardous area classification;
- process operating conditions, e.g., extremes in temperature, pressure, vibration;
- process composition, e.g., solids, salts, or corrosives;
- process interfaces;
- integration within the overall plant maintenance and operating management systems;
- communication through-put, e.g., electro-magnetic interference; and
- utility quality, e.g., electrical power, air, hydraulics.

Note 1 to entry: Some process applications may have special operating environment requirements necessary to survive a major accident event. For example some equipment requires special enclosures, purging, or fire protection.

3.2.45

operating mode

process operating mode

any planned state of process operation, including modes such as start-up after emergency shutdown, normal start-up, operation, and shutdown, temporary operations, and emergency operation and shutdown

3.2.46

operator interface

means by which information is communicated between a human operator and the SIS (e.g., display interfaces, indicating lights, push-buttons, horns, alarms)

Note 1 to entry: The operator interface is sometimes referred to as the human-machine interface (HMI).

3.2.47

output function

function which controls the process and its associated equipment according to output information from the logic function

3.2.48

performance

accomplishment of a given action or task measured against the specification and the IEC 61511 series

3.2.49

phase

period within the SIS safety life-cycle where activities described in the IEC 61511 series take place

3.2.50

prevention

action that reduces the likelihood of occurrence of a hazardous event

3.2.51

prior use

documented assessment by a user that a device is suitable for use in a SIS and can meet the required functional and safety integrity requirements, based on previous operating experience in similar operating environments

Note 1 to entry: To qualify a SIS device on the basis of prior use, the user can document that the device has achieved satisfactory performance in a similar operating environment. Understanding how the equipment behaves in the operating environment is necessary to achieve a high degree of certainty that the planned design, inspection, testing, maintenance, and operational practices are sufficient.

Note 2 to entry: Proven in use is based on the manufacturer's design basis (e.g., temperature limit, vibration limit, corrosion limit, desired maintenance support) for his device. Prior use deals with device's installed performance within a process sector application in a specific operating environment which is often different than the manufacturer's design basis.

3.2.52

process risk

risk arising from the process conditions caused by abnormal events (including BPCS malfunction)

Note 1 to entry: The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e., the risk associated with functional safety).

Note 2 to entry: Process risk analysis is described in IEC 61511-3:2016. The main purpose of determining the process risk is to establish a reference point for the risk without taking into account the protection layers.

Note 3 to entry: Assessment of this risk can include associated human factor issues.

Note 4 to entry: This term equates to "EUC risk" in IEC 61508-4:2010.

3.2.52.1

process safety time

time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed

Note 1 to entry: This is a property of the process only. The SIF has to detect the failure and complete its action soon enough to prevent the hazardous event taking into account any process lag (e.g. cooling of a vessel).

3.2.53

programmable electronics

PE

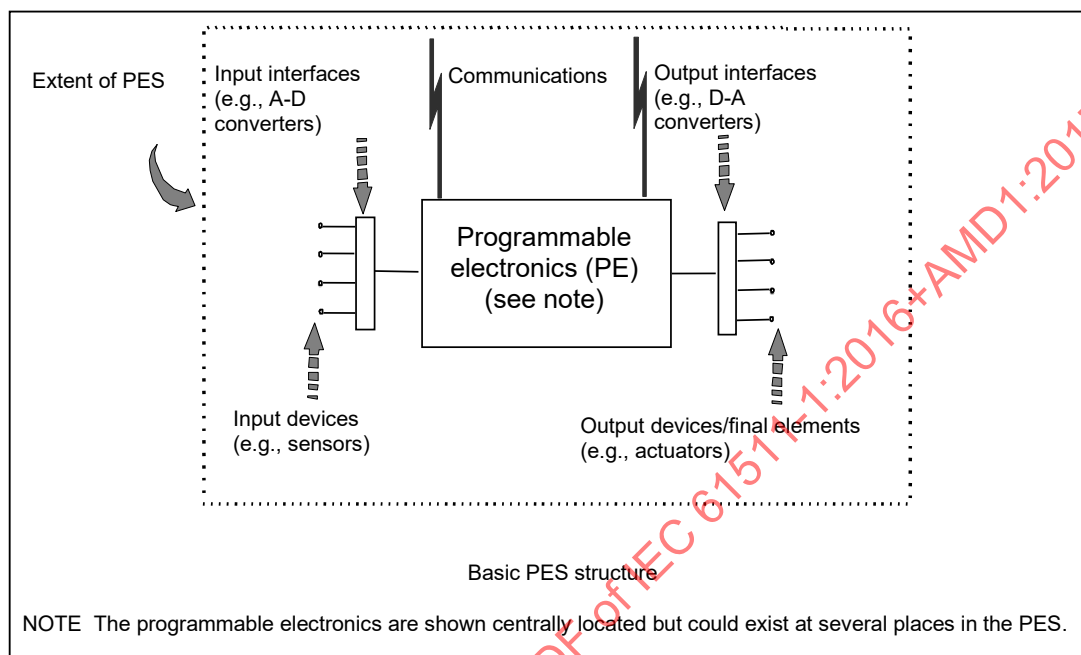
item based on computer technology which may be comprised of hardware, software, and of input and/or output units

Note 1 to entry: This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories. Examples of process sector programmable electronics include:

- smart sensors and final elements;
- programmable electronic logic solvers including:
 - programmable controllers;
 - programmable logic controllers;
 - loop controllers.

3.2.54 programmable electronic system PES

system for control, protection or monitoring based on one or more programmable electronic devices, including all devices of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices (see Figure 5)



IEC

Figure 5 – Programmable electronic system (PES): structure and terminology

3.2.55 programming coding

process of designing, writing and testing a set of instructions for solving a problem or processing data

Note 1 to entry: In the IEC 61511 series, programming is typically associated with PE.

3.2.56 proof test

periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition

3.2.57 protection layer

any independent mechanism that reduces risk by control, prevention or mitigation

Note 1 to entry: It can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical mechanism such as a relief valve, a SIS or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions (see Figure 9).

3.2.58 quality

totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs

Note 1 to entry: See ISO 9000 for more details.

3.2.59

random hardware failure

failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e., random) times.

Note 2 to entry: Two major differences distinguish the random hardware failures and the systematic failures:

- a random hardware failure involves only the system itself while a systematic failure involves both the system itself (a fault) and a particular condition (see 3.2.81). Then a random hardware failure is characterized by a single reliability parameter (i.e., the failure rate) while a systematic failure is characterized by two reliability parameters (i.e., the probability of the pre-existing fault and the hazard rate of the particular condition).
- a systematic failure can be eliminated after being detected while random hardware failures cannot.

This implies that the reliability parameters of random hardware failures can be estimated from field feedback while it is very difficult to do the same for systematic failures. A qualitative approach is preferred for systematic failures.

[SOURCE: IEC 61508-4:2010, 3.6.5, modified – The notes have been changed]

3.2.60

redundancy

the existence of more than one means for performing a required function or for representing information

Note 1 to entry: Examples are the use of duplicate devices and the addition of parity bits.

Note 2 to entry: Redundancy is used primarily to improve reliability or availability.

[SOURCE: IEC 61508-4:2010, 3.4.6]

3.2.61

risk

combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation, the occurrence of a hazardous event, and the possibility to avoid or limit the harm.

[SOURCE: ISO/IEC Guide 51:2014, 3.8]

3.2.62

safe failure

failure which favours a given safety action

Note 1 to entry: A failure is "safe" only with regard to a given safety function.

Note 2 to entry: When fault tolerance is implemented, safe failure can lead to either:

- operation where the safety action is available but with a higher probability of success on demand (~~demand mode of operation~~) or a lower likelihood to cause a hazardous event (~~continuous mode of operation~~);
- a spurious operation where the safety action is initiated.

Note 3 to entry: When no fault tolerance is implemented, safe failures result in the initiation of the safety action regardless of the process condition. This is also known as a spurious trip.

Note 4 to entry: A spurious trip may be safe with regard to a given safety function but may be dangerous with regard to another safety function.

Note 5 to entry: Spurious trips may also have detrimental effects on the production availability of the process.

3.2.63

safe state

state of the process when safety is achieved

Note 1 to entry: Some states are safer than others and in going from a hazardous condition to the final safe state, or in going from the nominal safe condition to a hazardous condition, the process may have to go through a number of intermediate safe-states.

Note 2 to entry: For some situations, a safe state exists only so long as the process is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

Note 3 to entry: A state which is safe with regard to a given safety function may increase the probability of hazardous event with regard to another given safety function. In this case, the maximum allowable average spurious trip frequency (see 10.3.2) for the first function can consider the potential increased risk associated with the other function.

Note 4 to entry: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.64

safety

freedom from risk which is not tolerable

Note 1 to entry: According to ISO/IEC Guide 51 the terms "acceptable risk" and "tolerable risk" are considered to be synonymous.

[SOURCE: ISO/IEC Guide 51:2014, 3.14, modified – The note has been added]

3.2.65

safety function

function to be implemented by one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

3.2.66

safety instrumented function

SIF

safety function to be implemented by a safety instrumented system (SIS)

Note 1 to entry: A SIF is designed to achieve a required SIL which is determined in relationship with the other protection layers participating to the reduction of the same risk.

3.2.67

safety instrumented system

SIS

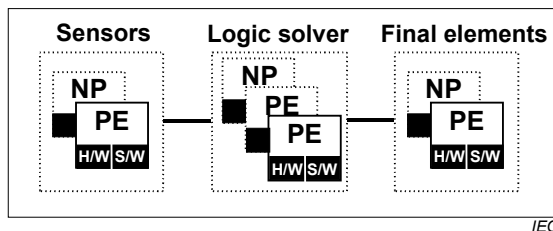
instrumented system used to implement one or more SIFs

Note 1 to entry: A SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s) (e.g., see Figure 6). It also includes communication and ancillary equipment (e.g., cables, tubing, power supply, impulse lines, heat tracing).

Note 2 to entry: A SIS may include software.

Note 3 to entry: A SIS may include human action as part of a SIF (see ISA TR84.00.04:2015, part 1).

SIS architecture and safety instrumented function example with different devices shown



IEC

Figure 6 – Example of SIS architectures comprising three SIS subsystems

3.2.68

safety integrity

ability of the SIS to perform the required SIF as and when required

Note 1 to entry: This definition is equivalent to the dependability of the SIS with regard to the required SIF. Dependability, being often understood as an economical rather than a safety concept, has not been used to avoid confusion.

Note 2 to entry: Ability includes both the functional response (e.g., closing a specified valve within a specified time) and the likelihood that the SIS will act as required.

Note 3 to entry: In determining safety integrity, all causes of random hardware and systematic failures which lead to an unsafe state can be included (e.g., hardware failures, software induced failures and failures due to electrical interferences). Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the average dangerous failure frequency or the probability of failure on demand. However, safety integrity also depends on many systematic factors, which cannot be accurately quantified and are often considered qualitatively throughout the life-cycle. The likelihood that systematic failures result in dangerous failure of the SIS is reduced through hardware fault tolerance (see 11.4) or other methods and techniques.

Note 4 to entry: Safety integrity comprises hardware safety integrity (see 3.2.26) and systematic safety integrity (see 3.2.82), but complex failures caused by the conjunction of both hardware and systematic interaction can also be considered.

3.2.69

safety integrity level

SIL

discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS

Note 1 to entry: The higher the SIL, the lower the expected PFD_{avg} ~~for demand mode or~~ the lower the average frequency of a dangerous failure causing a hazardous event ~~for continuous mode~~.

Note 2 to entry: The relationship between the target failure measure and the SIL is specified in Tables 4 and 5.

Note 3 to entry: SIL 4 is related to the highest level of safety integrity; SIL 1 is related to the lowest

Note 4 to entry: This definition differs from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.69.1

safety integrity requirements, pl

set of the IEC 61511 requirements which shall be satisfied by a SIS to claim a given SIL for a SIF implemented by this SIS

Note 1 to entry: The safety integrity requirements are strengthened when the related SIL increases.

3.2.70

SIS safety life-cycle

necessary activities involved in the implementation of SIF occurring during a period of time that starts at the concept phase of a project and finishes when all of the SIF are no longer available for use

Note 1 to entry: The term “functional safety life-cycle” is strictly more accurate, but the adjective “functional” is not considered necessary in this case within the context of the IEC 61511 series.

Note 2 to entry: The SIS safety life-cycle model used in IEC 61511 is shown in Figure 7.

3.2.71

safety manual

functional safety manual

information that defines how a SIS device, subsystem or system can be safely applied

Note 1 to entry: The safety manual may include inputs from the manufacturer as well as from the user.

Note 2 to entry: For IEC 61508 compliant devices, the manufacturer's input is the safety manual,

Note 3 to entry: This could be a generic stand-alone document, or a collection of documents.

Note 4 to entry: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.72 **safety requirements specification** **SRS**

specification containing the functional requirements for the SIFs and their associated safety integrity levels

[SOURCE: IEC 61508-4:2010, 3.5.11, modified – Aligned with IEC 61511 terminology]

3.2.73 **sensor**

part of the BPCS or SIS that measures or detects the process condition

Note 1 to entry: Examples are transmitters, transducers, process switches, and position switches.

3.2.74 **software**

programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

Note 1 to entry: Software is independent of the medium on which it is recorded.

Note 2 to entry: For examples of different types of software, see 3.2.75 and 3.2.76.

3.2.75 **application programming languages**

3.2.75.1 **fixed program language** **FPL**

language in which the user is limited to adjustment of a few pre-defined and fixed set of parameters

Note 1 to entry: Typical examples of device applications with FPL are: smart sensor (e.g., pressure transmitter without control algorithms), smart final element (e.g. valve without control algorithms), sequence of events recorder, set points for dedicated smart alarm box). The use of FPL is often referred to as "configuration of the device".

3.2.75.2 **limited variability language** **LVL**

programming language for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application as defined by the associated safety manual. The notation of this language may be textual or graphical or have characteristics of both.

Note 1 to entry: This type of language is designed to be easily understood by process sector users, and provides the capability to combine predefined, application specific, library functions to implement the SRS. LVL provides a close functional correspondence with the functions required to achieve the application.

Note 2 to entry: IEC 61511 assumes that the constraints necessary to achieve the safety properties are achieved by the combination of the safety manual, the closeness of the language notations to the functions the application programmer needs to define the process control algorithms, and the compile time and run time checks which the logic solver provider embeds into the logic solver system program and the logic solver development environment. The constraints identified in the certification report and safety manual can ensure the relevant requirements of IEC 61508-3:2010 are satisfied.

Note 3 to entry: LVL is the most commonly used language when the IEC 61511 series refers to "application program".

3.2.75.3 **full variability language** **FVL**

language designed to be comprehensible to computer programmers and that provides the capability to implement a wide variety of functions and applications

Note 1 to entry: Typical example of systems using FVL are general purpose computers.

Note 2 to entry: In the process sector, FVL is found in embedded software and rarely in application programming.

Note 3 to entry: FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

3.2.76 software & program types

3.2.76.1 application program

program specific to the user application containing, in general, logic sequences, permissives, limits and expressions that control the input, output, calculations, and decisions necessary to meet the SIS functional requirements

3.2.76.2 embedded software

software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user

Note 1 to entry: Embedded software is also referred to as firmware or system software. See 3.2.75.3 full variability language.

3.2.76.3 utility software

software tools for the creation, modification, and documentation of application programs

Note 1 to entry: These software tools are not required for the operation of the SIS.

3.2.77 application program life-cycle

activities occurring during a period of time that starts when the application program is conceived and ends when the application program is permanently disused

Note 1 to entry: An application program life-cycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and modification phase.

Note 2 to entry: Software, including application program, cannot be maintained; rather, it is modified.

3.2.78 SIS subsystem

independent part of a SIS whose disabling dangerous failure results in a disabling dangerous failure of the SIS

Note 1 to entry: Figure 6 illustrates a SIS made of three SIS subsystems.

Note 2 to entry: From the cut set approach point of view (see IEC 61025) a minimal cut set of a SIS subsystem is also a minimal cut set of the whole SIS. Therefore the SIFs implemented within a SIS are entirely dependent on the SIS subsystems of this SIS (i.e., when a SIS subsystem fails, the related SIFs also fail).

3.2.79 system

set of devices, which interact according to a specification

Note 1 to entry: A person can be part of a system.

Note 2 to entry: This definition deviates from the definition in IEC 61508 to reflect differences in process sector terminology.

3.2.80 systematic capability

measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual

Note 1 to entry: Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults in IEC 61508-2:2010 and IEC 61508-3:2010.

Note 2 to entry: The systematic failure mechanism depends on the nature of the device. For a device comprised solely of hardware, only hardware failure mechanisms are considered. For a device comprised of hardware and software, it is necessary to consider the interactions between hardware and software failure mechanisms.

Note 3 to entry: A systematic capability of SC N for a device means that the systematic safety integrity of SC N has been met when the device is applied in accordance with the instructions specified in the device safety manual for SC N.

3.2.81

systematic failure

failure related to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors.

Note 1 to entry: The cause of systematic failures of the software may be known as "bugs".

Note 2 to entry: Corrective maintenance without modification would usually not eliminate the failure cause which involves the failure under particular conditions.

Note 3 to entry: A systematic failure can be reproduced by deliberately applying the same conditions, although not all reproducible failures are systematic.

Note 4 to entry: Examples of faults leading to systematic failure include human error that originates in:

- the SRS;
- the design, manufacture, installation, operation or maintenance of the hardware;
- the design or implementation of software (including application program).

Note 5 to entry: Similar devices designed, installed, operated, implemented or maintained in the same way are likely to contain the same faults. Therefore they are subject to common cause failures when the particular conditions occur.

3.2.82

systematic safety integrity

part of the safety integrity of the SIS relating to systematic failures in a dangerous mode of failure

Note 1 to entry: Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity).

Note 2 to entry: See 3.2.26 also.

3.2.83

target failure measure

performance required from the SIF and specified in terms of either the average probability of failure to perform the SIF on demand for demand mode of operation or the average frequency of a dangerous failure for continuous mode of operation

Note 1 to entry: The relationship between the target failure measures and the SIL are given in Tables 4 and 5.

3.2.84

tolerable risk

level of risk which is accepted in a given context based on the current values of society

Note 1 to entry: See IEC 61511-3:2016, Annex A.

[SOURCE: ISO/IEC Guide 51:2014, 3.15]

3.2.85

undetected unrevealed covert

not detected or not revealed or not overt

Note 1 to entry: In IEC 61511 and except when the context suggests another meaning, the term “dangerous undetected failures/faults” is related to dangerous failures/faults not detected by diagnostic tests.

3.2.86

validation

confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: In the IEC 61511 series this means demonstrating that the SIF(s) and SIS after installation meet the SRS in all respects.

3.2.87

verification

confirmation by examination and provision of objective evidence that the requirements have been fulfilled

Note 1 to entry: In the IEC 61511 series this is the activity of demonstrating for each phase of the relevant SIS safety life-cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

Note 2 to entry: Example verification activities include:

- reviews on outputs (documents from all phases of the safety life-cycle) to ensure compliance with the objectives and requirements of the phase taking into account the specific inputs to that phase;
- design reviews;
- tests performed on the designed products to ensure that they perform according to their specification;
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

3.2.88

watchdog

combination of diagnostics and an output device (typically a switch) for monitoring the correct operation of the programmable electronic (PE) device and taking action upon detection of an incorrect operation

Note 1 to entry: The watchdog confirms that the software system is operating correctly by the regular resetting of an external device (e.g., hardware electronic watchdog timer) by an output device controlled by the software.

Note 2 to entry: The watchdog can be used to de-energize a group of safety outputs when dangerous failures are detected in order to achieve or maintain a safe state of the process with respect to the hazardous event. The watchdog is used to increase the on-line diagnostic coverage of the PE logic solver (see 3.2.13 and 3.2.15).

3.3 Abbreviations

Abbreviations used throughout IEC 61511 are given in Table 1. Also included are some common abbreviations related to process sector functional safety.

Table 1 – Abbreviations used in IEC 61511

Abbreviation	Full expression
AC/DC	Alternating current/direct current
AIChE	American Institute of Chemical Engineers
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
AP	Application program
BPCS	Basic process control system
CCPS	Centre for Chemical Process Safety (AIChE)
DC	Diagnostic coverage
E/E/PE	Electrical/electronic/programmable electronic
EMC	Electro-magnetic compatibility

Abbreviation	Full expression
FAT	Factory acceptance test
FPL	Fixed program language
FSA	Functional safety assessment
FSMS	Functional safety management system
FTA	Fault tree analysis
FVL	Full variability language
HFT	Hardware fault tolerance
H&RA	Hazard & risk assessment
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
LVL	Limited variability language
MooN	“M” out of “N” channel architecture
MPRT	Maximum permitted repair time
MRT	Mean repair time
MTTR	Mean time to restoration
NFPA	National Fire Protection Association(US)
NP	Non-programmable
OEM	Original Equipment Manufacturer
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of dangerous failure on demand
PFD _{avg}	Average probability of dangerous failure on demand
PFH	Probability (average frequency of dangerous failures) of failure per hour
pl	Plural
PLC	Programmable logic controller
SAT	Site acceptance test
SC	Systematic capability
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification

4 Conformance to the IEC 61511-1:2016

To conform to the IEC 61511-1:2016, it shall be shown that each of the requirements outlined in Clause 5 through Clause 19 has been satisfied to the defined criteria and therefore the clauses' objectives have been met.

5 Management of functional safety

5.1 Objective

The objective of the requirements of Clause 5 is to identify the management activities that are necessary to ensure the functional safety objectives are met.

NOTE 1: Clause 5 is solely aimed at the achievement and maintenance of the functional safety of SIS and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

5.2 Requirements

5.2.1 General

The policy and strategy for achieving functional safety shall be identified together with the methods for evaluating their achievement and shall be communicated within the organization.

5.2.2 Organization and resources

5.2.2.1 Persons, departments, organizations or other units which are responsible for carrying out and reviewing each of the SIS safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them.

5.2.2.2 Persons, departments or organizations involved in SIS safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

The following items shall be addressed and documented when considering the competence of persons, departments, organizations or other units involved in SIS safety life-cycle activities:

- a) engineering knowledge, training and experience appropriate to the process application;
- b) engineering knowledge, training and experience appropriate to the applicable technology used (e.g., electrical, electronic or programmable electronic);
- c) engineering knowledge, training and experience appropriate to the sensors and final elements;
- d) safety engineering knowledge (e.g., process safety analysis);
- e) knowledge of the legal and regulatory functional safety requirements;
- f) adequate management and leadership skills appropriate to their role in the SIS safety life-cycle activities;
- g) understanding of the potential consequence of an event;
- h) the SIL of the SIF;
- i) the novelty and complexity of the application and the technology.

5.2.2.3 A procedure shall be in place to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.

5.2.3 Risk evaluation and risk management

Hazards shall be identified, risks evaluated and the necessary risk reduction determined as defined in Clause 8.

NOTE It may be beneficial to consider also potential capital losses, for economic reasons.

5.2.4 Safety planning

Safety planning shall take place to define the activities that are required to be carried out along with the persons, departments, organizations or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire SIS safety life-cycle (see Clause 6) and carried out to a detailed activity level commensurate with the role the individual or organization is performing in the SIS safety life-cycle.

NOTE The safety planning can be incorporated in

- a section in the quality plan entitled “SIS Safety Life-cycle Plan”; or
- a separate document entitled “SIS Safety Life-cycle Plan”; or
- several documents which may include company procedures or working practices.

5.2.5 Implementing and monitoring

5.2.5.1 Procedures shall be implemented to ensure prompt follow-up and satisfactory resolution of recommendations pertaining to the SIS arising from

- a) hazard analysis and risk assessment;
- b) assurance activities;
- c) verification activities;
- d) validation activities;
- e) FSAs;
- f) functional safety audits;
- g) post-incident and post-accident activities.

5.2.5.2 Any supplier, providing products or services to an organization that has overall responsibility for one or more phases of the SIS safety life-cycle, shall deliver products or services as specified by that organization and shall have a quality management system. Procedures shall be in place to demonstrate the adequacy of the quality management system.

If a supplier makes any functional safety claims for a product or service, which are used by the organization to demonstrate compliance with the requirements of this part of IEC 61511, the supplier shall have a functional safety management system. Procedures shall be in place to demonstrate the adequacy of the functional safety management system.

The functional safety management system shall meet the requirements of the basic safety standard IEC 61508-1:2010, Clause 6, or the functional safety management requirements of the standard derived from IEC 61508 to which functional safety claims are made.

5.2.5.3 Procedures shall be implemented to evaluate the performance of the SIS against its safety requirements to:

- identify and prevent systematic failures which could jeopardize safety;
- monitor and assess whether reliability parameters of the SIS are in accordance with those assumed during the design;
- define the necessary corrective action to be taken if the failure rates are greater than what was assumed during design;
- compare the demand rate on the SIF during actual operation with the assumptions made during risk assessment when the SIL requirements were determined.

5.2.5.4 For existing SIS designed and constructed in accordance with code, standards, or practices prior to the issue of this standard the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

5.2.6 Assessment, auditing and revisions

5.2.6.1 Functional safety assessment (FSA)

5.2.6.1.1 A procedure shall be defined and executed for a FSA in such a way that a judgement can be made as to the functional safety and safety integrity achieved by every SIF of the SIS. The procedure shall require that a FSA team be appointed which includes the technical, application and operations expertise needed for the particular application.

5.2.6.1.2 The membership of the FSA team shall include at least one senior competent person not involved in the project design team (for stages 1, 2 and 3) or not involved in the operation and maintenance of the SIS (for stages 4 and 5).

5.2.6.1.3 The following shall be considered when planning a FSA:

- the scope of the FSA;
- who is to participate in the FSA;
- the skills, responsibilities and authorities of the FSA team;
- the information that will be generated as a result of any FSA activity;
- the identity of any other safety bodies involved in the FSA;
- the resources required to complete the FSA activity;
- the level of independence of the FSA team;
- the methods by which the FSA will be revalidated after modifications.

NOTE When the FSA team is large; consideration can be given to having more than one senior competent individual on the team who is independent from the project team.

5.2.6.1.4 A FSA team shall review the work carried out on all phases of the safety life cycle prior to the stage covered by the assessment that have not been already covered by previous FSAs. If previous FSAs have been carried out then the FSA team shall consider the conclusions and recommendations of the previous assessments. The stages in the SIS safety life-cycle at which the FSA activities are to be carried out shall be identified during the safety planning.

NOTE 1 Additional FSA activities can be introduced as new hazards are identified, after modification and at periodic intervals during operation.

NOTE 2 Consideration can be given to carrying out FSA activities at the following stages (see Figure 7).

- Stage 1 – After the H&RA has been carried out, the required protection layers have been identified and the SRS has been developed.
- Stage 2 – After the SIS has been designed.
- Stage 3 – After the installation, pre-commissioning and final validation of the SIS has been completed and operation and maintenance procedures have been developed.
- Stage 4 – After gaining experience in operating and maintenance.
- Stage 5 – After modification and prior to decommissioning of a SIS.

NOTE 3 The number, size and scope of FSA activities can depend upon the specific circumstances. The factors in this decision are likely to include:

- size of project;
- degree of complexity;
- SIL;
- duration of project;
- consequence in the event of failure;
- degree of standardization of design features;
- safety regulatory requirements;
- previous experience with a similar design;
- giving consideration to relevant factors such as:
 - time in operation;
 - number and scope of changes in operation;
 - proof test frequency.

5.2.6.1.5 Prior to the hazards being present the FSA team shall undertake functional safety assessment(s) and shall confirm:

- the H&RA has been carried out (see 8.1);
- the recommendations arising from the H&RA that apply to the SIS have been implemented or resolved;
- project design change procedures are in place and have been properly implemented;
- the recommendations arising from any FSA have been resolved;
- the SIS is designed, constructed and installed in accordance with the SRS, any differences having been identified and resolved;
- the safety, operating, maintenance and emergency procedures pertaining to the SIS are in place;
- the SIS validation planning is appropriate and the validation activities have been completed;
- the employee training has been completed and appropriate information about the SIS has been provided to the maintenance and operating personnel;
- plans or strategies for implementing further FSAs are in place.

5.2.6.1.6 Where design, development and production tools are used for any SIS safety life-cycle activity, they shall themselves be subject to an assessment demonstrating that they do not have any negative impact on the SIS or the output of the tools shall be confirmed by verification procedures.

NOTE 1 The degree to which such tools can be addressed will depend upon their impact on the risk level to be achieved.

NOTE 2 Examples of development and production tools include simulation and modelling tools, measuring equipment, test equipment, equipment used during maintenance activities and configuration management tools.

NOTE 3 Quality assurance of tools includes, but is not limited to, traceability to calibration standards, operating history and defect list.

5.2.6.1.7 The results of the FSA shall be available together with any recommendation coming from this assessment.

5.2.6.1.8 All relevant information shall be made available to the FSA team upon their request.

5.2.6.1.9 In cases where a FSA is carried out on a modification the assessment shall consider the impact analysis carried out on the proposed modification and confirm that the modification work performed is in compliance with the requirements of IEC 61511.

NOTE Safety life cycle (including FSA) requirements related to SIS modifications can be found in 17.2.3.

5.2.6.1.10 A FSA shall also be carried out periodically during the operations and maintenance phase to ensure that maintenance and operation are being carried out according to the assumptions made during design and that the requirements within IEC 61511 for safety management and verification are being met.

5.2.6.2 Functional safety audit and revision

5.2.6.2.1 The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.

5.2.6.2.2 All procedures identified as necessary resulting from all safety life-cycle activities shall be subject to safety audit.

5.2.6.2.3 Functional safety audit shall be performed by an independent person not undertaking work on the SIS to be audited. Procedures shall be defined and executed for auditing compliance with requirements including:

- the frequency of the functional safety audit activities;
- the degree of independence between the persons, departments, organizations or other units carrying out the work and those carrying out the functional safety auditing activities;
- the recording and follow-up activities.

5.2.6.2.4 Management of change procedures shall be in place to initiate, document, review, implement and approve changes to the SIS other than replacement in kind (i.e., like for like, an exact duplicate of an element or an approved substitution that does not require modification to the SIS as installed).

5.2.6.2.5 Management of change procedures shall be in place that identifies changes that will affect the requirements on the SIS (e.g., re-design of a BPCS, changes to manning in a certain area).

5.2.7 SIS configuration management

5.2.7.1 Procedures for configuration management of the SIS during any SIS safety life-cycle phase shall be available.

NOTE In particular, the following can be specified:

- the stage at which formal configuration management is to be implemented;
- the procedures to be used for uniquely identifying all components of a SIS or SIS-subsystem (e.g., devices, application programming);
- the procedures for preventing unauthorized devices from entering service.

5.2.7.2 The SIS software, hardware and procedures used to develop and execute the application program shall be subject to configuration management and shall be maintained under revision control.

NOTE SIS software includes application program (e.g., in logic solvers); embedded software (e.g., sensors, logic solvers, final elements); utility software (tools).

6 Safety life-cycle requirements

6.1 Objectives.

The objectives of Clause 6 are:

- to define the phases and establish the requirements of the SIS safety life-cycle activities;
- to define and organize the technical activities into a SIS safety life-cycle;
- to ensure that adequate planning exists (or is developed) that makes certain that the SIS meets the safety requirements.

NOTE 1 The overall approach of the IEC 61511 series is shown in Figure 7. It can be stressed that this approach is for illustration and is only meant to indicate the typical SIS safety life-cycle activities from initial conception through decommissioning.

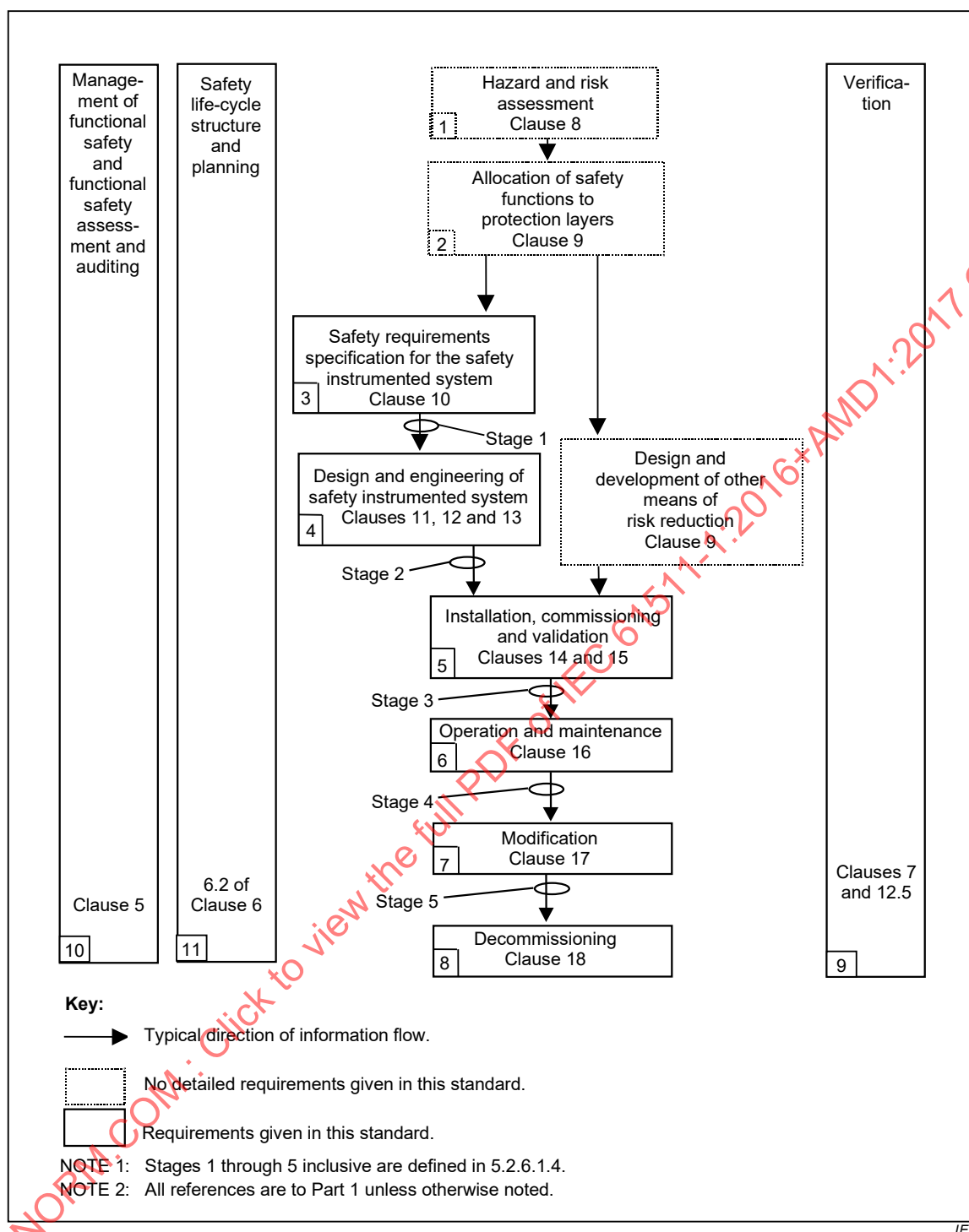


Figure 7 – SIS safety life-cycle phases and FSA stages

NOTE 2 Information in Figure 7 may flow from operation and maintenance back to the earlier life-cycle stages to reflect tracking of incidents and failures and to verify engineering assumptions.

6.2 Requirements

6.2.1 A SIS safety life-cycle incorporating the requirements of the IEC 61511 series shall be defined during safety planning. The safety life-cycle shall also address the application programming (see 6.3.1).

6.2.2 Each phase of the SIS safety life-cycle shall be defined in terms of its inputs, outputs and verification activities (see Table 2).

Table 2 – SIS safety life-cycle overview (1 of 2)

Safety life-cycle phase or activity		Objectives	Requirements Clause	Inputs	Outputs
Figure 7 box number	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	Clause 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
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL	Clause 9	A description of the required SIF and associated safety integrity requirements	Description of allocation of safety requirements
3	SIS safety requirements specification	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	Clause 10	Description of allocation of safety requirements	SIS safety requirements; application program safety requirements
4	SIS design and engineering	To design the SIS to meet the requirements for SIF and their associated safety integrity	Clauses 11, 12	SIS safety requirements Application program safety requirements	Design of the SIS hardware and application program in conformance with the SIS safety requirements; planning for the SIS integration test
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 their associated safety integrity	Clauses 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 safety requirements. Results of SIS integration tests Results of the installation, commissioning and validation activities

Table 2 (2 of 2)

Safety life-cycle phase or activity		Objectives	Requirements Clause	Inputs	Outputs
Figure 7 box number	Title				
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	Clause 16	SIS safety requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	Clause 17	Revised SIS safety requirements	Results of SIS modification
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remains appropriate	Clause 18	As built safety requirements and process information	SIF placed out of service
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	Clause 7, 12.5	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase
10	SIS FSA	To investigate and arrive at a judgement on the functional safety achieved by the SIS	Clause 5	Planning for SIS FSA SIS safety requirement	Results of SIS FSA
11	Safety lifecycle structure and planning	To establish how the lifecycle steps are accomplished	6.2	Not applicable	Safety plan

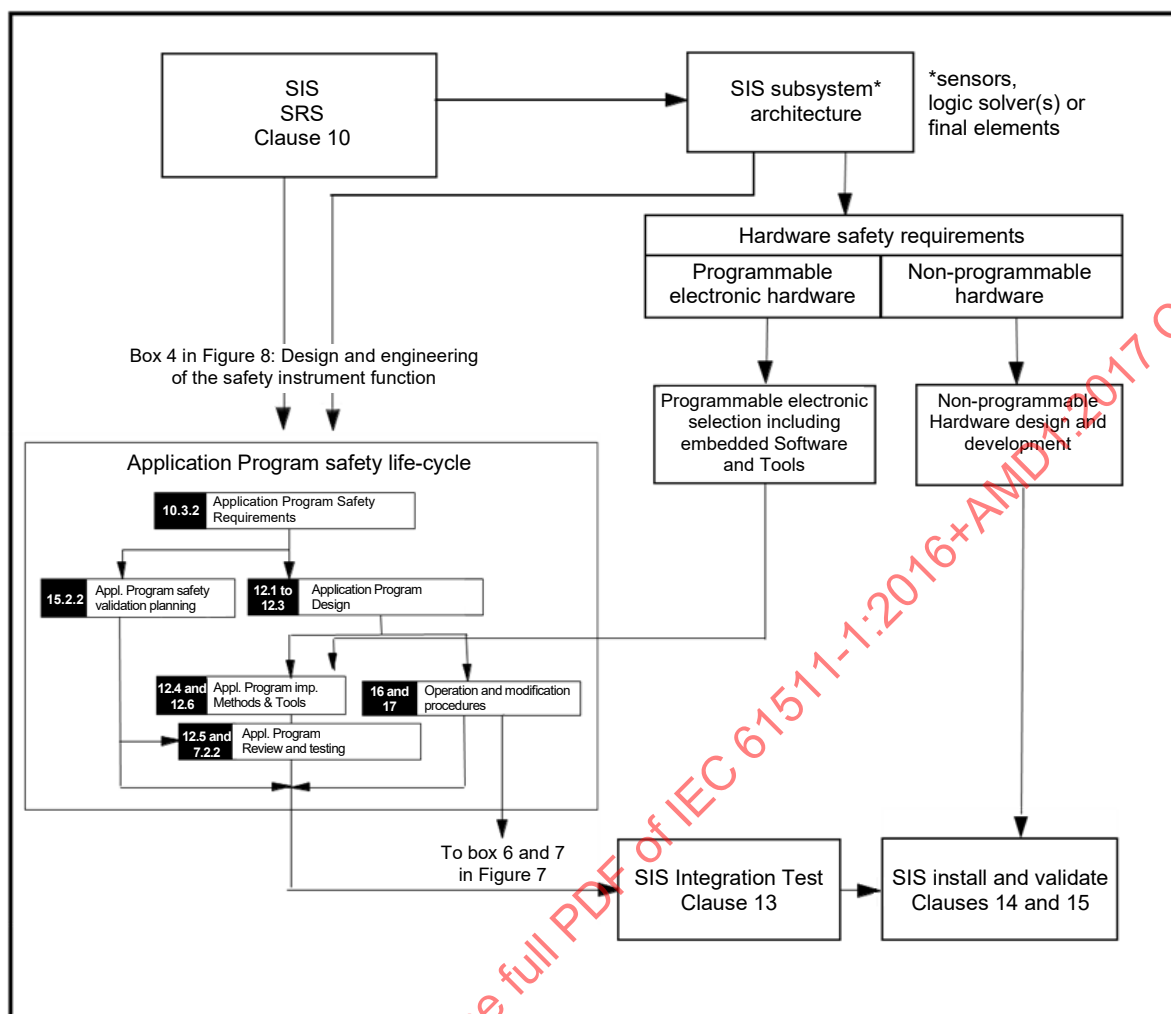
6.2.3 For all SIS safety life-cycle phases, safety planning shall take place to define the activities, criteria, techniques, measures, procedures and responsible organisation/people to:

- ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both functional and safety integrity requirements;
- ensure proper installation and commissioning of the SIS;
- ensure the safety integrity of the SIF after installation;
- maintain the safety integrity during operation (e.g., proof testing, failure analysis);
- manage the process hazards during maintenance activities on the SIS.

6.2.4 If at any stage of the safety life-cycle, a change is required pertaining to an earlier life-cycle phase, then that earlier SIS safety life-cycle phase and the subsequent phases shall be re-examined, altered as required and re-verified.

6.3 Application program SIS safety life-cycle requirements

6.3.1 Each phase of the application program safety life-cycle (see Figure 8) shall be defined in terms of its elementary activities, objectives, required input information and output results and verification requirements (see Table 3).



IEC

Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle

Table 3 – Application program safety life-cycle: overview (1 of 2)

Safety life-cycle phase		Objectives	Requirements Clause	Inputs	Outputs
Figure 8 box number	Title				
10.3.2	Application program safety requirements	To specify application program safety requirements for each SIS necessary to implement the required SIF. To specify the requirements for application program for each SIF allocated to that SIS.	10.3 11.5	SIS safety requirements. Safety manuals of the selected SIS. SIS architecture.	SIS application program safety requirements specification. Verification information.
15.2.2	Application program safety validation planning	To develop a plan for validating the application program.	15.2.2, 15.2.5	SIS application program safety requirements.	SIS safety validation planning. Verification information.
12.1 to 12.3	Application program development	Architecture. To create an application program architecture that fulfils the specified requirements for application program safety. To review and evaluate the requirements placed on the application program by the hardware architecture of the SIS. To specify the procedures for the development of the application program.	12.1 (also 10.3, 12.2)	SIS application program safety requirements. SIS hardware architecture design constraints.	Description of the architecture design, e.g., segregation of application program into related process sub-system and SIL, e.g., recognition of common application program modules such as pump or valve sequences. Application program architecture and sub-system integration test requirements. Verification information.
	Application program design	To develop the application program design. To identify a suitable set of configuration, library, management, and simulation and test tools, over the safety life-cycle of the application program.	12.3	SIS application program safety requirements. Description of the architecture design. Manuals of the SIS. Safety Manual of the selected SIS logic solver.	Application program design. Procedures for use during programming. Description of the standard (manufacturers) library functions to be used. Verification information.

Table 3 (2 of 2)

Safety life-cycle phase		Objectives	Requirements Clause	Inputs	Outputs
Figure 8 box number	Title				
12.4 12.6	Application program implementation	Application development and application module development. To implement the application program that fulfils the specified requirements for application safety. To use appropriate support tools and programming languages.	12.4 12.3.4 12.6	Description of the design. List of manuals and procedures of the selected logic solver for use with the application program.	Application program (e.g., function block diagrams, ladder logic). Application program simulation and integration test. Special purpose application program safety requirements. Verification information.
12.5 7.2.2	Application program verification	To verify that the requirements for application program safety have been achieved. To show that all SIS application programs interact correctly to perform their intended functions and do not perform unintended functions.	12.5 7.2.2	Application program simulation and integration test requirements (structure based testing). Application program architecture integration test requirements.	Application program test results. Verified and tested application program system. Verification information.
13	SIS integration test	To integrate the application program onto the target logic solver, including interaction with a sample set of field devices and or simulator.	Clause 13	Application program and logic solver integration test requirements.	Application program and logic solver integration test results.

6.3.2 Methods, techniques and tools shall be applied for each life-cycle phase in accordance with 12.6.2.

6.3.3 Each phase of the SIS safety life-cycle for which safety planning has been carried out shall be verified (see Clause 7) and the results shall be available as described in Clause 19.

7 Verification

7.1 Objective

The objective of Clause 7 is to demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases (Figure 7) as identified by the verification planning.

7.2 Requirements

7.2.1 Verification planning shall be carried out throughout the SIS safety life-cycle and shall define all activities required for the appropriate phase (Figure 7) of the safety life-cycle, including the application program. Verification planning shall conform to the IEC 61511 series by addressing the following:

- the verification activities;
- the procedures, measures and techniques to be used for verification including implementation and resolution of resulting recommendations;
- when these activities will take place;
- the persons, departments and organizations responsible for these activities, including levels of independence;
- identification of items to be verified;
- identification of the information against which the verification is carried out;
- the adequacy of the outputs against the requirements for that phase;
- correctness of the data;
- how to handle non-conformances;
- tools and supporting analysis;
- the completeness of the SIS implementation and the traceability of the requirements;
- the readability and audit-ability of the documentation;
- the testability of the design.

7.2.2 Where the verification includes testing, the verification planning shall also address the following:

- the strategy for integration of application program and hardware and field devices, including the integration of sub-systems that shall comply with other standards (such as machinery or burner);
- test scope (describes the test set-up and what type of test to be performed including the hardware, application programming, and programming devices to be included);
- test cases and test data (these will be specific scenarios with the associated data);
- types of tests to be performed;
- test environment including tools, hardware, all software and required configuration;
- test criteria (e.g., pass/fail criteria) on which the results of the test will be evaluated;
- procedures for corrective action on failure during test;
- physical location(s) (e.g., factory or site);
- dependence on external functionality;
- appropriate personnel;
- management of change;
- non-conformances.

7.2.3 Non-safety functions integrated with safety functions shall be verified for non-interference with the safety functions.

7.2.4 Verification shall be performed according to the verification planning.

7.2.5 During testing, any modification shall be subjected to an impact analysis which shall determine all SIS components impacted and the necessary re-verification activities.

7.2.6 The results of the verification process shall be available (see Clause 19), including whether the objective and criteria of the tests have been met.

NOTE 1 Selection of techniques and measures for the verification process and the degree of independence depends upon a number of factors including degree of complexity, novelty of design, novelty of technology and required SIL.

NOTE 2 Examples of some verification activities include design reviews, use of tools and techniques including software verification tools and computer based design analysis tools.

8 Process H&RA

8.1 Objectives

The objectives of the requirements of Clause 8 are 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;
- any requirements for risk reduction;
- the safety functions required to achieve the necessary risk reduction;
- if any of the safety functions are SIFs.

NOTE 1 Clause 8 addresses process engineers, hazard and risk specialists, safety managers as well as instrument engineers. Its purpose is to recognize the multi-disciplinary approach typically required for the determination of SIF.

NOTE 2 Where reasonably practicable, processes can be designed to be inherently safe. When this is not practicable, other layers of protection (see Figure 9) can be required. In some applications, industry standards can specify the use of particular protection layers.

NOTE 3 The risk reduction can be accomplished using several layers of protection ~~and the layers can be independent, sufficient, dependable and auditable~~ (see Clause 9).

8.2 Requirements

8.2.1 A H&RA shall be carried out on the materials, process and equipment. It shall result in:

- a description of each identified hazardous event and the factors that contribute to it;
- a description of the likelihood and consequence of each hazardous event;
- consideration of process operating modes such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown;
- the determination of additional risk reduction necessary to achieve the required functional safety;
- a description of, or references to information on, the measures taken to reduce or remove hazards and risk;
- a detailed description of the assumptions made during the analysis of the risks including demand rates on the protection layers and the average frequency of dangerous failures of the initiating sources, and of any credit taken for operational constraints or human intervention;
- identification of those safety function(s) applied as SIF(s).

NOTE 1 In determining the safety integrity requirements, account can be taken of the effects of common cause between systems that create demands and the protection layers that are designed to respond to those demands. An example of this would be where demands can arise through BPCS failure and the equipment used within the protective layers is similar or identical to the equipment used within the BPCS. In such cases, a demand caused by a failure of BPCS equipment may not be responded to effectively if a common cause has rendered similar equipment in the protection layer to be ineffective. It may not be possible to recognize common cause problems during the initial hazard identification and risk analysis because at such an early stage the design of the protection layers will not necessarily have been completed. In such cases, it can be necessary to reconsider the safety integrity requirements and SIF once the design of the SIS and other protection layers has been completed. In determining whether the overall design of process and protection layers meets requirements, common cause failures will be considered.

NOTE 2 Examples of techniques that can be used to establish the required SILs of SIFs are illustrated in IEC 61511-3:2016.

8.2.2 The average frequency of dangerous failures of a BPCS as an initiating source shall not be assumed to be $<10^{-5}$ per hour.

8.2.3 The H&RA shall be recorded in such a way that the relationship between the above items is clear and traceable.

NOTE 1 The above requirements do not mandate that the safety integrity requirements have to be assigned as numerical values. Qualitative or semi-quantitative approaches (see IEC 61511-3:2016, Annexes C, D & E) can also be used.

NOTE 2 The safety integrity requirements vary depending on the application and national legal requirements. An accepted principle in many countries is that additional risk reduction measures can be applied until the cost incurred becomes disproportionate to the improvement in safety integrity achieved.

8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction;
- a description of, or references to information on, the measures taken to reduce or remove the threats.

NOTE 1 Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

NOTE 2 The information and control of boundary conditions needed for the security risk assessment are typically with owner/operating company of a facility, not with the supplier. Where this is the case, the obligation to comply with 8.2.4 can be with the owner/operating company of the facility.

NOTE 3 The SIS security risk assessment can be included in an overall process automation security risk assessment.

NOTE 4 The SIS security risk assessment can range in focus from an individual SIF to all SISs within a company.

9 Allocation of safety functions to protection layers

9.1 Objectives

The objectives of the requirements of Clause 9 are to

- allocate safety functions to protection layers;
- determine the required SIFs;
- determine for each SIF the associated safety integrity requirements.

NOTE 1 Account can be taken, during the process of allocation, of other industry standards or codes.

NOTE 2 The integrity requirements for each SIF might include the associated risk reduction, PFD, PFH or SIL.

9.2 Requirements of the allocation process

9.2.1 The allocation process shall result in

- the allocation of safety functions required to achieve the necessary risk reduction to specific protection layers;
- the allocation of risk reduction or average frequency of dangerous failure to each SIF.

NOTE Legislative requirements or other industry codes may influence the allocation process.

9.2.2 The required SIL shall be derived taking into account the required PFD or PFH that is to be provided by the SIF.

NOTE Further guidance can be found in IEC 61511-3:2016.

9.2.3 For each SIF operating in demand mode, the required SIL shall be specified in accordance with either Table 4 or Table 5.

9.2.4 For each SIF operating in continuous mode, the required SIL shall be specified in accordance with Table 5.

Table 4 – Safety integrity requirements: PFD_{avg}

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	PFD_{avg}	Required risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10\ 000$ to $\leq 100\ 000$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 1\ 000$ to $\leq 10\ 000$
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to $\leq 1\ 000$
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	Average frequency of dangerous failures (failures per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE 1 Further explanation of modes of operation can be found in 3.2.39.

NOTE 2 The SIL is defined numerically so as to provide an objective measure for comparison of alternate designs and solutions. However, it is recognized that, given the current state of knowledge, many systematic causes of failure can only be assessed qualitatively.

NOTE 3 The required average frequency of dangerous failures for a continuous or demand mode SIF is determined by considering the risk caused by failure of the continuous or demand mode SIF together with the failures of other devices that lead to the same risk, taking into consideration the risk reduction provided by other protection layers.

9.2.5 In cases where the allocation process results in a risk reduction requirement of $>10\ 000$ or average frequency of dangerous failures $<10^{-8}$ per hour for a single SIS or multiple SISs or SIS in conjunction with a BPCS protection layer, there shall be a reconsideration of the application (e.g., process, other protection layers) to determine if any of the risk parameters can be modified so that the risk reduction requirement of $>10\ 000$ or average frequency of dangerous failures $<10^{-8}$ per hour is avoided. The review shall consider whether:

- the process or vessels/pipe work can be modified to remove or reduce hazards at the source;
- additional safety-related systems or other risk reduction means, not based on instrumentation, can be introduced;
- the severity of the consequence can be reduced, e.g., reducing the amount of hazardous material;

- the likelihood of the specified consequence can be reduced e.g., reducing the likelihood of the initiating source of the hazardous event.

NOTE Applications which require the use of a single SIF with a risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour need to be avoided because of the difficulty of achieving and maintaining such high levels of performance throughout the SIS safety life-cycle. Risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour can require high levels of competence and high levels of coverage for all factory acceptance testing, proof testing, verification, and validation activities.

9.2.6 If after further consideration of the application and confirmation that a risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour is still required, then consideration should be given to achieving the safety integrity requirement using a number of protection layers (e.g., SIS or BPCS) with lower risk reduction requirements. If the risk reduction is allocated to multiple protection layers then such protection layers shall be independent from each other or the lack of independence shall be assessed and shown to be sufficiently low compared to the risk reduction requirements. The following factors shall be considered during this assessment:

- common cause of failure of SIS and the cause of demand;

NOTE 1 The extent of the common cause can be assessed by considering the diversity of all devices where failure could cause a demand and all devices of the BPCS protection layer and/or the SIS used for risk reduction.

NOTE 2 An example of common cause between the SIS and the cause of demand is if loss of process control through sensor fault or failure can cause a demand and the sensor used for control is of the same type as the sensor used for the SIS.

- common cause of failure with other protection layers providing risk reduction;

NOTE 3 The extent of the common cause can be assessed by considering the diversity of all devices of the BPCS protection layer and/or the SIS used to achieve the risk reduction requirements.

NOTE 4 An example of common cause between SISs providing risk reduction is when two separate and independent SISs with diverse measurements and diverse logic solvers are used but the final actuation devices are two shut off valves of similar types or a single shut off valve actuated by both SISs.

- any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times;

NOTE 5 Even if the protective layers are diverse then synchronous proof testing will reduce the overall risk reduction achieved and this can be a significant factor impeding achievement of the necessary risk reduction for the hazardous event.

NOTE 6 When high levels of risk reduction are required and proof tests are desynchronised according to Note 5 then the dominant factor is normally common cause failure even if multiple independent protection layers are used to reduce risk. Dependency within and between protection layers providing risk reduction for the same hazardous event can be assessed and shown to be sufficiently low.

9.2.7 If a risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour is to be implemented, whether allocated to a single SIS or multiple SIS or SIS in conjunction with a BPCS protection layer, then a further risk assessment shall be carried out using a quantitative methodology to confirm that the safety integrity requirements are achieved. The methodology shall take into consideration dependency and common cause failures between the SIS and:

- any other protection layer whose failure would place a demand on it;
- any other SIS reducing the likelihood of the hazardous event;
- any other risk reduction means that reduce the likelihood of the hazardous event (e.g., safety alarms).

9.2.8 If the risk reduction required for a hazardous event is allocated to multiple SIFs in a single SIS, then the SIS shall meet the overall risk reduction requirement.

9.2.9 The results of the allocation process shall be recorded so that the SIFs are described in terms of the functional needs of the process, e.g., the actions to be taken, set points, reaction times, activation delays, fault treatment, valve closure requirements, and in terms of the risk reduction requirements.

NOTE This description can be in an unambiguous logical form and can be referred to as the process requirements specification or the safety description. The description can make the intent and the approach used in the allocation process clear. The process requirements specification is used as input information for the SRS covered in Clause 10 and can be sufficiently detailed to ensure adequate specification of the SIS and its devices. For example, the description can include the set-points for sensors, the process safety time available for response, and the valve closure requirements.

9.3 Requirements on the basic process control system as a protection layer

9.3.1 The basic process control system may be claimed as a protection layer as shown in Figure 9.

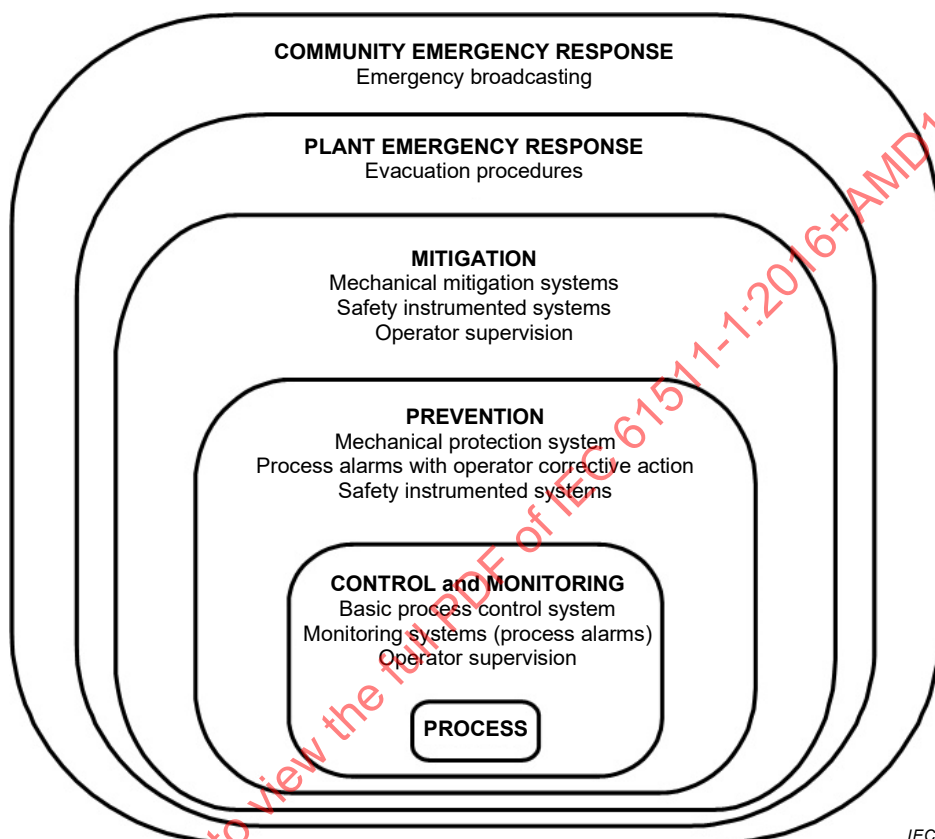


Figure 9 – Typical protection layers and risk reduction means

9.3.2 The risk reduction claimed for a BPCS protection layer shall be ≤ 10 .

NOTE Consideration can be given to the fact that a BPCS may also be an initiating source for the demand on the protection layer.

9.3.3 If the risk reduction claimed for a BPCS protection layer is > 10 , then the BPCS shall be designed and managed to the requirements within the IEC 61511 series.

9.3.4 If it is not intended that the BPCS conform to the IEC 61511 series, then:

- no more than one BPCS protection layer shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is the initiating source for the demand on the protection layer; or
- no more than two BPCS protection layers shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is not the initiating source of the demand.

NOTE The identified BPCS protection layer can consist of one BPCS as the initiating source for the demand (see 8.2.2) and a second independent BPCS protection layer (see 9.3.2 and 9.3.3) or up to two independent BPCS protection layers when the initiating source is not related to BPCS failure.

9.3.5 When 9.3.4 applies, each BPCS protection layer shall be independent and separate from the initiating source and from each other to the extent that the claimed risk reduction of each BPCS protection layer is not compromised.

NOTE 1 The assessment of separation and independence can consider what is necessary to achieve the risk reduction, e.g., the central processing units (CPU), input/output modules, relays, field devices, application programming, networks, program database, engineering tools, human machine interface, by-pass tools and other devices.

NOTE 2 A hot backup controller is not considered to be independent of the primary controller because it is subject to common cause failure (for example, hot backup controllers have components that are common to both the primary and the backup controller, such as the backplane, firmware, diagnostics, transfer mechanisms and undetected dangerous failures).

9.4 Requirements for preventing common cause, common mode and dependent failures

9.4.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between:

- protection layers;
- protection layers and the BPCS.

are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.

NOTE A definition of dependent failure is provided in 3.2.12.

9.4.2 The assessment shall consider the following:

- independence between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS.

NOTE 1 Common causes from the process can be addressed. Plugging of relief valves may cause the same problems as plugging of sensors in a SIS.

NOTE 2 Independence and physical separation can be addressed. A Human Machine Interface, SIS/BPCS networks or bypass means can cause common cause failure.

10 SIS safety requirements specification (SRS)

10.1 Objective

The objective of Clause 10 is to specify the requirements for the SIS, including any application programs and the architecture of the SIS.

10.2 General requirements

The safety requirements shall be derived from the allocation of SIF and from those requirements identified during H&RA. The SIS requirements shall be expressed and structured in such a way that they are

- clear, precise, verifiable, maintainable and feasible;
- written to aid comprehension and interpretation by those who will utilise the information at any phase of the safety life-cycle.

10.3 SIS safety requirements

10.3.1 The objective of 10.3 is to address issues that shall be considered when developing the SIS safety requirements.

10.3.2 These requirements shall be sufficient to design the SIS and shall include a description of the intent and approach applied during the development of the SIS safety requirements as applicable:

- a description of all the SIF necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative);
- a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);
- requirements to identify and take account of common cause failures;
- a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated;
- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system);
- the assumed sources of demand and demand rate on each SIF;
- requirements relating to proof test intervals;
- requirements relating to proof test implementation;
- response time requirements for each SIF to bring the process to a safe state within the process safety time;
NOTE See IEC 61511-2:2016 for further discussion of process safety time.
- the required SIL and mode of operation (demand/continuous) for each SIF;
- a description of SIS process measurements, range, accuracy and their trip points;
- a description of SIF process output actions and the criteria for successful operation, e.g., leakage rate for valves;
- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives for each SIF;
- requirements for manual shutdown for each SIF;
- requirements relating to energize or de-energize to trip for each SIF;
- requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element resets after trips);
- maximum allowable spurious trip rate for each SIF;
- failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shutdown);
- any specific requirements related to the procedures for starting up and restarting the SIS;
- all interfaces between the SIS and any other system (including the BPCS and operators);
- a description of the modes of operation of the plant and requirements relating to SIF operation within each mode;
- the application program safety requirements as listed in 10.3.23;
- requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared;
- the specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors;

- the mean repair time which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints;
- identification of the dangerous combinations of output states of the SIS that need to be avoided;
- identification of the extremes of all environment conditions that are likely to be encountered by the SIS during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;
- identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIFs may be required to support these process operating modes;
- definition of the requirements for any SIF necessary to survive a major accident event, e.g., time required for a valve to remain operational in the event of a fire.

10.3.3 The application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS. The application program safety requirements may be located in the SRS or in a separate document (e.g., application program requirements specification). The input to the application program safety requirements for each SIS subsystem shall include:

- a) the specified safety requirements of each SIF, including sensor voting, etc.;
- b) the requirements resulting from the SIS architecture and the safety manual such as limitations and constraints of the hardware and embedded software;
- c) any requirements of safety planning arising from 5.2.4.

10.3.4 The application program safety requirements shall be specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS.

10.3.5 The application program safety requirements specification shall be sufficiently detailed to allow the design and implementation to achieve the required functional safety and to allow a functional safety assessment to be carried out. The following shall be considered:

- the SIFs supported by the application program and their SIL;
- real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a specified time period;
- program sequencing and time delays if applicable;
- equipment and operator interfaces and their operability;
- all relevant modes of operation of the process as specified in the SRS;
- action to be taken on bad process variable such as sensor value out of range, excessive range of change, frozen value, detected open circuit, detected short circuit;
- functions enabling proof testing and automated diagnostic tests of external devices (e.g., sensors and final elements) performed in the application program;
- application program self-monitoring (e.g., application driven watch-dogs and data range validation);
- monitoring of other devices within the SIS (e.g., sensors and final elements);
- any requirements related to periodic testing of SIF when the process is operational;
- references to the input documents (e.g., specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS);

- the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;
- process dangerous states (for example closure of two isolation gas valves at the same time that could lead to pressure fluctuations thus leading to a dangerous state) generated by the application program shall be identified and avoided;
- definitions of process variable validation criteria for each SIF.

10.3.6 The application program safety requirements specification shall be expressed and structured in such a way that they:

- describe the intent and approach underpinning the application program safety requirements;
- are clear and understandable to those who will utilize the document at any phase of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by all users (e.g., plant operators, maintenance personnel, application programmers);
- are verifiable, testable, modifiable;
- are traceable back through all deliverables including the detailed design documents, the SRS and the H&RA that identifies the required SIF and SIL.

11 SIS design and engineering

11.1 Objective

The objective of the requirements of Clause 11 is to design one or multiple SIS to provide the SIF and meet the specified integrity requirements (e.g., SIL, associated risk reduction, PFD and /or PFH).

11.2 General requirements

11.2.1 The design of the SIS shall be in accordance with the SIS safety requirements specifications, taking into account all the requirements of Clause 11.

11.2.2 Where the SIS is to implement both SIFs and non-SIFs then all the hardware, embedded software and application program that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL of any of the SIFs it can impact.

11.2.3 Where the SIS is to implement SIF of different SIL, then the shared or common hardware and embedded software and application program shall conform to the highest SIL.

NOTE Embedded software or application programs of different SIL could coexist in the same device provided it can be demonstrated that the SIF of lower SIL cannot negatively affect the SIF of the higher SIL.

11.2.4 If it is intended not to qualify the BPCS to the IEC 61511 series, then the SIS shall be designed to be separate and independent from the BPCS to the extent that the safety integrity of the SIS is not compromised.

NOTE 1 Operating information can be exchanged but not compromise the functional safety of the SIS.

NOTE 2 Devices of the SIS can also be used for functions of the BPCS if it can be demonstrated that a failure of the BPCS does not compromise the SIF of the SIS.

11.2.5 Requirements for operability, maintainability, diagnostics, inspection and testability shall be addressed during the design of the SIS in order to reduce the likelihood of dangerous failures.

11.2.6 The design of the SIS shall take into account human capabilities and limitations and be suitable for the tasks assigned to operators and maintenance staff. The design of operator interfaces shall follow good human factors practice and shall accommodate the likely level of training that operators should receive.

NOTE 1 For example, human factor studies may be necessary if operation requires data entry of limits or other operator input on a regular basis.

11.2.7 The SIS shall be designed in such a way that once it has placed the process in a safe state, the process shall remain in the safe state until a reset has been initiated unless otherwise directed by the SRS.

11.2.8 Manual means (e.g., emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the SRS.

11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependency between the SIS and BPCS, and the SIS and other protection layers.

11.2.10 A device used by the BPCS shall not be used by the SIS where a failure of that device may result in both a demand on the SIF and a dangerous failure of the SIF, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand on the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared device because if the shared device fails, a demand will be created immediately to which the SIS may not be capable of responding. For that reason, additional analysis can be necessary in these cases to ensure that the dangerous failure rates of the shared devices are sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.

11.2.11 For any SIS device that on loss of utility (e.g., electrical power, air, hydraulics or pneumatic supply) does not fail to the safe state, loss of utility and SIS circuit integrity shall be detected and alarmed (e.g., end-of-line monitoring, supply pressure measurement, hydraulic or pneumatic pressure monitoring) and action taken according to 11.3.

NOTE 1 Utility integrity can be improved through using a supplementary supply (e.g., battery back-up, uninterruptible power supplies, air reservoir, hydraulic accumulator, second gas supply).

NOTE 2 The loss of a utility is likely to affect multiple SIFs and, possibly, multiple SISs. ~~Hence common cause failure of multiple SIFs can be considered.~~

11.2.12 The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

NOTE Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

11.2.13 A safety manual covering operation, maintenance, fault detection and constraints associated with the SIS shall be available covering the intended configurations of the devices and the intended operating environment.

11.2.14 All communications used to implement a SIF shall be established using techniques appropriate for safety applications to meet the required SIL.

11.3 Requirements for system behaviour on detection of a fault

11.3.1 When a dangerous fault in a SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation. If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken. Where the compensating measures depend on an operator taking specific action in response to an alarm (e.g., opening or closing a valve) then the alarm shall be considered part of the SIS.

NOTE 1 The specified action (fault reaction) required to achieve or maintain a safe state of the process can be specified in the SRS (see 10.3.1). It can consist of the safe shutdown of the process or of that part of the process which relies on the faulty SIS for risk reduction.

NOTE 2 The compensating measures required for continued safe operations can depend on safety integrity requirements, the tolerable risk associated with the hazardous event, the hardware fault tolerance of the SIS, the anticipated MRT and the availability of any other layers of protection. In some cases it can be adequate to ensure action is taken to ensure repair of the dangerous failure within the assumed MPRT in the calculation of the PFDavg but in other cases it can be judged necessary to provide other measures to compensate for the reduced risk reduction until the SIS is fully restored. See also 16.2.3.

11.3.2 Where any dangerous fault in an SIS is brought to the attention of an operator by an alarm then the alarm shall be subject to appropriate proof testing and management of change.

11.4 Hardware fault tolerance

11.4.1 The SIS shall have a minimum HFT with respect to each SIF it implements.

NOTE This does not exclude the possibility that the HFT may be reduced below the minimum requirement at certain times during operation of the system following the occurrence of faults.

11.4.2 When the SIS can be split into independent SIS subsystems (e.g. sensors, logic solvers and final elements), then the HFT can be assigned at the SIS subsystem level.

11.4.3 The HFT of the SIS or its SIS subsystems shall be in accordance with;

- 11.4.5 to 11.4.9 of clause 11 or,
- the requirements of 7.4.4.2 (route 1H) of IEC 61508-2:2010 or,
- the requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.

NOTE The route developed in IEC 61511 is derived from route 2_H of IEC 61508-2:2010.

11.4.4 When determining the achieved HFT, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements. Any such fault exclusions shall be justified and documented.

NOTE Further information about fault exclusion can be found in ISO13849-1:2006 and ISO13849-2:2012.

11.4.5 The minimum HFT for a SIS (or its SIS subsystems) implementing a SIF of a specified SIL shall be in accordance with Table 6 and if appropriate 11.4.6 and 11.4.7.

NOTE The HFT requirements in Table 6 represent the minimum system or, where relevant, the SIS subsystem redundancy. Depending on the application, device failure rate and proof-testing interval, additional redundancy can be required to satisfy the failure measure for the SIL of the SIF according to 11.9.

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

11.4.6 For a SIS or SIS subsystem that does not use FVL or LVL programmable devices and if the minimum HFT as specified in Table 6, would result in additional failures and lead to decreased overall process safety, then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.

NOTE Fault tolerance is the preferred solution to achieve the required confidence that a robust architecture has been achieved. When 11.4.6 applies, the purpose of the justification is to demonstrate that the proposed alternative architecture provides an equivalent or better solution. This may vary depending on the application and/or the technology in use; examples 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 diversified 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.

11.4.7 If a fault tolerance equal to zero results from applying 11.4.6, the justification required by 11.4.6 shall provide evidence that the related dangerous failure modes can be excluded, in accordance with 11.4.4 including consideration of the potential for systematic failures.

11.4.8 FVL and LVL programmable devices shall have diagnostic coverages not less than 60 %.

11.4.9 Reliability data used in the calculation of the failure measure shall be determined by an upper bound statistical confidence limit of no less than 70 %.

11.5 Requirements for selection of devices

11.5.1 Objectives

The objectives of the requirements of 11.5 are to:

- specify the requirements for the selection of devices which are to be used as part of the SIS;
- specify the requirements to enable a device to be integrated in the architecture of a SIS;
- specify acceptance criteria for devices in terms of associated SIF and safety integrity requirements.

11.5.2 General requirements

11.5.2.1 Devices selected for use as part of a SIS with a specified SIL shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010 and/or 11.5.3 through 11.5.6, as appropriate.

NOTE Devices assessed against IEC 61508-2:2010 and IEC 61508-3:2010 can be applied in accordance with the requirements for systematic capability in IEC 61508-2:2010.

11.5.2.2 All devices shall be suitable for the operating environment as determined through consideration of the manufacturer's documentation, the constraints within the SRS and the reliability parameters assumed in respect of 11.9. Suitability of the selected devices shall always be considered in the context of the operating environment.

NOTE Devices may exhibit different failure rates dependent on the operating environment and mode of operation. Failure rate data available from manufacturers may not be valid in all applications. For example, the failure rate and failure mode distribution can be different for a valve that is frequently exercised versus one that stands still for long periods of time.

11.5.3 Requirements for the selection of devices based on prior use

11.5.3.1 Appropriate evidence shall be available that the devices are suitable for use in the SIS.

NOTE 1 The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 2 Level of detail of the evidence can be in accordance with the complexity of the considered device.

NOTE 3 A prior use evaluation involves gathering documented information concerning the device performance in a similar operating environment. Prior use demonstrates the functionality and integrity of the installed device, including the process interfaces, full device boundary, communications, and utilities. The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 4 Prior use data can contribute to a database for the calculation of hardware failure rates as described in 11.9.3.

11.5.3.2 The evidence of suitability shall include the following:

- consideration of the manufacturer's quality, management and configuration management systems;
- adequate identification and specification of the devices;
- demonstration of the performance of the devices in similar operating environments;

NOTE 1 In the case of field devices (e.g., sensors and final elements) fulfilling a given specification, the behaviour of the device in the operating environment is usually identical in safety and non-safety applications. Therefore, evidence of the performance of similar devices in non-safety applications can also be used to satisfy this requirement.

- the volume of the operating experience.

NOTE 2 For field devices, information relating to operating experience is mainly recorded in the user's list of equipment approved for use in their facilities, based on an extensive history of successful performance in safety and non-safety applications, and on the elimination of equipment not performing in a satisfactory manner. The list of field devices can be used to support claims of experience in operation, provided that:

- the list is updated and monitored regularly;
- field devices are only added when sufficient operating experience has been obtained;
- field devices are removed when they show a history of not performing in a satisfactory manner;
- the operating environment is included in the list where relevant.

NOTE 3 Device performance is highly affected by the operating environment. It is generally recommended that selection of devices can be based on adequate performance of an installed sufficient number of devices in multiple installations for a sufficient operating time. The gained experience can allow time to reveal early failures, such as those related to specification, handling, installation, and commissioning.

NOTE 4 The amount of operational experience to gain credible statistical reliability data is typically much higher compared to the operational experience necessary to get evidence of prior use.

11.5.3.3 All devices selected on the basis of prior use shall be identified by a specified revision number and shall be under the control of a management of change procedure. In the case of a change being made to the device, the continued validity of the evidence of prior use shall be justified by evaluating the significance of the change made.

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

11.5.4.1 For SIL 1, SIL 2, and SIL 3, the requirements of 11.5.2 and 11.5.3 apply, together with the following subclauses.

11.5.4.2 All configuration options of the device possibly influencing safety shall be identified and considered. It is important to check that wherever specific settings are not defined that the default settings of the device are confirmed to be appropriate. Unused features of the devices shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required SIF.

11.5.4.3 For the specific configuration and operating environment of the device, the evidence of suitability shall consider:

- characteristics of input and output signals;
- modes of use;
- functions and configurations used;
- prior use in similar operating environments.

11.5.4.4 In addition, for SIL 3 applications, an assessment of the FPL device shall be carried out to show that:

- the FPL device is both able to perform the required functions and that prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous

event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;

- appropriate standards for hardware and software have been applied;
- the FPL device has been used or tested in configurations representative of the intended operational profiles.

11.5.5 Requirements for selection of LVL programmable devices based on prior use

11.5.5.1 The following requirements apply to PE devices used in SISs which implement SIL 1 or SIL 2 SIFs.

11.5.5.2 The requirements of 11.5.4 apply.

11.5.5.3 Where there is any difference between the operating environment of a device as experienced previously, and the operating environment of the device when used within the SIS, then any such differences shall be identified and there shall be an assessment based on analysis and testing, as appropriate, to show that the likelihood of systematic faults when used in the SIS is sufficiently low.

11.5.5.4 The operating experience considered necessary to justify the suitability shall be determined taking into account:

- the SIL of the SIF;
- the complexity and functionality of the devices.

11.5.5.5 For SIL 1 or 2 applications, a safety configured PE logic solver may be used provided that all the following additional provisions are met:

- understanding of unsafe failure modes;
- use of techniques for safety configuration that address the identified failure modes;
- the embedded software has a good history of use for safety applications;
- protection against unauthorized or unintended modifications.

NOTE A safety configured PE logic solver is a general purpose industrial grade PE logic solver which is specifically configured by the OEM, a systems engineer or the end-user for use in safety applications.

11.5.5.6 A formal assessment of any PE logic solver used in a SIL 2 application shall be carried out to show that:

- it is both able to perform the required functions and that prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;
- measures are implemented to detect faults during program execution and initiate appropriate responses; these measures shall comprise all of the following:
 - program sequence monitoring;
 - protection of code against modifications or failure detection by on-line monitoring;
 - failure assertion or diverse programming;
 - range check of variables or plausibility check of values;
 - modular approach;
 - appropriate coding standards have been used for the embedded and utility software;
 - testing in typical configurations, with test cases representative of the intended operational profiles;
 - trusted verified software modules and components have been used;
 - the system has undergone dynamic analysis and testing;

- the system does not use artificial intelligence or dynamic reconfiguration;
- documented fault-insertion testing (negative testing) has been performed.

11.5.6 Requirements for selection of FVL programmable devices

When the applications are programmed using a FVL, the PE device shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010.

11.6 Field devices

11.6.1 Field devices shall be selected and installed to minimize failures that could result in inaccurate information due to conditions arising from the operating environment. Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, coking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse lines.

11.6.2 Energize to trip circuits shall apply means to ensure circuit and power supply integrity.

NOTE 1 An example of such means is an end-of-line monitor, where a pilot current is continuously monitored to detect circuit continuity and where the pilot current is not of sufficient magnitude to affect proper I/O operation.

NOTE 2 Additional requirements for loss of power can be found in 11.2.11.

11.6.3 Smart sensors shall be write-protected to prevent inadvertent modification, unless appropriate safety review (e.g., H&RA) allows the use of read/write.

NOTE The review can take into account human factors such as failure to follow procedures.

11.7 Interfaces

11.7.1 General

Interfaces to the SIS can include, but are not limited to:

- operator interface(s);
- maintenance/engineering interface(s);
- communication interface(s).

11.7.2 Operator interface requirements

11.7.2.1 Where the SIS operator interface is via the BPCS operator interface, account shall be taken of credible failures that may occur in the BPCS operator interface.

NOTE This can include preparing plans to enable an orderly safe shutdown in the event of total failure of the operational displays.

11.7.2.2 The design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while hazards are present. If the design does require the use of operator actions, the design should include facilities for protection against operator error.

NOTE If the operator has to select a particular option, there can be a confirmation step.

11.7.2.3 Bypass switches or means shall be protected to prevent unauthorized use (e.g., by key locks or passwords in conjunction with effective management controls).

NOTE Consideration can be given to enforcing time limits on bypass operation and to limiting the number of bypasses that can be active at any one time.

11.7.2.4 The SIS status information that is critical to maintaining the SIF shall be available as part of the operator interface. This information may include:

- where the process is in its sequence;
- indication that SIS protective action has occurred;
- indication that a protective function is bypassed;
- indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- status of sensors and final elements;
- the loss of energy where that energy loss impacts safety;
- the results of diagnostics;
- failure of environmental conditioning equipment which is necessary to support the SIS.

11.7.2.5 The SIS operator interface design (see 11.7.2.7) shall be such as to prevent changes to the SIS application program.

11.7.2.6 Where information is transferred from the BPCS to the SIS, systems, equipment or procedures shall be applied to confirm that the correct information has been transferred and that the safety integrity of the SIS is not compromised.

NOTE The systems, equipment or procedures used can include control over selective writing from the BPCS to specific SIS variables.

11.7.2.7 The design of the SIS operator interface via the BPCS operator interface shall be such that provision of incorrect information or data from the BPCS to the SIS shall not compromise safety.

11.7.3 Maintenance/engineering interface requirements

11.7.3.1 The design of the SIS maintenance/engineering interface shall ensure that any failure of this interface shall not adversely affect the ability of the SIS to carry out the required SIFs. This may require disconnecting of maintenance/engineering interfaces, such as programming panels, during normal SIS operation.

11.7.3.2 The maintenance/engineering interface shall provide the following functions with access security protection to each:

- SIS mode of operation, program, data, means of disabling alarm communication, test, bypass, maintenance;
- SIS diagnostics, voting and fault handling services;
- add, delete, or modify application program;
- data necessary to troubleshoot the SIS;
- where bypasses are required they should be installed such that alarms and manual shutdown facilities are not disabled.

11.7.3.3 The maintenance/engineering interface shall not be used as the operator interface.

11.7.3.4 Enabling and disabling the read-write access shall be carried out only by a configuration management process using the maintenance/engineering interface with appropriate documentation and security measures such as authentication and user secure channels.

11.7.4 Communication interface requirements

11.7.4.1 The design of any SIS communication interface shall ensure that any failure of the communication interface shall not adversely affect the ability of the SIS to achieve or maintain a safe state of the process.

11.7.4.2 When the SIS is able to communicate with the BPCS and peripherals, the communication interface, BPCS, or peripherals shall not adversely impact any of the SIFs within the SIS.

11.7.4.3 The communication interface shall be sufficiently robust to withstand electro-magnetic interference including power surges without causing a dangerous failure of the SIS.

11.7.4.4 The communication interface shall be suitable for communication between devices referenced to different electrical ground potentials.

NOTE An alternate medium (e.g., fibre optics) can be required.

11.8 Maintenance or testing design requirements

11.8.1 The design shall allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.

NOTE The term “end-to-end” means from process fluid at sensor end to process fluid at actuation end.

11.8.2 When on-line proof testing is required, test facilities shall be an integral part of the SIS design.

11.8.3 When test or bypass facilities are included in the SIS, they shall conform with the following:

- The SIS shall be designed in accordance with the maintenance and testing requirements defined in the SRS;
- The operator shall be alerted to the bypass of any portion of the SIS via an alarm or operating procedure.

11.8.4 The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.

11.8.5 Compensating measures that ensure continued safe operation shall be provided in accordance with 11.3 when the SIS is in bypass (repair or testing).

11.8.6 Forcing of inputs and outputs in PE SIS shall not be used as a part of application program(s), operating procedure(s) and maintenance (except as noted below).

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

11.9 Quantification of random failure

11.9.1 The calculated failure measure of each SIF shall be equal to, or better than, the target failure measure related to the SIL as specified in the SRS. This shall be determined by calculation.

NOTE In complex applications, the hazardous event frequency can be used as an alternative to the target failure measures (e.g., where different demand causes have different safety integrity requirements or where non-independent SISs act in sequence).

11.9.2 The calculated failure measure of each SIF due to random failures shall take into account all contributing factors including the following:

- a) the architecture of the SIS and of its SIS subsystems where relevant as they relate to each SIF under consideration;

- b) the estimated failure rate related to each failure mode, due to random hardware failures, which would contribute to a dangerous failure of the SIS but which are detected by diagnostic tests;
- c) the estimated failure rate related to each failure mode, due to random hardware failures, which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests but which are detected by proof tests;
- d) the estimated failure rate related to each failure mode, due to random hardware failure, which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests and undetected by proof tests;
- e) the susceptibility of the SIS to failures caused by the proof tests themselves;
- f) the susceptibility of the SIS to common cause failures;
- g) the diagnostic coverage of any periodic diagnostic tests, the associated diagnostic test interval and the probability of failure of the diagnostic facilities;
- h) the coverage of any periodic proof tests, the associated proof test procedure and the reliability for the proof test facilities and procedure;
- i) the repair times for detected failures and the state of the SIS during repairs (on line or off line);
- j) the estimated dangerous failure rate of any communication process in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);
- k) the estimated likelihood that operator response would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);
- l) the reliability of any utility necessary for the SIS.

NOTE Several modelling approaches are available and the most appropriate approach is a matter for the analyst and can depend on the circumstances. Available means include (see IEC 61508-6:2010, annex B):

- cause consequence analysis;
- reliability block diagrams;
- fault-tree analysis;
- Markov models;
- Petri nets models.

The probabilistic calculations can be performed analytically or by numerical simulation (e.g., Monte Carlo simulation).

11.9.3 The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified and shall be based on field feedback from similar devices used in a similar operating environment.

NOTE 1 This includes user collected data, vendor/provider/user data derived from data collected on devices, data from general field feedback reliability databases, etc. In some cases, engineering judgement can be used to assess missing reliability data or evaluate the impact on reliability data collected in a different operating environment.

NOTE 2 The lack of reliability data reflective of the operating environment is a recurrent shortcoming of probabilistic calculations. End-users can organize relevant device reliability data collections in accordance with IEC 60300-3-2:2004 or ISO 14224:2006 to improve the implementation of the IEC 61511 series.

NOTE 3 Vendor data based on returns can be restricted to a population where there is full knowledge of the operational environment and fully recorded in accordance with IEC 60300-3-2:2004 or ISO 14224:2006. The user can also record the operational environment for the SIF and be able to demonstrate that the vendor's operational environment data matches the environment of the SIF.

11.9.4 The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.

NOTE 1 The reliability data uncertainties can be evaluated according to the amount of field feedback (less field feedback results in more uncertainty) or/and exercise of expert judgement. Published standards (IEC 60605-4), Bayesian approaches, engineering judgement techniques, etc. can be used to estimate the reliability data uncertainties.

NOTE 2 The following techniques can be used for calculating the failure measures (more information can be found in IEC 61511-2:2016):

- use of an upper bound confidence of 70 % for each input reliability parameter instead of its mean in order to obtain conservative point estimations of the failure measures, or;
- use the probabilistic distributions functions of input reliability parameters, perform Monte Carlo simulations to obtain an histogram representing the distribution of the failure measure and assess a conservative value from this distribution (e.g., that there is a 90 % confidence that the true failure measure is better than the value calculated).

11.9.5 If, for a particular design, the target failure measure for the relevant SIF is not achieved then:

- a) identify the devices or parameters contributing most to the failure measure;

NOTE Fault tree cut-set analysis can be useful here.

- b) evaluate the effect of possible improvement measures on the identified devices or parameters (e.g., more reliable devices, additional defences against common mode failures, increased diagnostic or proof test coverage, increased redundancy, reduced proof test interval, staggering tests, etc.);
- c) select and implement improvement measures to establish the new result;
- d) compare the new result to the target failure measure and repeat the steps a) to d) until the target failure measure is achieved in a conservative manner.

12 SIS application program development

12.1 Objective

The objective of Clause 12 is to define the requirements for the development of the application program.

12.2 General requirements

12.2.1 The application program of the SIS shall be in accordance with the application program safety requirements (see 10.3.3) and all the requirements of this clause for all SIL up to and including SIL 3.

12.2.2 The application programmer shall review the information in the SRS and the application program safety requirements to ensure that the requirements are comprehensive, unambiguous, understandable and consistent. Any deficiencies in the application program safety requirements shall be identified and resolved, and if changes are made to the application program safety requirements, an impact analysis shall be carried out.

12.2.3 The IEC 61511 series addresses programming in Limited Variability Languages (LVL) and the use of devices using Fixed Program Languages (FPL). The IEC 61511 series does not address Full Variability Language (FVL) and the IEC 61511 series does not address SIL 4 application programming. Where function blocks are written in FVL then these shall be developed and modified under IEC 61508-3:2010.

12.2.4 Where the application program of the SIS is to implement both safety and non-safety functions, then all of the application program shall be treated as part of the SIS and shall comply with this standard and in addition, it shall be shown through assessment and test that the non-safety functions cannot interfere with the safety functions.

12.2.5 The application program shall be designed in such a way as to ensure that once the SIS has placed the process in a safe state, the process remains in the safe state, including under loss of power conditions and on power restoration, until a reset has been initiated unless otherwise directed by the SRS.

NOTE 1 If the SIF does not have a reset then there can be a documented engineering argument as to why it is acceptable to reinitiate the process without requiring the safe delay a reset would impose.

NOTE 2 More information can be found in 11.2.7.

12.2.6 During SIS start-up (or power up) the application program shall ensure that safety outputs remain in the safe state (typically de-energized state) until a reset has been initiated unless otherwise directed by the SRS.

12.2.7 The application program shall be designed in such a way that all parts of the application program are executed on every application program scan unless there is a specific alternate requirement that is supported in the safety manual. Process safety time requirements shall be considered when establishing application program scanning requirements.

12.2.8 The SIS application program and data shall be subject to modification, revision control, version management, back-up and restoration procedures.

12.2.9 ~~The application program specifies requirements for application programming for users and integrators of SISs. In particular, requirements for the following are specified~~ The SIS application program safety life cycle planning shall address the following aspects:

- SIS safety life-cycle phases and activities that are to be applied during the design and development of the application program. These requirements include the application of measures and techniques, which are intended to avoid errors in the application program and to control failures which may occur;
- information relating to the application program validation to be passed to the organization carrying out the SIS integration;
- preparation of information and procedures ~~concerning the application program~~ needed by the user for ~~the~~ operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications of the application program.

12.3 Application program design

12.3.1 An application program design shall address all SIS logic including all process operating modes for each SIF.

12.3.2 The input to the application program design shall be the SRS including the application program requirements (see Clause 10), the SIS architecture (see Clause 11) and the means and tools for developing the application program design (see 12.6). The application program design shall be consistent with and traceable back to the SRS.

12.3.3 The application program design shall allow an assessment of functional safety to be carried out.

12.3.4 The application program design and its decomposition into modules if applicable, shall address how the requirements are to be implemented, including the following as appropriate:

- the functions that enable the process to achieve or maintain a safe state;
- the specification of all identified application program components, and the description of connections and interactions between identified components;
- the timing constraints associated with the application program functions and their implementation in program scan time(s);
- a detailed description of the standard library modules (function blocks) being used;
- a detailed description of the application specific modules (function blocks) being used;
- a description of the way memory allocation has been achieved;
- the list of global variables used and the way in which their integrity is protected;

- identification of all non-SIF and the interfaces to non-safety related parts of the application program, to ensure that they cannot affect the proper operation of any SIF;
- definition of input and output interfaces, including tag listings and the associated data types;
- details of the data exchanged between the SIS application program and the operator interfaces;
- details of the data exchanged between the SIS application program and the BPCS and peripherals such as printers, data storage, etc.;
- how external and internal diagnostic information will be processed and logged;
- detailed description of how the operation and maintenance interfaces are implemented, including the way in which alarms are prioritised, indicated and accepted;
- a detailed description of any application level diagnostics that may be implemented such as external watch dogs, application data integrity checking, sensor validation to meet the required SIL;
- system configuration checks including the existence and accessibility of expected hardware devices and software modules;
- how the complexity in the application program design is minimised e.g., through use of modular design and simple functionality;
- functions related to the detection, annunciation and management of faults in SIS subsystems;
- functions related to the periodic testing of SIF on-line;
- functions related to the periodic testing of SIF off-line;
- functions that allow maintenance of the SIS to be carried out safely;
- references to documents on which the application program design specification is based.

12.3.5 The application program design shall ensure:

- completeness with respect to the SRS and its intended purpose;
- correctness with respect to the SRS and its intended purpose;
- freedom from ambiguity, i.e., clear to those who will utilize the document at any stage of the SIS safety life-cycle: this includes the use of terminology and descriptions which are unambiguous and understood by plant operators and system maintainers, as well as the application programmers;
- freedom from design faults.

12.4 Application program implementation

12.4.1 The application program development methodology shall comply with the development tools and restrictions given by the manufacturer of the SIS PE subsystem on which the application program shall be used.

12.4.2 The following information shall be contained in the application program or related documentation:

- a) the application program originator;
- b) a description of the purpose of the application program;
- c) the versions of the safety manuals that were used;
- d) identification of the dependency of each SIF on the parts (modules) of the application program;
- e) traceability to the application program safety requirements specification;
- f) identification of each SIF and its SIL;

- g) identification and description of the symbols used, including logic conventions, standard library functions, application library functions;
- h) identification of the SIS logic solver input and output signals;
- i) where the overall SIS utilises communications, a description of the communications information flow;

NOTE An example would be where a SIF uses several logic solvers.

- 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 sub-systems and any limitations imposed by scan times;
- k) If required by the SRS, the means by which:
 - the correctness of field data is ensured, (e.g., comparison between analog sensors to improve the diagnostic coverage);
 - the correctness of data sent over a communication link is ensured (e.g., when communicating from an HMI, before implementation of a command an 'ack' or 'acknowledge' is transmitted);
 - communications are made secure (e.g., cyber security measures);
- l) version identification and a history of changes.

12.4.3 If previously developed application program library functions are to be used as part of the design, their suitability shall be justified and based upon:

- compliance to IEC 61508; if proven-in-use evaluation for FVL in compliance to IEC 61508-3:2010 is undertaken, the programmable devices on which the application program library functions execute shall also be evaluated as proven-in-use according to IEC 61508-2:2010; or
- compliance to IEC 61511 prior use requirements (see 11.5.4 or 11.5.5) when using FPL or LVL;
- in all cases, demonstrating that any unused functions do not adversely impact the application program.

12.4.4 The application program shall be produced in a structured way so as to achieve:

- modular decomposition of the functionality;
- keep the complexity of SIF application program to a minimum consistent with that of the complexity of the required SIF;
- testability of functionality (including fault tolerant features) and of the internal structure of the application program;
- traceability to, and explanation of, application functions and associated constraints;
- one to one mapping between the hardware architecture and application program architecture.

12.5 Requirements for application program verification (review and testing)

12.5.1 Verification planning shall be carried out in accordance with Clause 7.

12.5.2 The application program including its documentation shall be reviewed by a competent person not involved in the original development. The approach used for the review and the review results shall be documented.

12.5.3 The application program, including its decomposition into modules if appropriate, shall be verified through review, analysis, simulation and testing techniques using written procedures and test specifications, that shall be carried out to confirm that the application program functions meet the SRS and that unintended functions are not executed and that there are no unintended side effects with respect to the SIF. The following shall be addressed:

- conformance to the application program design specification, the defined means and procedures, and the requirements of safety validation and test planning;
- exercising of all parts of the application program;
- exercising a representative range of data conditions;
- testing for failure conditions (i.e., negative testing);
- timing and the sequence of execution;
- testing of communications to and from the SIS;

~~NOTE—Wherever feasible the communication overload condition can be verified and tested.~~

- integration of the off-line application program with the logic solver hardware and the underlying PE;
- internal data flow checks to confirm that the logic solver is not just apparently working, but is working as expected;
- when possible, integration of the application program and 3rd party devices.

12.5.4 The mapping of the I/O data to the application program, including data type and range, shall be verified.

12.5.5 During testing, modifications to the application program shall be subject to an impact analysis in order to determine:

- all application program parts impacted;
- the necessary re-design and re-verification activities.

12.5.6 The results of application program testing shall be documented and include:

- the versions of the application program and its supporting documentation being tested;
- the versions of supporting software and test tools;
- names of the person(s) who performed the tests and reviews and dates;
- descriptions of the tests, reviews and dates performed;
- the test results;
- whether the objective and criteria of the tests have been met;
- if there was a failure during the test, the reasons why the failure occurred, the analysis of the failure and the records of its correction and re-test requirements.

12.6 Requirements for application program methodology and tools

12.6.1 The application program development shall comply with the constraints in the applicable safety manual(s).

~~NOTE—When reviewing the safety manual(s) can be reviewed and~~, if required for a specific application, additional procedures for and/or constraints on the use of methodologies and tools can be implemented.

12.6.2 Methods, techniques and tools shall be selected and applied for each life-cycle phase so as to:

- minimize the risk of introducing faults into the application program;
- reveal and remove faults that already exist in the application program;
- ensure as far as is practicable that any faults remaining in the application program will not lead to unacceptable results;
- enhance the means of managing modifications of the application program throughout the lifetime of the SIS;
- provide evidence that the application program has the required quality.

13 Factory acceptance test (FAT)

13.1 Objective

The objective of Clause 13 is to test the devices of the SIS to ensure that the requirements defined in the SRS are met.

NOTE 1 By testing the logic solver, associated software and hardware prior to installation, errors can be readily identified and corrected.

NOTE 2 The FAT is sometimes referred to as an integration test and can be part of the validation.

NOTE 3 Testing of field elements together with the logic solver can be recommended when there needs to be a high confidence in operation prior to final installation, e.g., subsea applications.

13.2 Recommendations

13.2.1 The need for a FAT shall be specified during the safety planning for a project.

NOTE 1 Close co-operation between the logic solver supplier and design contractor can be required in order to develop the integration tests.

NOTE 2 The activities follow the design and development phases and precede the installation and commissioning.

NOTE 3 The activities are applicable to the SIS subsystems with or without programmable electronics.

NOTE 4 It is usual for the FAT to take place in a factory environment prior to installation and commissioning in the plant.

13.2.2 The planning for a FAT shall specify the following:

- Types of tests to be performed including black-box system functionality tests; performance tests; internal checks; performance tests; environmental tests; interface testing; testing in degraded or faulted condition; exception testing; testing for safe reaction in case of power failure (including restart after power restored); and application of the SIS maintenance and operating manuals;

NOTE 1 Black-box functionality testing is a test design method that treats the system as a “black box”, so it does not explicitly use knowledge of its internal structure. Black-box test design is usually described as focusing on testing function requirements. Synonyms for black box include behavioural, functional, opaque-box, and closed-box testing.

NOTE 2 Performance tests determine whether the system meets timing, reliability and availability, integrity, safety targets and constraints.

NOTE 3 Environmental tests include EMC, life-and stress-testing.

NOTE 4 Internal data flow checks can be carried out to confirm that the SIS is processing input data and generating output response as specified.

- Test cases, test description and test data;

NOTE 5 Clarity in defining who is responsible for developing the test case and who is going to be responsible for carrying out the test and witnessing the test can be very important.

- Dependence on other systems/interfaces;
- Test environment and tools;
- Logic solver, sensor and final element configuration;
- Test criteria on which the completion of the test shall be judged;
- Procedures for corrective action on failure of test;
- Test personnel competences;
- Physical location;
- Hazards posed by the testing especially dealing with stored energy;
- A clear diagram of the test-set up.
- Recording of tests conducted, data, results and observations whilst the tests are being conducted.

NOTE 6 Tests that cannot be physically demonstrated are normally resolved by a formal line of reasoning as to why the SIS achieves the requirement, target or constraint.

13.2.3 The FAT shall take place on a defined version of the logic solver.

13.2.4 The FAT shall be conducted in accordance with the FAT planning. These tests shall show that all the logic performs correctly.

13.2.5 For each test carried out the following shall be addressed:

- the version of the test planning being used;
- the SIF and performance characteristic being tested;
- the detailed test procedures and test descriptions;
- a chronological record of the test activities;
- the tools, equipment and interfaces used.

13.2.6 The results of FAT shall be documented, stating

- the test cases;
- the test results;
- whether the objectives and test criteria have been met.

If there is a failure during test, the reasons for the failure shall be documented and analysed and the appropriate corrective action should be implemented.

13.2.7 During FAT, any modification or change shall be subject to a safety analysis to determine:

- the extent of impact on each SIF;
- the extent of testing and verification which shall be defined and implemented.

NOTE Commissioning can commence whilst corrective action is undertaken, depending on the results of the FAT.

14 SIS installation and commissioning

14.1 Objectives

The objectives of the requirements of Clause 14 are to:

- install the SIS according to the specifications and drawings;
- commission the SIS so that it is ready for final system validation.

NOTE The purpose of commissioning activities is to ensure that each of the SIS devices is individually ready to operate, as specified in the design phase.

14.2 Requirements

14.2.1 Installation and commissioning planning shall define all activities required for installation and commissioning. The planning shall provide the following:

- the installation and commissioning activities;
- the procedures, measures and techniques to be used for installation and commissioning;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities.

Installation and commissioning planning may be integrated in the overall project planning where appropriate.

14.2.2 All SIS devices shall be properly installed according to the design and installation plan(s).

14.2.3 The SIS shall be commissioned in accordance with planning in preparation for the final system validation. Commissioning activities shall include, but not be limited to, confirmation of the following:

- earthing (grounding) has been properly connected;
- energy sources have been properly connected and are operational;
- transportation stops and packing materials have been removed;
- no physical damage is present;
- all instruments have been properly calibrated and configured;
- all field devices are operational;
- logic solver and input/outputs are operational;
- the interfaces to other systems and peripherals are operational;
- all communications between remote SIS systems are operational.

14.2.4 Appropriate records of the commissioning of the SIS shall be produced, stating the results of the activities and whether the objectives and criteria identified during the design phase have been met. If there is a failure, the reasons for the failure shall be recorded.

14.2.5 Where it has been established that the actual installation does not conform to the design information then the difference shall be evaluated by a competent person and impact of the difference on safety shall be determined. If it is established that the difference has no impact on safety, then the design information shall be updated to “as-built” status. If the difference has a negative impact on safety, then the installation shall be modified to meet the design requirements.

15 SIS safety validation

15.1 Objective

The objective of the requirements of Clause 15 is to validate, through inspection and testing, that the installed and commissioned SIS and its associated SIF(s) achieve the requirements as stated in the SRS.

NOTE This is sometimes referred to as a site acceptance test (SAT).

15.2 Requirements

15.2.1 Validation planning of the SIS shall be carried out throughout the SIS safety life-cycle and shall define all activities and equipment required for validation. The following items shall be included:

- the validation activities including validation of the SIS with respect to the SRS including implementation and resolution of resulting recommendations;
- validation of all relevant process operating modes of the process and its associated equipment including;
 - preparation for use including setting and adjustment;
 - start-up, automatic, manual, semi-automatic, steady state of operation;
 - re-setting, shutdown, maintenance;
 - other modes identified in previous phases of the SIS safety life-cycle;

- the procedures, measures and techniques to be used for validation, including how validation activities can be performed, without putting the plant and process at risk of the hazardous events the SIS is to protect against;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities and the levels of independence for validation activities;
- reference to information against which validation shall be carried out (e.g., cause and effect chart);
- the equipment and facilities that needs to be installed or made available (e.g. isolation valves and leak detection equipment that will be needed for the testing of valves).

NOTE Examples of validation activities include loop testing, logic testing, calibration procedures, simulation of application program.

15.2.2 Validation planning for the application program shall include the following:

- identification of the application program functions which needs to be validated for each process operating mode before commissioning begins;
- the technical strategy for the validation including (where relevant):
 - manual and automated techniques;
 - static and dynamic techniques;
 - analytical and statistical techniques.
- in accordance with the preceding bullet, the measures (techniques) and procedures that will be used for confirming that each SIF conforms with the specified safety requirements and the specified SIL;
- the required environment in which the validation activities are to take place (e.g., for tests this would include calibrated tools and equipment);
- the application program;
- the pass/fail criteria for accomplishing validation including:
 - the required process and operator input signals with their sequences and their values;
 - the anticipated output signals with their sequences and their values;
 - other acceptance criteria, for example memory usage, timing and value tolerances.
- the policies and procedures for evaluating the results of the validation, particularly failures;
- all documents (see Clause 19) are validated for accuracy, consistency and traceability of the SIF from inception during the H&RA through the final installed SIF.

15.2.3 Where measurement accuracy is required as part of the validation then instruments used for this function should be calibrated against a specification traceable to a standard within an uncertainty appropriate to the application. If such a calibration is not feasible, an alternative method shall be used and documented.

15.2.4 The validation of the SIS and its associated SIF(s) shall be carried out in accordance with the SIS validation planning. Validation activities shall include, but not be limited to, the following:

- confirmation that the SIS performs under normal and abnormal process operating modes (e.g., start-up, shutdown) as identified in the SRS;
- confirmation that adverse interaction of the BPCS and other connected systems do not affect the proper operation of the SIS;
- the SIS properly communicates (where required) with the BPCS or any other system or network, including during abnormal conditions such as a data overload;

- sensors, logic solver, and final elements perform in accordance with the SRS, including all redundant channels, including abnormal condition such as data overload;

NOTE If a factory acceptance test (FAT) was performed on the logic solver as described in Clause 13, credit can be taken for validation of the logic solver by the FAT. After all equipment is installed in the plant, full loop validation will test the logic solver functionality and its connections to other SIS subsystems.

- SIS design documentation is consistent with the installed system;
- confirmation that the SIF performs as specified on invalid process variable values (e.g., out of range);
- the proper shutdown sequence is activated;
- the SIS provides the proper annunciation and proper operation display;
- computations that are included in the SIS are correct for expected range of values but also at limits and over the limits;
- the SIS reset functions perform as defined in the SRS;
- bypass functions operate correctly;
- start-up overrides operate correctly;
- manual shutdown systems operate correctly;
- the proof-test policy documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- confirmation that the SIS performs as required on loss of utilities (e.g., electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the SIS returns to the desired state;
- confirmation that the EMC immunity, as specified in the SRS (see 10.3), has been achieved.

15.2.5 The validation of the application program shall determine whether:

- all of the specified application program safety requirements (see 10.3.2) are correctly performed;
- the application program does not jeopardize the safety requirements under SIS fault conditions and in degraded modes of operation and for BPCS fault conditions for any interfaces between the SIS and BPCS;
- the application program does not jeopardize the safety requirements by executing “unused” software functionality, i.e., functionality not defined in the specification.

The information of the validation activities shall be available.

15.2.6 The results from the validation plan activities shall represent and cover the entire SIS validation process. SIS validation documentation shall be produced which provides:

- the version of the SIS validation planning being used;
- the SIF(s) under test (or analysis), along with the specific reference to the requirement identified during the SIS validation planning;
- tools and equipment used, along with their calibration data;
- the results of each test;
- the version of the test specification used;
- the criteria for acceptance of the completed tests;
- the version of the SIS hardware, application program(s), and other software being tested;
- any discrepancy between expected and actual results and the resolution of that discrepancy;

- the analysis made and the decisions taken on whether to continue the test or to issue a change request, in the case where discrepancies occur.

15.2.7 The results shall be verified against the expected results. All discrepancies shall be analysed and the findings shall be available as part of the validation documentation. This shall include the analysis made and the decisions taken on whether to continue the validation or to issue a change request and to return to an earlier part of the development life-cycle.

15.2.8 After the SIS validation and prior to the identified hazards being present, the following activities shall be carried out:

- all bypass functions (e.g., PE logic solver and PE sensor forces, disabled alarms) shall be returned to their normal position;
- all process isolation valves shall be set according to the process start-up requirements and procedures;
- all test materials (e.g., fluids) shall be removed;
- all commissioning overrides and force permissives shall be removed.

16 SIS operation and maintenance

16.1 Objectives

The objectives of the requirements of Clause 16 are to ensure that:

- the required SIL of each SIF is maintained during operation and maintenance;
- the SIS is operated and maintained in a way that sustains the required safety integrity.

16.2 Requirements

16.2.1 Operation and maintenance planning for the SIS shall be carried out. It shall provide the following:

- routine and abnormal operation activities;
- inspection, proof testing, preventive and breakdown maintenance activities;
- the procedures, measures and techniques to be used for operation and maintenance;
- the operational response to faults and failures identified by diagnostics, inspections or proof-tests;
- verification of conformity to operations and maintenance procedures;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities;
- a SIS maintenance plan.

NOTE The SIS maintenance plan can state different maintenance features depending on the SIL level.

16.2.2 Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:

- a) the routine methods and procedures which need to be carried out to maintain the "as designed" functional safety of the SIS;
- b) the procedures used to ensure the quality and consistency of proof testing, and to ensure adequate validation is being performed after replacement of any device;
- c) the measures and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (e.g., when a system needs to be bypassed for testing or maintenance, what additional risk reduction needs to be implemented);
- d) the methods and procedures which are used to test the diagnostics;

e) the information which needs to be maintained on SIS failure and the demand rates on the SIS;

f) procedures for collecting data related to the demand rate and SIS reliability parameters;

NOTE 1 Collection and analysis of failure data has many benefits including the potential to reduce maintenance costs if failures rates in operation are significantly lower than what were predicted during design. Implementation costs of new installations can also be reduced because new designs can be based on less conservative failure rates.

g) the information which needs to be maintained showing results of audits and tests on the SIS;

h) the maintenance procedures to be followed when faults or failures occur in the SIS, including:

- procedures for fault diagnostics and repair;
- procedures for revalidation;
- maintenance reporting requirements;
- procedures for tracking maintenance performance.

NOTE 2 Considerations include:

- procedures for reporting failures;
- procedures for analysing systematic failures;
- the actions to allow safe shutdown in the event of BPCS failure;
- ensuring that test equipment is properly calibrated and maintained.

16.2.3 Operation procedures shall be made available. Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.). The operator shall be provided with information on the procedures to be applied before and during bypass and what should be done before the removal of the bypass and the maximum time allowed to be in the bypass state. This information shall be reviewed on a regular basis.

NOTE The operating and maintenance procedures can include verification that bypasses are removed after proof testing.

16.2.4 Continued process operation with a SIS device in bypass shall only be permitted if a hazards analysis has determined that compensating measures are in place and that they provide adequate risk reduction. Operating procedures shall be developed accordingly.

16.2.5 Operation and maintenance shall proceed in accordance with the relevant procedures.

16.2.6 Operators shall be trained on the function and operation of the SIS in their area. This training shall ensure that they understand:

- how the SIS functions (trip points and the resulting action that is taken by the SIS);

NOTE 1 This can also include impact of an SIS action to remaining operational plant.

- the hazard the SIS is protecting against;
- the correct operation and management of all bypass/override switches and under what circumstances these bypasses are to be used;
- the operation of any manual shutdown switches and manual start-up activity and when these manual switches are to be activated;

NOTE 2 This can include “system reset” and “system restart”.

- expectation on activation of any diagnostic alarms (e.g., what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS);
- the proper verification of the diagnostics.

16.2.7 The status of all bypasses shall be recorded in a bypass log. All bypasses need authorization and indication.

16.2.8 Maintenance personnel shall be trained as required to sustain full functional performance of the SIS (hardware and software) to meet the target SIL of each SIF.

16.2.9 Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:

- the demand rate on each SIF (see 5.2.5.3);
- the actions taken following a demand on the system;
- the failures and failure modes of equipment forming part of the SIS, including those identified during normal operation, inspection, testing or demand on a SIF;
- the cause of the demands;
- the cause and frequency of spurious trips;
- the failure of equipment forming part of any compensating measures

16.2.10 The operation and maintenance procedures may require revision, if necessary, following:

- functional safety audits;
- tests on the SIS;
- experience from normal or abnormal operation and maintenance events.

16.2.11 Written proof-test procedures shall be developed for every SIF to reveal dangerous failures undetected by diagnostics. These written test procedures shall describe every step that is to be performed and shall include:

- the correct operation of each sensor and final element;
- correct logic action;
- correct alarms and indications.

NOTE The following methods can be used to determine the undetected failures that need to be tested:

- examination of fault trees;
- failure mode and effect analysis;
- reliability centred maintenance.

16.2.12 SIS spare parts shall be identified and shall be made available to minimize the bypass duration due to unavailability of any replacement part for the SIS.

NOTE Replacements that are not in kind (like for like) can be managed as a modification to the SIS.

16.2.13 Persons responsible for operations and maintenance shall review the hazard and risk analysis, allocation and design to ensure the assumptions made are valid e.g. assumptions on occupancy and corrosion protection.

16.3 Proof testing and inspection

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.

NOTE 1 Particular attention can be made to identify failure causes that may lead to common cause failures.

NOTE 2 Functional test procedures can also emphasize the need to avoid introducing common cause failures.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).

NOTE Testing of the SIS can be performed either end-to-end or in segments (see 11.8.1).

16.3.1.3 The schedule for the proof tests shall be according to the SRS. The frequency of proof tests for a SIF shall be determined through PFD_{avg} or PFH calculation in accordance with 11.9 for the SIS as installed in the operating environment.

NOTE Different parts of the SIS can require different test intervals, for example, the logic solver can require a different test interval than the sensors or final elements.

16.3.1.4 Any deficiencies found during the proof testing shall be repaired in a safe and timely manner. A proof test shall be repeated after the repair is completed.

16.3.1.5 At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.

NOTE The user can adjust the test frequency based on this data and an analysis of the original basis for test frequency.

16.3.1.6 Any change to the application program requires full validation and a proof test of any SIF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were designed per the updated safety requirements and correctly implemented.

16.3.1.7 Suitable management procedures shall be applied to review deferrals and prevent significant delay to proof testing.

16.3.2 Inspection

Each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (e.g., missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation).

NOTE These problems could indicate an increase in the frequency of faults.

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

- a) description of the tests and inspections performed including identification of the test procedure used;
- 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 including the "as-found" condition, all faults found (including the failure mode) and the "as-left" condition.

17 SIS modification

17.1 Objectives

The objectives of the requirements of Clause 17 are:

- that modifications to any SIS are properly planned, reviewed, approved and documented prior to making the change;
- to ensure that the required safety integrity of the SIS is maintained despite of any changes made to the SIS.

NOTE Modifications to the BPCS, other equipment, process or operating conditions can be reviewed to determine whether they are such that the nature or frequency of demands on the SIS will be affected. Those having an adverse effect can be considered further to determine whether the level of risk reduction will still be sufficient.

17.2 Requirements

17.2.1 Prior to carrying out any modification to a SIS, procedures for authorizing and controlling changes shall be in place.

17.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and the hazards that may be affected.

17.2.3 Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification could impact safety then there shall be a return to the first phase of the SIS safety life-cycle affected by the modification.

17.2.4 Safety planning for the modification and re-verification shall be available. Modifications and re-verifications shall be carried out in accordance with the planning.

17.2.5 All documentation affected by the modification shall be updated.

17.2.6 Modification activity shall not begin until a FSA is completed in accordance with 5.2.6.1.9 and after proper authorisation.

17.2.7 Appropriate information shall be maintained for all changes to the SIS. The information shall include:

- a description of the modification or change;
- the reason for the change;
- identified hazards and SIFs which may be affected;
- an analysis of the impact of the modification activity on the SIS;
- all approvals required for the changes;
- tests used to verify that the change was properly implemented and the SIS performs as required;
- details of all SIS modification activities (e.g., a modification log);
- appropriate configuration history;
- tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.

17.2.8 Modification shall be performed with qualified personnel who have been properly trained. All affected and appropriate personnel should be notified of the change and trained with regard to the change.

18 SIS decommissioning

18.1 Objectives

The objectives of the requirements of Clause 18 are to ensure that:

- prior to decommissioning any SIS from active service, a proper review is conducted and required authorization is obtained;
- the required SIF(s) remain operational during decommissioning activities.

18.2 Requirements

18.2.1 Prior to carrying out any decommissioning of part or all of a SIS or SIF, procedures for authorizing and controlling changes shall be in place.

18.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and identifying the hazards that may be affected.

18.2.3 An analysis shall be carried out on the impact on functional safety as a result of the proposed decommissioning activity. The assessment shall include an update of the H&RA sufficient to determine the scope of impact to the SIS safety life cycle. The subsequent SIS safety life-cycle phases shall need to be re-evaluated. The assessment shall also consider:

- functional safety during the execution of the decommissioning activities;
- the impact of decommissioning the SIS on adjacent operating units and facility services.

18.2.4 The results of the impact analysis shall be used during safety planning to re-implement the relevant requirements of the IEC 61511 series including re-verification and re-validation.

18.2.5 Decommissioning activities shall not begin without proper documentation and authorization.

19 Information and documentation requirements

19.1 Objectives

The objectives of the requirements of Clause 19 are to ensure that the necessary information is available and documented in order that:

- all phases of the SIS safety life-cycle can be effectively performed;
- verification, validation and FSA activities can be effectively performed.

19.2 Requirements

19.2.1 The documentation required by the IEC 61511 series shall be available to personnel implementing the requirements of the IEC 61511 series.

19.2.2 The documentation shall:

- describe the installation, system or equipment and the use of it;
- be accurate and up to date;
- be easy to understand;
- suit the purpose for which it is intended;
- be available in an accessible, maintainable and editable form, so that appropriate and relevant documents can be readily and accurately identified, located, retrieved and revised.

NOTE Further details of the requirements for information are included in Clause 14 and Clause 15.

19.2.3 The documentation shall have unique identities so it shall be possible to reference the different parts.

19.2.4 The documentation shall have designations indicating the type of information.

19.2.5 The documentation shall be traceable to the functional and integrity requirements arising from this standard, including the H&RA.

19.2.6 The documentation shall have a revision index (for example, version numbers) to make it possible to identify different versions of the information.

19.2.7 The documentation shall be structured to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document.

NOTE The physical structure of the documentation can vary depending upon a number of factors such as the size of the system, its complexity and the organizational requirements.

19.2.8 All relevant documentation shall be revised, amended, reviewed, approved and shall be under the control of an appropriate information control scheme.

19.2.9 Current documentation pertaining to the following shall be maintained:

- a) the results of the H&RA and the related assumptions;
- b) the equipment used for SIF together with its safety requirements;
- c) the organization responsible for maintaining functional safety;
- d) the procedures necessary to achieve and maintain functional safety of the SIS;
- e) the modification information as defined in 17.2.5;
- f) the safety manual(s);
- g) design, implementation, test and validation.

NOTE Further details of the requirements for information are included in 12.4.2, Clauses 14 and 15 and in 16.3.3.

Bibliography

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at <http://www.electropedia.org/>)

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

IEC 60300-3-2:2004, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60605-4:2001, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60617-12:1997, *Graphical symbols for diagrams – Part 12: Binary logic elements*¹

IEC TS 61000-1-2:2008, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61131-3:2013, *Programmable controllers – Part 3: Programming language*

IEC 61131-6:2012, *Programmable controllers – Part 6: Functional Safety*

IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations*

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*

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

IEC 61511-3:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443-2-1:2010, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC 62682:2014, *Management of alarms for the process industry*

ISO/IEC 2382:2006, *Information technology – Vocabulary*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

¹ Withdrawn.

ISO/IEC 90003:2014, *Software engineering – Part 3: Guidelines for the application of ISO 9001:2000 to computer software*

ISO 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

ISO 9001:2008, *Quality management systems – Requirements*

ISO TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

ISO 13849-1:2006, *Safety of machinery – Safety related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety related parts of control systems – Part 2: Validation*

ISO 14224:2006, *Petroleum, petrochemical and natural gas industries- Collection and exchange of reliability and maintenance of data for equipment*

ISA TR 84.00.04 Part 1:2015, *Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

ISA TR 84.00.09:2013, *Security Countermeasures Related to Safety Instrumented Systems (SIS)*

SOMMAIRE

AVANT-PROPOS	85
INTRODUCTION	87
1 Domaine d'application	91
2 Références normatives	97
3 Termes, définitions et abréviations	97
3.1 Termes	97
3.2 Termes et définitions	97
3.3 Abréviations	119
4 Conformité à l'IEC 61511-1:2016	120
5 Gestion de la sécurité fonctionnelle	120
5.1 Objectif	120
5.2 Exigences	120
5.2.1 Généralités	120
5.2.2 Organisation et ressources	120
5.2.3 Evaluation et gestion des risques	121
5.2.4 Planification de la sécurité	121
5.2.5 Mise en œuvre et surveillance	121
5.2.6 Evaluation, audits et révisions	122
5.2.7 Gestion de configuration du SIS	125
6 Exigences relatives au cycle de vie de sécurité	125
6.1 Objectifs	125
6.2 Exigences	127
6.3 Exigences relatives au cycle de vie de sécurité du SIS du programme d'application	130
7 Vérification	133
7.1 Objectif	133
7.2 Exigences	133
8 Analyse de danger et de risque du processus	135
8.1 Objectifs	135
8.2 Exigences	135
9 Affectation des fonctions de sécurité aux couches de protection	136
9.1 Objectifs	136
9.2 Exigences relatives au processus d'allocation	137
9.3 Exigences relatives au système de commande de processus de base en tant que couche de protection	139
9.4 Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes	141
10 Spécification des exigences de sécurité (SRS) du SIS	141
10.1 Objectif	141
10.2 Exigences générales	142
10.3 Exigences de sécurité du SIS	142
11 Conception et ingénierie du SIS	144
11.1 Objectif	144
11.2 Exigences générales	144
11.3 Exigences relatives au comportement du système lors de la détection d'une anomalie	146

11.4	Tolérance aux défauts du matériel	146
11.5	Exigences relatives au choix des appareils	148
11.5.1	Objectifs	148
11.5.2	Exigences générales	148
11.5.3	Exigences relatives au choix des appareils basés sur l'utilisation préalable	148
11.5.4	Exigences relatives au choix des appareils programmables FPL (p. ex.: appareils de terrain) basés sur l'utilisation préalable	149
11.5.5	Exigences relatives au choix des appareils programmables LVL basés sur l'utilisation préalable	150
11.5.6	Exigences relatives au choix des appareils programmables FVL	151
11.6	Appareils de terrain	151
11.7	Interfaces	151
11.7.1	Généralités	151
11.7.2	Exigences relatives à l'interface opérateur	151
11.7.3	Exigences relatives à l'interface de maintenance/d'ingénierie	152
11.7.4	Exigences relatives à l'interface de communication	153
11.8	Exigences relatives à la maintenance ou à la conception des essais	153
11.9	Quantification de défaillance aléatoire	154
12	Développement du programme d'application du SIS	155
12.1	Objectif	155
12.2	Exigences générales	156
12.3	Conception du programme d'application	156
12.4	Mise en œuvre du programme d'application	158
12.5	Exigences relatives à la vérification du programme d'application (revue et essai)	159
12.6	Exigences relatives à la méthodologie et aux outils du programme d'application	160
13	Essai de réception en usine (ERU)	161
13.1	Objectif	161
13.2	Recommandations	161
14	Installation et mise en service du SIS	162
14.1	Objectifs	162
14.2	Exigences	162
15	Validation de sécurité du SIS	163
15.1	Objectif	163
15.2	Exigences	163
16	Fonctionnement et maintenance du SIS	166
16.1	Objectifs	166
16.2	Exigences	166
16.3	Essais périodiques et inspection	169
16.3.1	Essais périodiques	169
16.3.2	Inspection	170
16.3.3	Documentation des essais périodiques et de l'inspection	170
17	Modification du SIS	170
17.1	Objectifs	170
17.2	Exigences	171
18	Déclassement du SIS	171
18.1	Objectifs	171

18.2 Exigences	172
19 Exigences relatives aux informations et à la documentation.....	172
19.1 Objectifs	172
19.2 Exigences	172
Bibliographie.....	174
Figure 1 – Cadre général de la série IEC 61511.....	90
Figure 2 – Relations entre l'IEC 61511 et l'IEC 61508.....	93
Figure 3 – Relations détaillées entre l'IEC 61511 et l'IEC 61508	95
Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions.....	96
Figure 5 – Système électronique programmable (PES): structure et terminologie.....	110
Figure 6 – Exemple d'architectures SIS comprenant trois sous-systèmes SIS.....	113
Figure 7 – Phases de cycle de vie de sécurité d'un SIS et étapes FSA	127
Figure 8 – Cycle de vie de sécurité du programme d'application et ses relations avec le cycle de vie de sécurité du SIS	131
Figure 9 – Couches de protection types et moyens de réduction de risque.....	140
Tableau 1 – Abréviations utilisées dans l'IEC 61511	119
Tableau 2 – Vue d'ensemble du cycle de vie de sécurité d'un SIS (1 de 2)	128
Tableau 3 – Cycle de vie de sécurité du programme d'application: vue d'ensemble (1 de 2).....	132
Tableau 4 – Exigences concernant l'intégrité de sécurité: PFD_{avg}	137
Tableau 5 – Exigences concernant l'intégrité de sécurité: fréquence moyenne de défaillance dangereuse de la SIF.....	137
Tableau 6 – Exigences de HFT minimale en fonction du SIL	147

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

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.

DÉGAGEMENT DE RESPONSABILITÉ

Cette version consolidée n'est pas une Norme IEC officielle, elle a été préparée par commodité pour l'utilisateur. Seules les versions courantes de cette norme et de son(ses) amendement(s) doivent être considérées comme les documents officiels.

Cette version consolidée de l'IEC 61511-1 porte le numéro d'édition 2.1. Elle comprend la deuxième édition (2016-02) [documents 65A/777/FDIS et 65A/784/RVD], son corrigendum 1 (2016-09) et son amendement 1 (2017-08) [documents 65A/844/FDIS et 65A/848/RVD]. Le contenu technique est identique à celui de l'édition de base et à son amendement.

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par l'amendement 1. Les ajouts sont en vert, les suppressions sont en rouge, barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

La Norme internationale IEC 61511-1 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 constitue une révision technique et inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- remplacement des références et exigences logiciel par des références et exigences de programmation d'application;
- exigences d'évaluation de la sécurité fonctionnelle décrites avec plus de détails pour améliorer la gestion de la sécurité fonctionnelle.
- ajout de la gestion des exigences de changement;
- ajout des exigences d'évaluation du risque de sécurité;
- extension des exigences au système de base de contrôle de processus comme couche de protection;
- modification des exigences relatives à la tolérance de panne matérielle et réexamen minutieux pour comprendre les options utilisateurs/intégrateurs.

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

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 la publication de base et de son amendement 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 et certains niveaux de performance minimaux.

La série IEC 61511 concerne l'application des SIS aux industries de transformation. La série IEC 61511 porte également sur la réalisation d'une analyse de danger et de risque relative au processus (H&RA) visant à en déduire la spécification relative aux SIS. D'autres contributions du système de sécurité sont uniquement prises en compte eu égard aux exigences de performance du SIS. Le SIS inclut tous les appareils nécessaires à l'acheminement de la SIF entre le capteur et l'élément terminal.

La série IEC 61511 aborde deux concepts essentiels à son application: le cycle de vie de sécurité des SIS et les niveaux d'intégrité de sécurité (SIL).

La série IEC 61511 concerne les SIS reposant sur l'utilisation d'une technologie électrique/électronique/électronique programmable. Si d'autres technologies sont utilisées pour les unités logiques, il convient d'appliquer les principes de base de la série IEC 61511 pour garantir que les exigences de sécurité fonctionnelle soient 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 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 principes minimaux. Cette approche a été adoptée afin de mettre en œuvre une politique technique cohérente et rationnelle.

Dans la plupart des cas, la sécurité est obtenue de la meilleure façon par une conception de processus à sécurité intrinsèque. Toutefois, dans certains cas, cela s'avère impossible ou peu pratique. Si nécessaire, cette approche peut être combinée à un ou plusieurs systèmes de protection afin de couvrir les risques résiduels identifiés éventuels. Les systèmes de protection peuvent reposer sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). Pour faciliter cette approche, la série IEC 61511:

- aborde la réalisation d'une analyse de danger et de risque pour identifier les exigences de sécurité globales;
- prend en compte l'affectation des exigences de sécurité aux SIS;
- s'inscrit dans un cadre applicable à tous les moyens instrumentés 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.

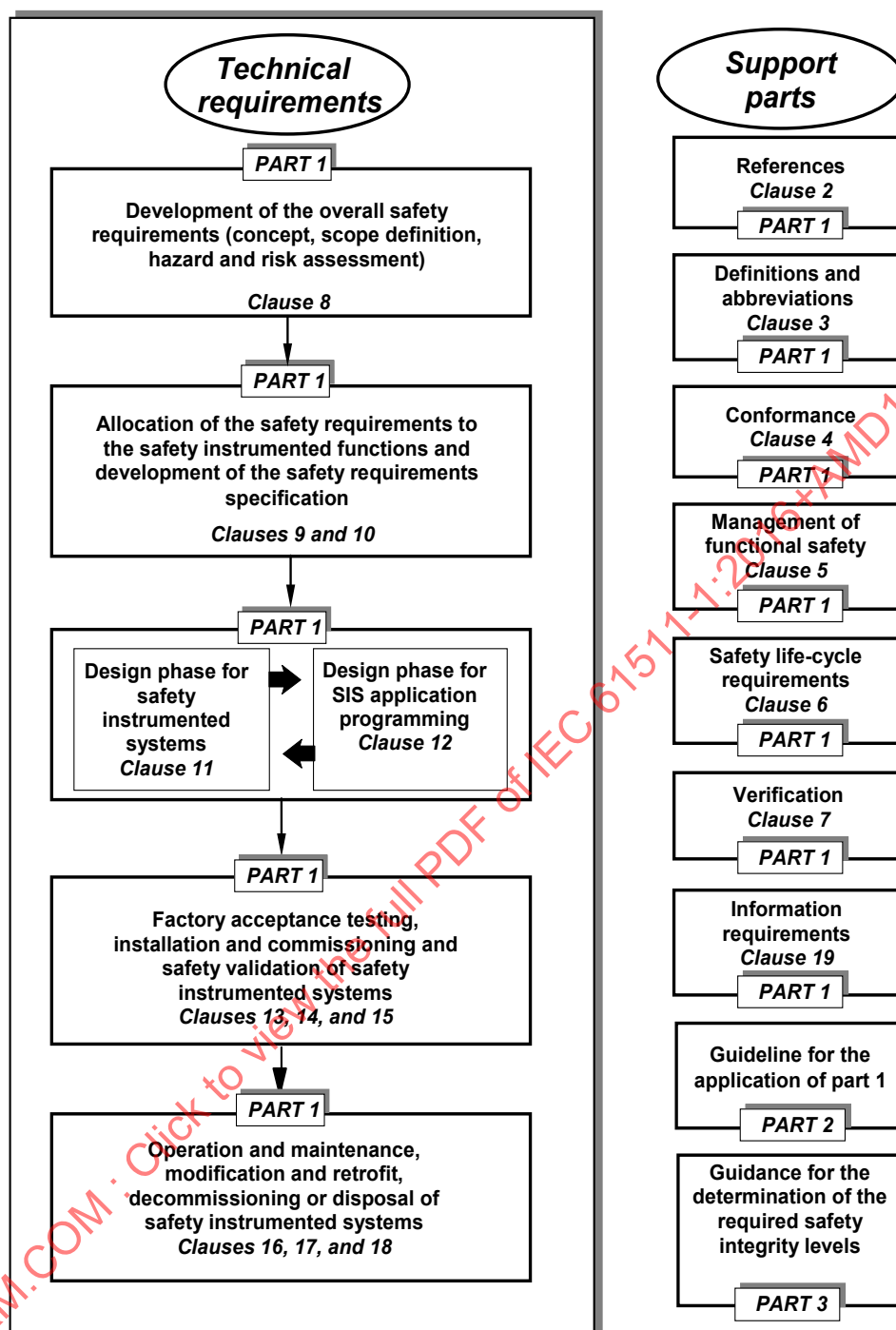
La série IEC 61511 relative aux SIS pour les industries de transformation:

- prend en compte toutes les phases relatives au cycle de vie de sécurité des SIS (concept initial, conception, mise en œuvre, fonctionnement, maintenance et déclassement);
- permet d'harmoniser les normes des industries de transformation nationales existantes ou nouvelles par rapport à la série IEC 61511.

L'IEC 61511 vise à obtenir un haut niveau de cohérence (p. ex.: des principes sous-jacents, de la terminologie et de l'information) dans le secteur des industries de transformation. Il convient de noter que cela présente des avantages tant du point de vue de la sécurité que du point de vue économique. La Figure 1 ci-dessous présente un cadre général de la série IEC 61511.

Dans les juridictions où les autorités compétentes (p. ex.: nationales, fédérales, étatiques, provinciales, cantonales, municipales) ont défini des réglementations relatives à la conception de la sécurité des processus, la gestion de la sécurité des processus ou autres, ces réglementations sont prioritaires par rapport aux exigences définies dans la série IEC 61511.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016+AMD1:2017 CSV



Anglais	Français
Technical requirements	Exigences techniques
PART 1	PARTIE 1
PART 2	PARTIE 2
PART 3	PARTIE 3
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
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification Clauses 9 and 10	Allocation 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
Guidance for the determination of the required safety integrity levels	Ligne directrice pour la détermination des niveaux d'intégrité de sécurité exigés

Figure 1 – Cadre général de la série IEC 61511

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

Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

1 Domaine d'application

La présente partie de l'IEC 61511 décrit les exigences relatives à la spécification, la conception, l'installation, au fonctionnement et à la maintenance d'un système instrumenté de sécurité (SIS, Safety Instrumented System) de manière à ce qu'il puisse être mis en œuvre en toute confiance pour établir ou maintenir le processus dans un état de sécurité convenable. L'IEC 61511-1 a été conçue pour être une mise en œuvre de l'IEC 61508:2010 dans le secteur des industries de transformation.

En particulier, l'IEC 61511-1:

- a) spécifie les exigences permettant d'obtenir la sécurité fonctionnelle, mais ne spécifie pas la responsabilité de la mise en œuvre des exigences (p. ex.: les concepteurs, les fournisseurs, la société propriétaire/exploitante, l'entrepreneur). Cette responsabilité sera assignée aux différentes parties selon la planification de la sécurité, la planification et la gestion de projets, ainsi que les règlements nationaux;
- b) s'applique lorsque des appareils satisfaisant aux exigences de la série IEC 61508 parue en 2010 ou de l'IEC 61511-1:2016 [115] sont intégrés dans un système qui doit être utilisé pour une application du secteur des industries de transformation. Elle ne concerne pas les fabricants qui souhaitent revendiquer la possibilité d'utiliser ces appareils dans les SIS du secteur des industries de transformation (voir l'IEC 61508-2:2010 et l'IEC 61508-3:2010);
- c) définit les relations entre les normes IEC 61511 et IEC 61508 (voir Figures 2 et 3);
- d) s'applique lorsque des programmes d'application sont développés pour des systèmes possédant un langage de variabilité limitée ou lors de l'utilisation d'appareil à langage de programmation figé, mais ne s'applique pas aux fabricants, concepteurs, intégrateurs et utilisateurs du SIS qui développent des logiciels intégrés (logiciels système) ou utilisent des langages de variabilité totale (voir l'IEC 61508-3:2010);
- e) s'applique à de nombreuses industries de transformation (p. ex.: produits chimiques, pétrole et gaz, pâte à papier et papier, produits pharmaceutiques, produits alimentaires et boissons, production d'électricité non-nucléaire);
NOTE 1 Dans le secteur des industries de transformation, certaines applications peuvent faire l'objet d'exigences supplémentaires qui doivent être satisfaites.
- f) met en évidence les relations entre les SIF et d'autres fonctions instrumentées (voir Figure 4);
- g) aboutit à l'identification des exigences fonctionnelles et des exigences concernant l'intégrité de sécurité relatives aux SIF en tenant compte de la réduction de risque obtenue par d'autres méthodes;
- h) spécifie les exigences relatives au cycle de vie de l'architecture du système et la configuration du matériel, ainsi que de la programmation d'application et de l'intégration du système;
- i) spécifie les exigences relatives à la programmation d'application pour les intégrateurs et utilisateurs de SIS;

- j) s'applique lorsque la sécurité fonctionnelle est obtenue en utilisant une ou plusieurs SIF pour la protection du personnel, la protection du grand public ou la protection de l'environnement;
 - k) peut s'appliquer dans des applications non liées à la sécurité (la protection de biens, par exemple);
 - l) définit les exigences pour la mise en œuvre des SIF dans le cadre des dispositions globales permettant d'obtenir la sécurité fonctionnelle;
 - m) utilise le cycle de vie de sécurité d'un SIS (voir Figure 7) et définit une liste des activités devant être réalisées pour déterminer les exigences fonctionnelles, ainsi que les exigences concernant l'intégrité de sécurité relatives au SIS;
 - n) spécifie qu'une H&RA doit être réalisée pour définir les exigences de sécurité fonctionnelle et les niveaux d'intégrité de sécurité (SIL) de chaque SIF;
- NOTE 2 Pour avoir une vue d'ensemble des moyens de réduction de risque, voir la Figure 9.
- o) établit des objectifs quantitatifs relatifs à la probabilité moyenne de défaillance en cas de sollicitation (en mode sollicitation) et à la fréquence moyenne de défaillance dangereuse (en mode sollicitation ou en mode continu) pour chaque SIL;
 - p) spécifie des exigences minimales pour la tolérance aux défauts du matériel (HFT);
 - q) spécifie les mesures et techniques exigées pour obtenir le SIL indiqué;
 - r) définit un niveau maximal de performance de sécurité fonctionnelle (SIL 4) qui peut être atteint pour une SIF mise en œuvre conformément à l'IEC 61511-1;
 - s) définit un niveau minimal de performance de sécurité fonctionnelle (SIL 1) au-dessous duquel l'IEC 61511-1 ne s'applique pas;
 - t) fournit un cadre pour l'établissement du SIL, mais ne spécifie pas le SIL exigé pour les applications spécifiques (qu'il convient d'établir sur la base de la connaissance de l'application particulière et par rapport à la réduction de risque globale souhaitée);
 - u) spécifie les exigences pour toutes les parties du SIS, depuis le capteur jusqu'à l'élément terminal ou jusqu'aux éléments terminaux;
 - v) définit les informations qui sont nécessaires pendant le cycle de vie de sécurité du SIS;
 - w) spécifie que la conception du SIS tient compte des facteurs humains;
 - x) n'applique aucune exigence directe relative à l'opérateur individuel ou au technicien de maintenance.

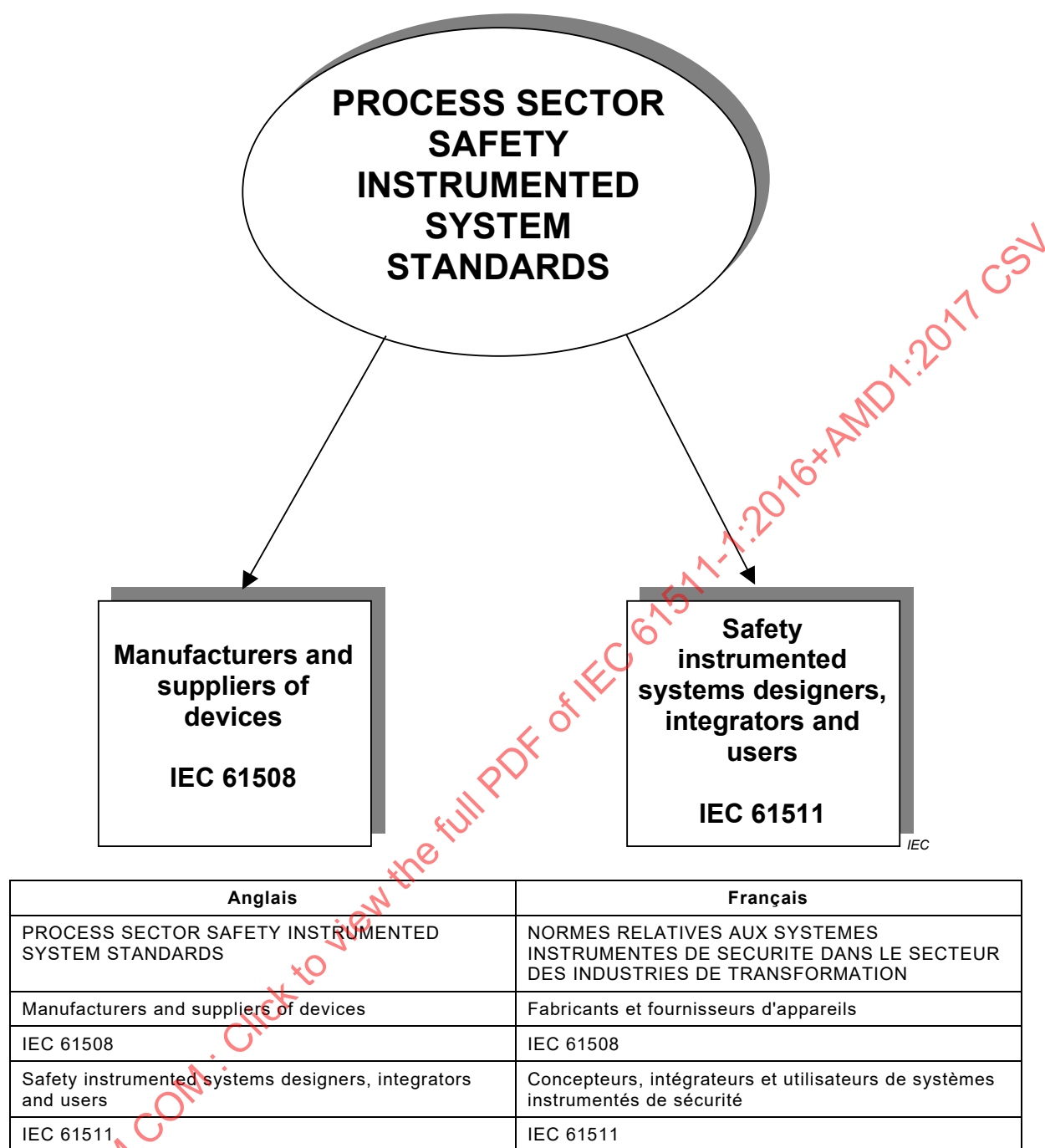
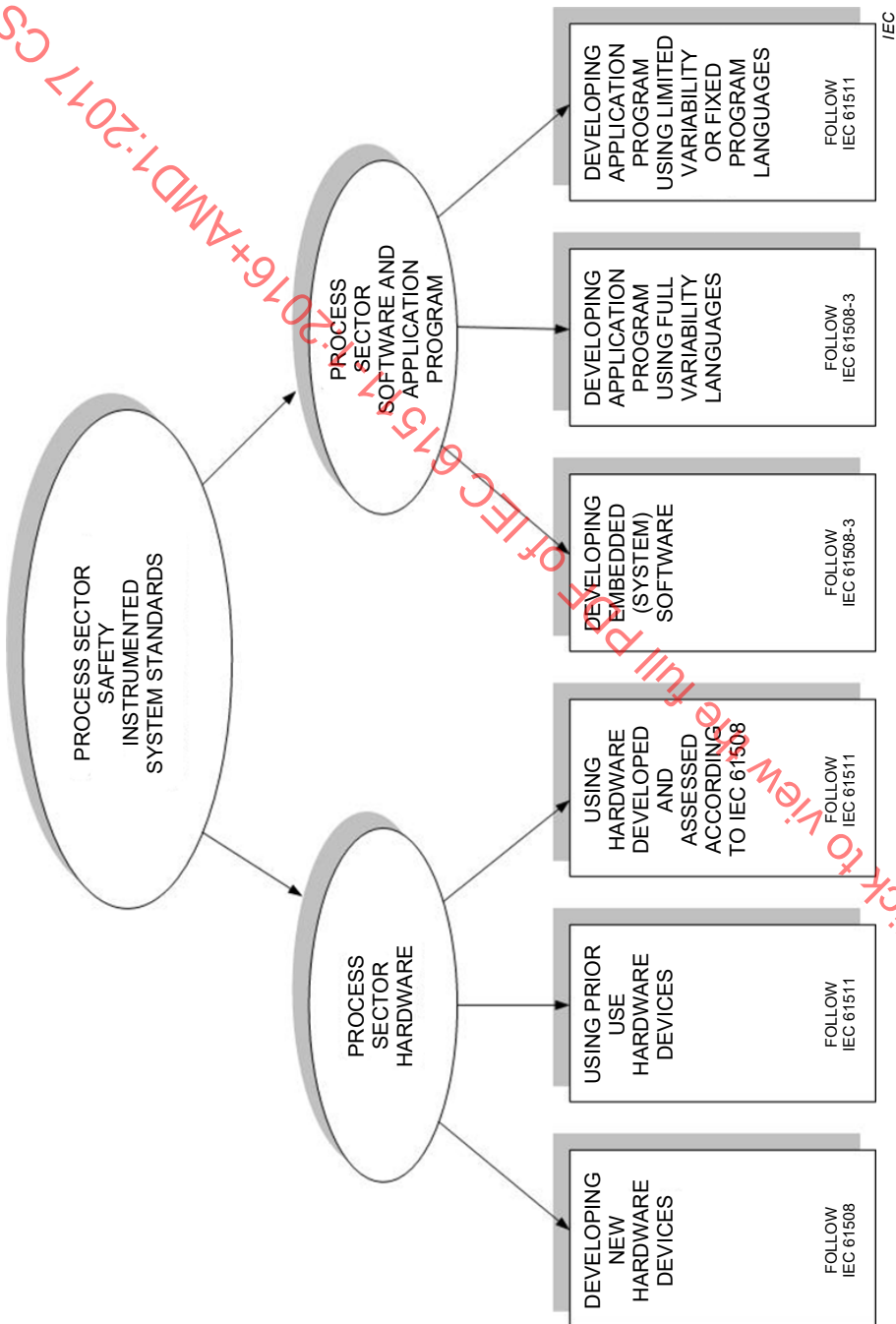


Figure 2 – Relations entre l'IEC 61511 et l'IEC 61508

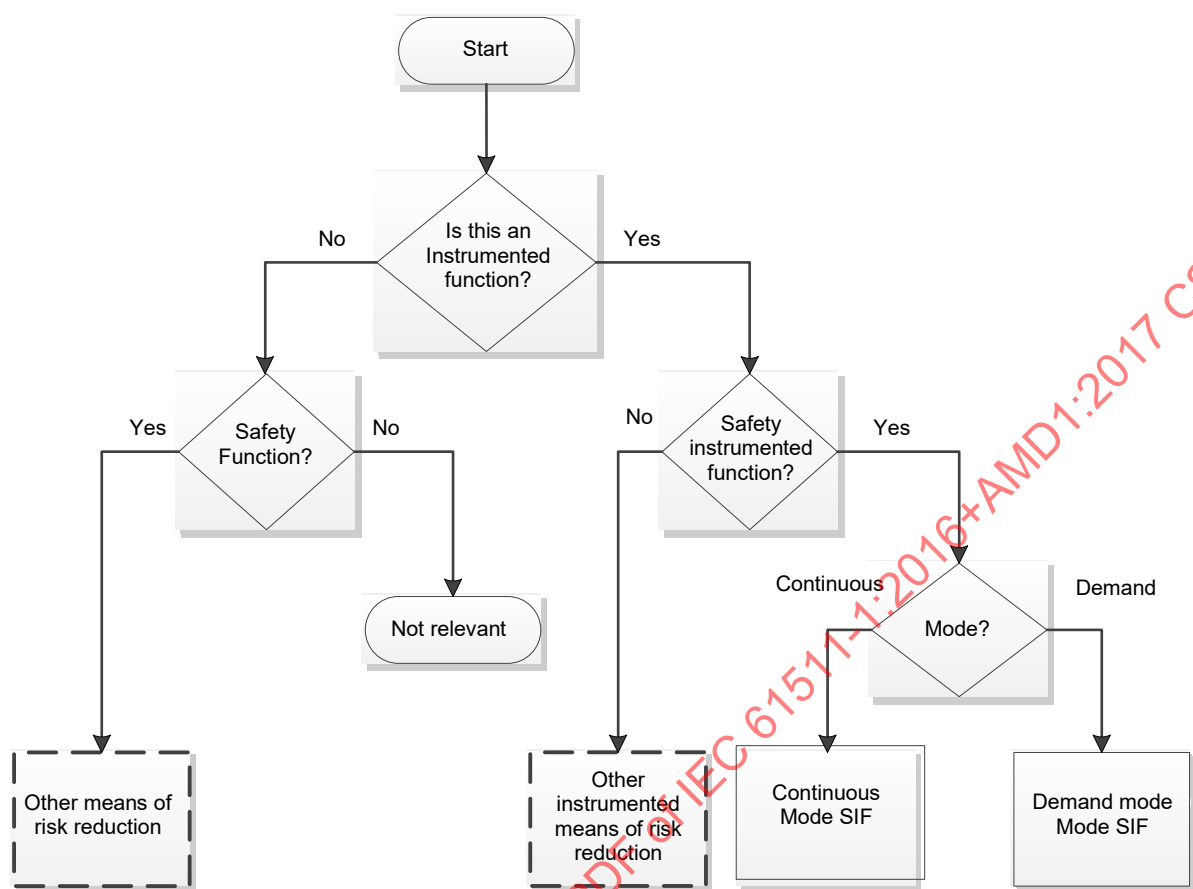
NOTE 3 L'IEC 61508 est également utilisée par les concepteurs, intégrateurs et utilisateurs de SIS lorsque cela est indiqué dans l'IEC 61511.



Anglais	Français
PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS	NORMES RELATIVES AUX SYSTEMES INSTRUMENTES DE SECURITE DANS LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
PROCESS SECTOR HARDWARE	MATERIEL POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
PROCESS SECTOR SOFTWARE & APPLICATION PROGRAM	LOGICIEL ET PROGRAMME D'APPLICATION POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
DEVELOPING NEW HARDWARE DEVICES	DEVELOPPEMENT DE NOUVEAUX APPAREILS MATERIELS
FOLLOW IEC 61508	SUIVRE L'IEC 61508
USING PRIOR USE HARDWARE DEVICES	UTILISATION D'APPAREILS MATERIELS BASES SUR L'UTILISATION ANTERIEURE
FOLLOW IEC 61511	SUIVRE L'IEC 61511
USING HARDWARE DEVELOPED AND ASSESSED ACCORDING TO IEC 61508	UTILISATION DE MATERIEL DEVELOPPE ET EVALUE CONFORMEMENT A L'IEC 61508
DEVELOPING EMBEDDED (SYSTEM) SOFTWARE	DEVELOPPEMENT DE LOGICIELS (SYSTEME) INTEGRES
FOLLOW IEC 61508-3	SUIVRE L'IEC 61508-3
DEVELOPING APPLICATION PROGRAM USING FULL VARIABILITY LANGUAGES	DEVELOPPEMENT DE PROGRAMME D'APPLICATION UTILISANT DES LANGAGES DE VARIABILITE TOTALE
DEVELOPING APPLICATION PROGRAM USING LIMITED VARIABILITY OR FIXED PROGRAM LANGUAGES	DEVELOPPEMENT DE PROGRAMME D'APPLICATION UTILISANT DES LANGAGES DE VARIABILITE LIMITEE OU DES LANGAGES DE PROGRAMME FIGE

Figure 3 – Relations détaillées entre l'IEC 61511 et l'IEC 61508

NOTE 4 Pour connaître les lignes directrices concernant le traitement de l'intégration des sous-systèmes qui satisfont à d'autres normes (machines, brûleur, etc.), voir 7.2.2 de l'IEC 61511-1:2016 et A.7.2.2 de l'IEC 61511-2:2016.



Standard specifies activities which are to be carried out but requirements are not detailed

IEC

Anglais	Français
Start	Démarrage
Is this an Instrumented function?	Est-ce une fonction instrumentée?
No	Non
Yes	Oui
Safety Function?	Fonction de sécurité?
Safety instrumented function?	Fonction instrumentée de sécurité?
Not relevant	Non pertinent
Mode?	Mode?
Continuous	Continu
Demand	Sollicitation
Other means of risk reduction	Autres moyens de réduction de risque
Other instrumented means of risk reduction	Autres moyens instrumentés de réduction de risque
Continuous Mode SIF	SIF en mode continu
Demand mode Mode SIF	SIF en mode sollicitation
Standard specifies activities which are to be carried out but requirements are not detailed	La norme spécifie les activités devant être réalisées, mais les exigences ne sont pas détaillées

Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions

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 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

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*

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

3 Termes, définitions et abréviations

3.1 Termes

Les termes figurent dans l'ordre alphabétique en 3.2.

3.2 Termes et définitions

Pour les besoins du présent document, les définitions suivantes s'appliquent.

Dans certains cas, ces définitions diffèrent de celles correspondant aux mêmes termes dans l'IEC 61508-4:2010. Dans certains cas, cela est dû à la terminologie utilisée dans le secteur des industries de transformation. Dans d'autres cas, ces définitions ont été alignées avec d'autres références définitives pertinentes (p. ex.: l'IEC 60050, le Vocabulaire Electrotechnique International, l'ISO/IEC Guide 51:2013). Toutefois, sauf indication contraire, il n'existe aucune différence de signification technique entre ces définitions et celles des mêmes termes dans l'IEC 61508-4:2010.

3.2.1

architecture

configuration

configuration spécifique des éléments matériels et logiciels dans un système

Note 1 à l'article: Dans la série IEC 61511, cela peut signifier, par exemple, la disposition des sous-systèmes SIS, la structure interne d'un sous-système SIS ou la structure interne des programmes d'application du SIS.

3.2.2

protection de biens

fonction allouée à la conception d'un système dans le but de prévenir la perte ou l'endommagement de biens

3.2.3

système de commande de processus de base

BPCS

système qui répond aux signaux d'entrée provenant du processus, de ses équipements associés, d'autres systèmes programmables et/ou des opérateurs, et qui génère des signaux de sortie faisant fonctionner le processus et ses équipements associés de la manière souhaitée, mais qui n'exécute aucune fonction instrumentée de sécurité (SIF)

Note 1 à l'article: Un BPCS inclut tous les appareils nécessaires pour s'assurer que le processus fonctionne de la manière souhaitée.

Note 2 à l'article: Un BPCS peut habituellement mettre en œuvre différentes fonctions (p. ex.: fonctions de commande de processus, surveillance, et alarmes).

Note 3 à l'article: L'abréviation «BPCS» est dérivée du terme anglais développé correspondant «basic process control system».

3.2.4

dérivation

action ou installation empêchant l'exécution de tout ou partie des fonctionnalités du SIS

Note 1 à l'article: Des exemples de dérivation incluent ce qui suit:

- le signal d'entrée en provenance du circuit de déclenchement est bloqué, mais les paramètres d'entrée et l'alarme sont toujours présentés à l'opérateur;
- le signal de sortie du circuit de déclenchement à un élément terminal est maintenu à l'état normal empêchant le fonctionnement de l'élément terminal;
- une ligne de dérivation physique est fournie autour de l'élément terminal;
- un état d'entrée présélectionné (p. ex.: acheminer/arrêter le signal d'entrée) ou un ensemble de paramètres est forcé par l'intermédiaire d'un outil d'ingénierie (p. ex.: dans le programme d'application).

Note 2 à l'article: La notion de dérivation est également rendue par d'autres termes (p. ex.: neutralisation, mise en échec, désactivation, forçage, inhibition, shuntage ou blocage).

3.2.5

canal

appareil ou groupe d'appareils exécutant une fonction indépendante spécifique

Note 1 à l'article: Les appareils d'un canal peuvent comporter des appareils d'entrée et de sortie (E/S), des unités logiques, des capteurs et des éléments terminaux.

Note 2 à l'article: Une configuration à double canal (à deux canaux) comprend deux canaux réalisant indépendamment la même fonction. Les canaux peuvent être identiques ou différents.

Note 3 à l'article: Ce terme peut être utilisé pour décrire un système complet ou une partie seulement d'un système (p. ex.: les capteurs ou les éléments terminaux).

Note 4 à l'article: Un canal décrit les éléments architecturaux matériels d'un SIS souvent utilisés pour satisfaire aux exigences de tolérance aux défauts du matériel.

3.2.6

cause commune

3.2.6.1

défaillances de cause commune, pl

défaillances concomitantes affectant plusieurs appareils, qui proviennent d'un événement unique et ne résultent pas les unes des autres

Note 1 à l'article: Toutes les défaillances résultant d'une cause commune ne se produisent pas nécessairement exactement à la même heure, et cela peut laisser du temps pour détecter l'occurrence de la cause commune avant qu'un SIS ne subisse réellement une défaillance.

Note 2 à l'article: Les défaillances de cause commune peuvent également donner lieu à des défaillances de mode commun.

Note 3 à l'article: La possibilité de défaillances de cause commune réduit l'efficacité de la redondance ou de la tolérance aux anomalies d'un système (p. ex.: augmente la probabilité de défaillance de deux canaux ou plus dans un système multicanal).

Note 4 à l'article: Les défaillances de cause commune sont des défaillances dépendantes. Elles peuvent résulter d'événements extérieurs (p. ex.: température, humidité, surtension, incendie et corrosion), d'erreurs systématiques (p. ex.: erreurs de conception, d'assemblage ou d'installation, bogues), d'erreurs humaines (p. ex.: mauvaise utilisation), etc.

Note 5 à l'article: Par extension, une défaillance de cause commune (au singulier) est une défaillance appartenant à un ensemble de défaillances concomitantes (au pluriel) selon la définition donnée en 3.2.6.1.

3.2.6.2

défaillances de mode commun, pl

défaillances concomitantes affectant plusieurs appareils, caractérisées par le même mode de défaillance (c'est-à-dire des défaillances identiques)

Note 1 à l'article: Les défaillances de mode commun peuvent avoir différentes causes.

Note 2 à l'article: Les défaillances de mode commun peuvent également être le résultat de défaillances de cause commune (3.2.6.1).

Note 3 à l'article: La possibilité de défaillances de mode commun réduit l'efficacité de la redondance ou de la tolérance aux anomalies d'un système (p. ex.: défaillance de deux canaux ou plus de la même manière, ce qui entraîne le même résultat erroné).

Note 4 à l'article: Par extension, une défaillance de mode commun (au singulier) est une défaillance appartenant à un ensemble de défaillances concomitantes (au pluriel) selon la définition donnée en 3.2.6.2.

3.2.7

mesure compensatoire

mise en œuvre temporaire de méthodes planifiées et documentées de gestion des risques au cours d'une période de maintenance ou de fonctionnement du processus lorsque les performances du SIS sont réputées être dégradées

3.2.8

composant

l'une des parties d'un système, d'un sous-système SIS ou d'un appareil, exécutant une fonction spécifique

Note 1 à l'article: Un composant peut également inclure des logiciels.

3.2.9

gestion de configuration

discipline d'identification des composants d'un système évolutif et des dispositions de ces composants ayant pour objectif de maîtriser les modifications de ces composants et de maintenir la continuité du système et la traçabilité des changements apportés tout au long du cycle de vie

3.2.9.1

approche prudente

manière prévoyante de réaliser des analyses et calculs

Note 1 à l'article: Dans le domaine de la sécurité, chaque fois qu'une analyse ou qu'une hypothèse doit être formulée ou qu'un calcul doit être réalisé (concernant des modèles, des données d'entrée, des calculs, etc.), une approche prudente peut être choisie pour s'assurer de produire des résultats pessimistes.

3.2.10

système de commande

système qui réagit à des signaux d'entrée provenant du processus et/ou d'un opérateur et qui produit des signaux de sortie qui font que le processus fonctionne de la manière souhaitée

Note 1 à l'article: Le système de commande comprend des capteurs et des éléments terminaux et peut être soit un BPCS, soit un SIS ou une combinaison des deux.

3.2.11

défaillance dangereuse

défaillance qui neutralise ou désactive une action de sécurité donnée

Note 1 à l'article: Une défaillance est "dangereuse" uniquement au regard d'une SIF donnée.

Note 2 à l'article: Lorsque la tolérance aux anomalies est mise en œuvre, une défaillance dangereuse peut conduire à:

- une SIF dégradée où l'action de sécurité est disponible, mais où il existe une plus grande probabilité de PFD ou de PFH (~~fonctionnement en mode sollicitation~~) ou une plus grande probabilité de déclencher un événement dangereux (~~fonctionnement en mode continu~~); ou;

- une SIF désactivée où l'action de sécurité est complètement désactivée (~~fonctionnement en mode sollicitation~~) ou l'événement dangereux a été induit (~~fonctionnement en mode continu~~).

Note 3 à l'article: Lorsqu'aucune tolérance aux anomalies n'est mise en œuvre, toutes les défaillances dangereuses conduisent à une SIF désactivée.

3.2.12

défaillance dépendante

défaillance dont la probabilité ne peut pas être exprimée en tant que simple produit des probabilités non conditionnelles de chacun des événements individuels qui l'ont provoquée

Note 1 à l'article: Deux événements A et B sont dépendants si la probabilité d'occurrence de A et B, $P(A \text{ et } B)$, est supérieure à $P(A) \times P(B)$.

Note 2 à l'article: Pour plus d'informations sur les défaillances dépendantes entre les couches de protection, voir 9.4.2 et l'IEC 61511-3:2016, Annexe J.

Note 3 à l'article: Les défaillances dépendantes incluent la cause commune.

3.2.13

défecté

révélé

déclaré

se rapporte aux défaillances ou erreurs du matériel et du logiciel qui ne sont pas cachées, parce qu'elles s'annoncent elles-mêmes ou qu'elles sont détectées lors du fonctionnement normal ou par des méthodes de détection dédiées

Note 1 à l'article: Il existe quelques différences pour l'utilisation de ces adjectifs:

- L'adjectif "déclaré" désigne les défaillances ou erreurs qui s'annoncent elles-mêmes au moment où elles surviennent (p. ex.: du fait du changement d'état). La réparation de telles défaillances peut débuter dès leur occurrence.
- L'adjectif "détecté" désigne les défaillances ou erreurs qui ne s'annoncent pas elles-mêmes au moment où elles surviennent et qui restent cachées jusqu'à ce qu'elles soient détectées par les essais de diagnostic, les essais périodiques ou l'intervention de l'opérateur (p. ex.: examen physique et essais manuels). La réparation de telles défaillances ne peut débuter qu'une fois qu'elles ont été révélées. Pour connaître l'usage spécifique de ce terme dans l'IEC 61511, se reporter à la Note 2.
- L'adjectif "révélé" désigne les défaillances ou erreurs qui deviennent évidentes parce qu'elles sont déclarées ou ont été détectées.

Note 2 à l'article: Dans l'IEC 61511 et excepté lorsque le contexte suggère une autre signification, le terme "défaillances/erreurs détectées dangereuses" se rapporte aux défaillances/erreurs dangereuses détectées par les essais de diagnostic.

Note 3 à l'article: Lorsque la détection est très rapide (p. ex.: essais de diagnostic), les défaillances ou erreurs détectées peuvent être considérées comme des défaillances ou erreurs déclarées.

Lorsque la détection n'est pas très rapide (p. ex.: essais périodiques), les défaillances ou erreurs détectées ne peuvent pas être considérées comme des défaillances ou erreurs déclarées en ce qui concerne les niveaux d'intégrité de sécurité.

Note 4 à l'article: Une défaillance révélée dangereuse peut uniquement être traitée comme une défaillance en sécurité si des mesures efficaces (automatiques ou manuelles) sont mises en œuvre dans un délai suffisamment court pour maintenir la sécurité du processus.

3.2.14

appareil

matériel, avec ou sans logiciel, capable de réaliser une fonction spécifiée

Note 1 à l'article: Des exemples incluent les capteurs, les unités logiques, les éléments terminaux, les interfaces opérateur et les raccordements à l'installation.

3.2.14.1

appareil de terrain

appareil SIS ou BPCS connecté directement au processus ou situé à proximité du processus

Note 1 à l'article: Des exemples incluent les capteurs, les éléments terminaux et les commutateurs manuels.

3.2.15 **diagnostic**

essai automatique fréquent (lié au temps de sécurité du processus) visant à révéler des défaillances

3.2.15.1 **couverture du diagnostic** DC

taux de défaillances dangereuses détectées par les diagnostics. La couverture du diagnostic ne comprend aucune défaillance détectée par les essais périodiques

Note 1 à l'article: La couverture du diagnostic s'applique habituellement aux appareils SIS ou aux sous-systèmes SIS. Par exemple, la couverture du diagnostic est généralement déterminée pour un capteur, un élément terminal ou une unité logique.

Note 2 à l'article: Pour les applications de sécurité, la couverture du diagnostic s'applique habituellement aux défaillances dangereuses des appareils SIS ou des sous-systèmes SIS. Par exemple, la couverture du diagnostic pour les défaillances dangereuses d'un appareil est $DC = \lambda_{DD} / \lambda_{DT}$, où λ_{DD} est le taux de défaillances dangereuses détectées et λ_{DT} est le taux de défaillances dangereuses totales. Pour un sous-système SIS avec redondance interne, DC dépend du temps: $DC(t) = \lambda_{DD}(t) / \lambda_{DT}(t)$.

Note 3 à l'article: Lorsque la couverture du diagnostic (DC) et le taux de défaillances dangereuses totales (λ_{DT}) sont donnés, les taux de défaillances dangereuses détectées (λ_{DD}) et non détectées (λ_{DU}) peuvent être calculés comme suit:

$$\lambda_{DD} = DC \times \lambda_{DT} \text{ et } \lambda_{DU} = (1-DC) \times \lambda_{DT}.$$

Note 4 à l'article: L'abréviation "DC" est dérivée du terme anglais développé correspondant "diagnostic coverage".

3.2.16 **diversité** moyens différents pour réaliser une fonction exigée

Note 1 à l'article: La diversité peut être réalisée en utilisant des moyens physiques, des techniques de programmation ou des approches de conception différents.

3.2.17 **erreur**

écart entre une valeur ou condition calculée, observée ou mesurée et la valeur ou condition vraie, spécifiée ou théoriquement correcte

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.2.18 **défaillance** perte de l'aptitude à fonctionner tel que requis

Note 1 à l'article: La défaillance d'un appareil est un événement qui provoque un état d'anomalie de cet appareil.

Note 2 à l'article: Lorsque la perte d'aptitude est causée par une panne latente, la défaillance survient lorsqu'un ensemble particulier de circonstances est réuni.

Note 3 à l'article: L'accomplissement des fonctions exigées exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportement à éviter. L'occurrence d'un tel comportement est une défaillance.

Note 4 à l'article: Les défaillances sont soit aléatoires, soit systématiques (~~voir 3.2.61 et 3.2.83~~ voir 3.2.59 et 3.2.81).

[SOURCE: IEC 60050-192:2015, 192-03-01, modifiée – Les notes à l'article ont été modifiées]

3.2.18.1 **mode de défaillance** manière selon laquelle une défaillance se produit

Note 1 à l'article: Un mode de défaillance peut être défini par la fonction perdue ou par la transition d'état qui s'est produite.

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.2.19

anomalie

inaptitude à fonctionner tel que requis, due à un état interne

Note 1 à l'article: La panne d'une entité est due soit à une défaillance de l'entité elle-même, soit à une imperfection lors d'une étape précédente du cycle de vie, telle que la spécification, la conception, la fabrication ou la maintenance.

Note 2 à l'article: Une panne d'un appareil donne lieu à une défaillance lorsqu'un ensemble particulier de circonstances est réuni.

[SOURCE: IEC 60050-192:2015, 192-04-01, modifiée – Certaines notes à l'article ont été modifiées, d'autres supprimées. "Panne" a été changé en "anomalie"]

3.2.20

évitement des anomalies

utilisation de techniques et procédures destinées à éviter l'apparition d'anomalies durant chacune des phases du cycle de vie de sécurité du SIS

3.2.20.1

exclusion des anomalies

élimination dans les examens futurs d'anomalies résultant de modes de défaillance improbables

Note 1 à l'article: Pour plus d'informations sur l'exclusion des anomalies, l'ISO 13849-1 et l'ISO 13849-2 peuvent être consultées. Outre ces normes, l'exclusion des anomalies peut reposer sur:

- l'improbabilité technique de l'occurrence de certaines anomalies;
- l'expérience technique généralement acceptée, indépendamment de l'application concernée;
- les exigences techniques relatives à l'application et au danger spécifique.

Note 2 à l'article: Les modes de défaillance (identifiés dans les appareils réalisant la fonction de sécurité) peuvent être exclus, car leurs taux de défaillances dangereuses sont très faibles par rapport au niveau objectif de défaillances relatif à la fonction de sécurité à l'étude. Autrement dit, la somme des taux de défaillances dangereuses de tous les appareils en série sur lesquels l'exclusion des anomalies est revendiquée ne peut en général pas être supérieure à 1 % du niveau objectif de défaillances.

3.2.21

tolérance aux anomalies

aptitude d'une entité fonctionnelle à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs

3.2.22

élément terminal

partie du BPCS ou du SIS qui met en œuvre l'action physique nécessaire pour obtenir ou maintenir un état de sécurité

Note 1 à l'article: Des exemples sont les vannes, appareils de commutation et moteurs, comprenant leurs éléments auxiliaires (p. ex.: une électrovanne et un actionneur utilisés pour faire fonctionner une vanne).

3.2.23

sécurité fonctionnelle

sous-ensemble de la sécurité globale se rapportant au processus et au BPCS, qui dépend du fonctionnement correct du SIS et d'autres couches de protection

3.2.24

évaluation de la sécurité fonctionnelle

FSA

recherche, à partir de preuves, destinée à juger de l'état de sécurité fonctionnelle atteint par un ou plusieurs SIS et/ou d'autres couches de protection

Note 1 à l'article: L'abréviation «FSA» est dérivée du terme anglais développé correspondant «functional safety assessment».

3.2.25

audit de la sécurité fonctionnelle

examen systématique et indépendant destiné à déterminer si les procédures spécifiques aux exigences sur la sécurité fonctionnelle sont conformes aux procédures prévues, sont effectivement mises en œuvre et permettent d'atteindre les objectifs spécifiés

Note 1 à l'article: Un audit de la sécurité fonctionnelle peut être mené dans le cadre d'une FSA.

3.2.26

intégrité de sécurité du matériel

partie de l'intégrité de sécurité du SIS liée aux défaillances aléatoires du matériel en mode de défaillance dangereux

Note 1 à l'article: Les deux niveaux de défaillances qui sont pertinents dans ce contexte sont la fréquence moyenne de défaillance dangereuse (~~fonctionnement en mode continu~~) et la probabilité moyenne de défaillance en cas de sollicitation (~~fonctionnement en mode sollicitation~~).

Note 2 à l'article: Voir 3.2.82.

Note 3 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.27

dommage

blessure ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.2.27.1

événement préjudiciable

événement dangereux qui conduit à un dommage

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés à la situation dangereuse et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence. Un événement dangereux qui a conduit à un dommage est appelé "événement préjudiciable".

3.2.28

danger

source potentielle de dommage

Note 1 à l'article: Ce terme comprend le danger sur des personnes survenant dans un court laps de temps (p. ex.: feu ou explosion), et aussi le danger à long terme sur la santé d'une personne (p. ex.: dégagement d'une substance toxique ou radioactivité).

[SOURCE: ISO/IEC Guide 51:2014, 3.2, modifiée – La Note 1 à l'article a été ajoutée]

3.2.28.1

événement dangereux

événement pouvant conduire à un dommage

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés à la situation dangereuse et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence.

[SOURCE: ISO/IEC Guide 51:2014: 3.3, modifiée – voir Note 1]

3.2.28.2

situation dangereuse

situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs dangers

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.2.29

erreur humaine

action humaine ou absence d'intervention prévue ou non prévue, qui produit un résultat non approprié

Note 1 à l'article: Les fautes, chutes et inattentions constituent des exemples d'erreurs humaines.

Note 2 à l'article: Les actions malveillantes sont exclues.

3.2.30

analyse d'impact

activité consistant à déterminer l'effet que la modification à une fonction ou à un composant d'un système aura sur les autres fonctions ou les autres composants de ce système tout comme sur d'autres systèmes

3.2.31

organisation indépendante

organisation distincte et séparée, par sa direction et ses autres ressources, de celles responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité du SIS et qui est chargée de la FSA ou de la validation

3.2.32

personne indépendante

personne distincte et séparée de celles responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité du SIS, qui est chargée de la FSA ou de la validation, et qui n'a pas de responsabilité directe dans ces activités

3.2.33

fonction d'entrée

fonction qui contrôle le processus et ses équipements associés afin de fournir des informations d'entrée à l'unité logique

Note 1 à l'article: Une fonction d'entrée peut être une fonction manuelle.

3.2.34

instrument

appareil utilisé pour effectuer une action (généralement présent dans les systèmes instrumentés)

3.2.34.1

système instrumenté

système composé de capteurs (p. ex.: transmetteurs de pression, de débit et de température), d'unités logiques (p. ex.: contrôleurs programmables, systèmes de commande distribués, contrôleurs discrets) et d'éléments terminaux (p. ex.: vannes de commande, circuits de commande moteur)

Note 1 à l'article: Les systèmes instrumentés réalisent des fonctions instrumentées, notamment des fonctions de commande, de surveillance, d'alarme et de protection. Les systèmes instrumentés peuvent être des SIS (voir 3.2.67) ou des BPCS (voir 3.2.3).

3.2.35

fonction logique

fonction qui réalise les transformations entre les informations d'entrée (fournies par une ou plusieurs fonctions d'entrée) et les informations de sortie (utilisées par une ou plusieurs fonctions de sortie)

Note 1 à l'article: Les fonctions logiques assurent la transformation d'une ou de plusieurs fonctions d'entrée en une ou plusieurs fonctions de sortie.

Note 2 à l'article: Pour d'autres lignes directrices, voir l'IEC 61131-3:2012 et l'IEC 60617-12:1997.

3.2.36

unité logique

partie d'un BPCS ou d'un SIS qui exécute une ou plusieurs fonctions logiques

Note 1 à l'article: Dans l'IEC 61511, les termes suivants sont utilisés pour désigner des unités logiques:

- systèmes logiques électriques pour la technologie électromécanique;
- systèmes logiques électroniques pour la technologie électronique;
- systèmes logiques programmables (PE) pour les systèmes électroniques programmables.

Note 2 à l'article: Des exemples incluent les systèmes électriques, les systèmes électroniques, les systèmes électroniques programmables, les systèmes pneumatiques et les systèmes hydrauliques. Les capteurs et les éléments terminaux ne font pas partie de l'unité logique.

3.2.36.1

unité logique PE configurée pour la sécurité

unité logique de catégorie "électronique programmable pour usage général industriel" spécifiquement configurée pour être utilisée dans des applications de sécurité

Note 1 à l'article: D'autres lignes directrices peuvent être consultées en 11.5.

3.2.37

interface de maintenance/d'ingénierie

matériels et logiciels fournis pour permettre la maintenance ou la modification ad hoc du SIS

Note 1 à l'article: L'interface de maintenance/d'ingénierie peut comprendre des instructions et des diagnostics, pouvant être trouvés dans le logiciel, les terminaux de programmation avec les protocoles de transmission appropriés, des outils de diagnostic, des indicateurs, des appareils de dérivation, des appareils d'essai, et des appareils d'étalonnage.

3.2.37.1

temps moyen de dépannage

MRT

durée totale de dépannage prévue

Note 1 à l'article: Le MRT comprend les temps (b), (c) et (d) pour les durées applicables à la MTTR (voir 3.2.37.2).

Note 2 à l'article: L'abréviation «MRT» est dérivée du terme anglais développé correspondant «mean repair time».

3.2.37.2

durée moyenne de rétablissement

MTTR

durée prévue de rétablissement effectif

Note 1 à l'article: La MTTR comprend:

- le temps de détection de la défaillance (a);
- le temps écoulé avant de commencer la réparation (b);
- le temps de réparation effectif (c);
- le temps écoulé avant la remise en fonctionnement du composant (d).

Le temps de démarrage applicable à (b) est la fin du temps (a); le temps de démarrage applicable à (c) est la fin du temps (b) et le temps de démarrage applicable à (d) est la fin du temps (c).

Note 2 à l'article: L'abréviation «MTTR» est dérivée du terme anglais développé correspondant «mean time to restoration».

3.2.37.3

temps de dépannage maximal admis

MPRT

durée maximale admise pour réparer une défaillance après sa détection

Note 1 à l'article: Le MRT peut être utilisé comme MPRT, mais le MPRT peut être défini sans rapport avec le MRT:

- Un MPRT inférieur au MRT peut être choisi pour diminuer la probabilité d'un événement dangereux.
- Un MPRT supérieur au MRT peut être choisi si la probabilité d'un événement dangereux peut être réduite.

Note 2 à l'article: Lorsqu'un MPRT a été défini, il peut être utilisé à la place du MRT lors du calcul de la probabilité des défaillances aléatoires du matériel.

Note 3 à l'article: L'abréviation «MPRT» est dérivée du terme anglais développé correspondant «maximum permitted repair time».

3.2.38

atténuation

action qui atténue la (les) conséquence(s) d'un événement dangereux

Note 1 à l'article: Il s'agit, par exemple, de la dépressurisation de secours ou de la fermeture des clapets de ventilation en cas de détection ou de confirmation d'incendie ou de fuite de gaz ou le déclenchement de déluge suite à la détection confirmée d'un incendie.

3.2.39

mode de fonctionnement (d'une SIF)

manière dont fonctionne une SIF qui peut être le mode à faible sollicitation, le mode à sollicitation élevée ou le mode continu

- a) **mode à faible sollicitation:** mode de fonctionnement dans lequel la SIF n'est réalisée que sur sollicitation, afin de faire passer le processus dans un état de sécurité spécifié, et où la fréquence des sollicitations n'est pas supérieure à une par an.
- b) **mode à sollicitation élevée:** mode de fonctionnement dans lequel la SIF n'est réalisée que sur sollicitation, afin de faire passer le processus dans un état de sécurité spécifié, et où la fréquence des sollicitations est supérieure à une par an.
- c) **mode continu:** mode de fonctionnement dans lequel la SIF maintient le processus dans un état de sécurité en fonctionnement normal.

3.2.39.1

SIF en mode sollicitation

fonctionnement de la SIF en mode à faible sollicitation (3.2.39 a)) ou en mode à sollicitation élevée (3.2.39 b))

Note 1 à l'article: Dans l'éventualité d'une défaillance dangereuse de la SIF, un événement dangereux ne peut se produire que:

- si la défaillance n'est pas détectée et qu'une sollicitation survient avant l'essai périodique suivant;
- si la défaillance est détectée par les essais de diagnostic, mais que le processus concerné et ses équipements associés n'ont pas basculé dans un état de sécurité avant qu'une sollicitation ne survienne.

Note 2 à l'article: En mode à sollicitation élevée, il sera normalement approprié d'utiliser les critères du mode continu.

Note 3 à l'article: Les niveaux d'intégrité de sécurité des SIF fonctionnant en mode sollicitation sont définis au Tableau 4 et au Tableau 5.

3.2.39.2

SIF en mode continu

SIF fonctionnant en mode continu (3.2.39 c))

Note 1 à l'article: Dans l'éventualité d'une défaillance dangereuse de la SIF, un événement dangereux se produira, sans autre défaillance, sauf si une action est entreprise pour l'empêcher dans le temps de sécurité du processus.

Note 2 à l'article: Le mode continu couvre les SIF qui mettent en œuvre une commande continue pour maintenir la sécurité fonctionnelle.

Note 3 à l'article: Les niveaux d'intégrité de sécurité des SIF fonctionnant en mode continu sont définis au Tableau 5.

3.2.40 module

partie monobloc d'un programme d'application SIS (peut être interne à un programme ou un ensemble de programmes) exécutant une fonction spécifique (p. ex.: séquence de démarrage/d'arrêt/d'essai d'un élément terminal, séquence spécifique à une application au sein d'une SIF)

Note 1 à l'article: Dans le contexte de l'IEC 61131-3:2012, un module logiciel est une fonction ou un bloc de fonctions.

Note 2 à l'article: La plupart des modules ont une utilisation répétitive au sein d'un programme d'application.

3.2.41 Moon

SIS, ou partie de celui-ci, composé de "*N*" canaux indépendants, qui sont connectés de telle manière que "*M*" canaux sont suffisants pour exécuter la SIF

3.2.42 réduction de risque nécessaire

réduction de risque devant être réalisée par le ou les SIS et/ou d'autres couches de protection afin de s'assurer que le risque tolérable n'est pas dépassé

3.2.43 système non programmable système (NP)

système non basé sur les technologies de l'informatique (c'est-à-dire un système non basé sur une électronique programmable [PE] ou sur un logiciel)

Note 1 à l'article: Des exemples incluraient les systèmes électriques ou électroniques câblés, les systèmes mécaniques, hydrauliques ou pneumatiques.

3.2.44 environnement de fonctionnement

conditions inhérentes à l'installation d'un appareil affectant potentiellement ses fonctionnalités et son intégrité de sécurité, telles que:

- l'environnement externe (p. ex.: besoins d'hivernage, classification en zones dangereuses);
- les conditions de fonctionnement des processus (p. ex.: valeurs extrêmes de température, pression et vibration);
- la composition des processus (p. ex.: solides, sels ou corrosifs);
- les interfaces de processus;
- l'intégration aux systèmes globaux de gestion du fonctionnement et de la maintenance de l'installation;
- le débit des communications (p. ex.: interférences électromagnétiques); et
- la qualité du réseau d'alimentation (p. ex.: puissance électrique, air, hydraulique).

Note 1 à l'article: Certaines applications de processus peuvent comporter des exigences d'environnement de fonctionnement particulières nécessaires pour survivre à un événement accidentel majeur. Par exemple, certains équipements exigent des enveloppes spéciales, une purge ou une protection contre l'incendie.

3.2.45

mode de fonctionnement

mode de fonctionnement du processus

état de fonctionnement planifié du processus incluant des modes tels que le démarrage après un arrêt d'urgence, le démarrage, le fonctionnement et l'arrêt normaux, les opérations temporaires, ainsi que le fonctionnement et l'arrêt d'urgence

3.2.46

interface opérateur

moyens par lesquels les informations sont communiquées entre un opérateur humain et le SIS (p. ex.: interfaces d'affichage, voyants lumineux, boutons-poussoirs, klaxons, alarmes)

Note 1 à l'article: L'interface opérateur est parfois désignée sous le nom d'interface homme-machine (IHM).

3.2.47

fonction de sortie

fonction qui commande le processus et ses équipements associés, en fonction des informations de sortie, à partir de la fonction logique

3.2.48

performance

réalisation d'une action ou d'une tâche donnée mesurée par rapport à la spécification et à la série de normes IEC 61511

3.2.49

phase

période comprise dans le cycle de vie de sécurité du SIS, où sont mises en œuvre les activités décrites dans la série IEC 61511

3.2.50

prévention

action qui réduit la probabilité d'occurrence d'un événement dangereux

3.2.51

utilisation antérieure

évaluation documentée par un utilisateur, démontrant qu'un appareil convient à l'utilisation dans un SIS et qu'il peut satisfaire aux exigences fonctionnelles et aux exigences concernant l'intégrité de sécurité, en s'appuyant sur une expérience de fonctionnement antérieure dans des environnements de fonctionnement similaires

Note 1 à l'article: Pour qualifier un appareil SIS sur la base d'une utilisation antérieure, l'utilisateur peut justifier le fait que l'appareil a atteint des performances satisfaisantes dans un environnement de fonctionnement similaire. La manière dont les équipements se comportent dans l'environnement de fonctionnement doit être comprise afin d'obtenir un degré élevé de certitude que les pratiques prévues de conception, d'inspection, d'essai, de maintenance et de fonctionnement sont suffisantes.

Note 2 à l'article: La validation en utilisation s'appuie sur les bases de conception du fabricant (p. ex.: limite de température, limite de vibration, limite de corrosion, support de maintenance souhaité) de cet appareil. L'utilisation antérieure concerne les performances installées de l'appareil au sein d'une application du secteur des industries de transformation, dans un environnement de fonctionnement particulier souvent différent des bases de conception du fabricant.

3.2.52

risque de processus

risque provenant des conditions du processus provoquées par des événements anormaux (comprenant un mauvais fonctionnement du BPCS)

Note 1 à l'article: Dans ce contexte, il s'agit du risque associé à l'événement dangereux spécifique pour lequel les SIS doivent être utilisés afin d'apporter la réduction de risque nécessaire (c'est-à-dire le risque associé à la sécurité fonctionnelle).

Note 2 à l'article: L'analyse de risque de processus est décrite dans l'IEC 61511-3:2016. L'objectif principal dans la détermination du risque de processus est d'établir un point de référence pour le risque, sans prendre en compte les couches de protection.

Note 3 à l'article: L'évaluation de ce risque peut comprendre les problèmes associés aux facteurs humains.

Note 4 à l'article: Ce terme équivaut au "risque EUC" de l'IEC 61508-4:2010.

3.2.52.1

temps de sécurité du processus

durée entre l'occurrence d'une défaillance se produisant dans le processus ou le système de commande de processus de base (avec risque de donner lieu à un événement dangereux) et l'occurrence de l'événement dangereux si la SIF n'est pas exécutée

Note 1 à l'article: Il s'agit d'une propriété du processus uniquement. La SIF doit détecter la défaillance et exécuter son action suffisamment tôt pour empêcher l'événement dangereux, en tenant compte du décalage de processus (p. ex.: le refroidissement d'une cuve).

3.2.53

électronique programmable

PE

entité basée sur les technologies de l'informatique pouvant se composer de matériel, de logiciel, ainsi que d'unités d'entrée et/ou de sortie

Note 1 à l'article: Ce terme recouvre les appareils microélectroniques basés sur une ou plusieurs unités centrales de traitement (CPU, Central Processing Unit) associées à des mémoires. Des exemples d'appareils électroniques programmables dans le secteur des industries de transformation comprennent:

- capteurs intelligents et éléments terminaux;
- unités logiques électroniques programmables, notamment:
- contrôleurs programmables;
- automates programmables;
- contrôleurs de boucle.

Note 2 à l'article: L'abréviation «PE» est dérivée du terme anglais développé correspondant «programmable electronics».

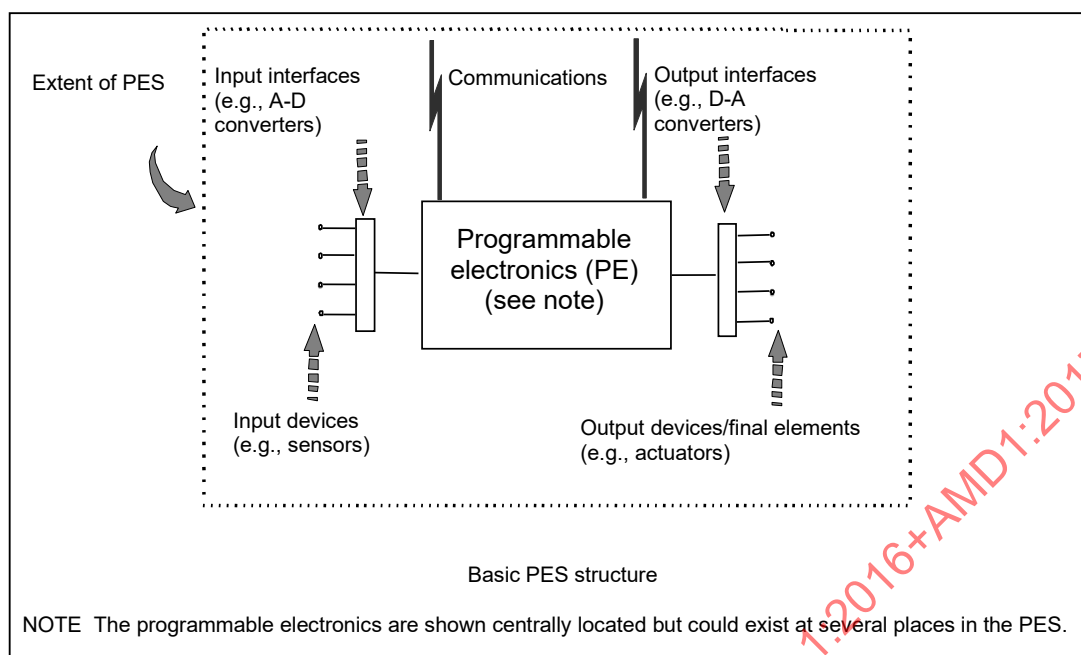
3.2.54

système électronique programmable

PES

système de commande, de protection ou de surveillance basé sur un ou plusieurs appareils électroniques programmables, comprenant tous les éléments du système, tels que les alimentations, les capteurs et d'autres appareils d'entrée, en passant par les autoroutes de données et d'autres voies de communication, jusqu'aux actionneurs et d'autres appareils de sortie (voir Figure 5)

Note 1 à l'article: L'abréviation «PES» est dérivée du terme anglais développé correspondant «programmable electronic system»



IEC

Anglais	Français
Extent of PES	Etendue du PES
Input interfaces (e.g., A-D converters)	Interfaces d'entrée (p. ex.: convertisseurs A-C)
Communications	Communications
Output interfaces (e.g., D-A converters)	Interfaces de sortie (p. ex.: convertisseurs C-A)
Programmable electronics (PE) (see note)	Electronique programmable (PE) (voir note)
Input devices (e.g., sensors)	Appareils d'entrée (p. ex.: capteurs)
Output devices/final elements (e.g., actuators)	Appareils de sortie/éléments terminaux (p. ex.: actionneurs)
Basic PES structure	Structure de base d'un PES
NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.	NOTE L'électronique programmable est présentée de façon centrale, mais pourrait se situer en différents endroits du PES.

Figure 5 – Système électronique programmable (PES): structure et terminologie

3.2.55 programmation codage

processus consistant à concevoir, à écrire et à soumettre à l'essai un ensemble d'instructions pour résoudre un problème ou traiter des données

Note 1 à l'article: Dans la série IEC 61511, la programmation est typiquement associée à une électronique programmable (PE).

3.2.56 essai périodique

essai périodique destiné à détecter les anomalies dangereuses cachées dans un SIS de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition "comme neuf" ou dans une condition aussi proche que possible de celle-ci

3.2.57

couche de protection

tout mécanisme indépendant réduisant le risque par contrôle, prévention ou atténuation

Note 1 à l'article: Il peut s'agir d'un mécanisme d'ingénierie de processus, tel que la taille des cuves contenant des produits chimiques dangereux, un mécanisme de génie mécanique, tel qu'une soupape de sécurité, un SIS ou une procédure administrative, telle qu'un plan de secours contre un danger imminent. Ces réponses peuvent être automatisées ou déclenchées par des actions humaines (voir Figure 9).

3.2.58

qualité

ensemble des caractéristiques d'une entité portant sur sa capacité à satisfaire aux besoins exprimés et implicites

Note 1 à l'article: Voir l'ISO 9000 pour plus de détails.

3.2.59

défaillance aléatoire du matériel

défaillance survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel

Note 1 à l'article: Il existe de nombreux mécanismes de dégradation se produisant à des fréquences différentes dans divers composants et, puisque les tolérances de fabrication ont pour conséquence une défaillance des composants causée par ces mécanismes après des durées de fonctionnement inégales, les défaillances survenant dans un équipement comprenant plusieurs composants surviennent à des fréquences prévisibles, mais à des instants imprévisibles (c'est-à-dire aléatoires).

Note 2 à l'article: Deux différences majeures permettent de distinguer les défaillances aléatoires du matériel et les défaillances systématiques:

- une défaillance aléatoire du matériel implique le système proprement dit seulement, tandis qu'une défaillance systématique implique à la fois le système proprement dit (une anomalie) et une condition particulière (voir 3.2.81). Ensuite, une défaillance aléatoire du matériel est caractérisée par un seul paramètre de fiabilité (c'est-à-dire le taux de défaillance) alors qu'une défaillance systématique est caractérisée par deux paramètres de fiabilité (c'est-à-dire la probabilité de l'anomalie préexistante et le taux de danger de la condition particulière);
- une défaillance systématique peut être éliminée après avoir été détectée tandis que les défaillances aléatoires du matériel ne le peuvent pas.

Cela implique que les paramètres de fiabilité des défaillances aléatoires du matériel peuvent être estimés à partir des informations de situation alors qu'il est très difficile de réaliser la même chose pour les défaillances systématiques. Une approche qualitative est préférentielle pour les défaillances systématiques.

[SOURCE: IEC 61508-4:20103.6.5, modifiée – Les notes ont été changées]

3.2.60

redondance

existence de plusieurs moyens pour accomplir une fonction exigée ou représenter des informations

Note 1 à l'article: Des exemples incluent l'utilisation d'appareils en double et l'adjonction de bits de parité.

Note 2 à l'article: La redondance sert essentiellement à améliorer la fiabilité ou la disponibilité.

[SOURCE: IEC 61508-4:2010, 3.4.6]

3.2.61

risque

combinaison de la probabilité d'un dommage et de sa gravité

Note 1 à l'article: La probabilité d'une occurrence inclut l'exposition à une situation dangereuse, survenue d'un événement dangereux et l'impossibilité d'éviter ou de limiter le dommage.

[SOURCE: ISO/IEC Guide 51:2014, 3.8]

3.2.62

défaillance en sécurité

défaillance qui privilégie une action de sécurité donnée

Note 1 à l'article: Une défaillance est "en sécurité" uniquement au regard d'une fonction de sécurité donnée.

Note 2 à l'article: Lorsque la tolérance aux anomalies est mise en œuvre, une défaillance en sécurité peut conduire à:

- un fonctionnement où l'action de sécurité est disponible, mais avec une probabilité plus élevée de réussite en sollicitation ~~(fonctionnement en mode sollicitation)~~ ou une probabilité plus faible d'engendrer un événement dangereux ~~(fonctionnement en mode continu)~~;
- un fonctionnement parasite où l'action de sécurité est déclenchée.

Note 3 à l'article: Lorsqu'aucune tolérance aux anomalies n'est mise en œuvre, les défaillances en sécurité donnent lieu au déclenchement de l'action de sécurité, quelle que soit la condition du processus. Ce phénomène est également connu sous le nom de "déclenchement parasite".

Note 4 à l'article: Un déclenchement parasite peut être en sécurité au regard d'une fonction de sécurité donnée, mais peut être dangereux au regard d'une autre fonction de sécurité.

Note 5 à l'article: Des déclenchements parasites peuvent également avoir des effets néfastes sur la disponibilité en production du processus.

3.2.63

état de sécurité

état du processus lorsque la sécurité est réalisée

Note 1 à l'article: Certains états apportent une plus grande sécurité que d'autres pendant le passage d'une condition dangereuse à l'état de sécurité final ou le passage de la condition de sécurité nominale à une condition dangereuse, le processus pouvant devoir traverser un certain nombre d'états de sécurité intermédiaires.

Note 2 à l'article: Dans certaines situations, l'état de sécurité n'existe que durant le laps de temps où le processus est continuellement contrôlé. Ce contrôle continu peut s'étendre sur une période de temps courte ou indéfinie.

Note 3 à l'article: Un état dit de sécurité au regard d'une fonction de sécurité donnée peut augmenter la probabilité d'engendrer un événement dangereux au regard d'une autre fonction de sécurité donnée. Dans ce cas, l'augmentation de risque potentielle associée à l'autre fonction dans le calcul de la fréquence de déclenchement parasite moyenne maximale admissible (voir 10.3.2) de la première fonction peut être considérée.

Note 4 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.64

sécurité

absence de risque intolérable

Note 1 à l'article: Selon l'ISO/IEC Guide 51, les termes "risque acceptable" et "risque tolérable" sont considérés comme des synonymes.

[SOURCE: ISO/IEC Guide 51:2014, 3.14, modifiée – La note à l'article a été ajoutée]

3.2.65

fonction de sécurité

fonction à réaliser par une ou plusieurs couches de protection, prévue pour assurer ou maintenir un état de sécurité au processus, par rapport à un événement dangereux spécifique

3.2.66

fonction instrumentée de sécurité

SIF

fonction de sécurité devant être mise en œuvre par un système instrumenté de sécurité (SIS)

Note 1 à l'article: Une SIF est conçue pour atteindre un SIL exigé qui est déterminé par rapport aux autres couches de protection participant à la réduction du même risque.

Note 2 à l'article: L'abréviation «SIF» est dérivée du terme anglais développé correspondant «safety instrumented function».

3.2.67

système instrumenté de sécurité

SIS

système instrumenté utilisé pour mettre en œuvre une ou plusieurs SIF

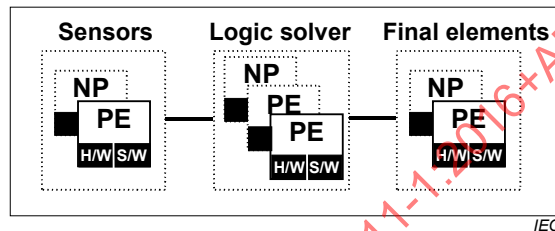
Note 1 à l'article: Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unité(s) logique(s) et d'élément(s) terminal(aux) (p. ex.: voir Figure 6). Il inclut également des équipements de communication et auxiliaires (p. ex.: câbles, tuyauterie, alimentation, lignes d'impulsion, réchauffage des conduites).

Note 2 à l'article: Un SIS peut inclure le logiciel.

Note 3 à l'article: Un SIS peut inclure une action humaine dans le cadre d'une SIF (voir l'ISA TR84.00.04:2015, Partie 1).

Note 4 à l'article: L'abréviation «SIS» est dérivée du terme anglais développé correspondant «safety instrumented system».

SIS architecture and safety instrumented function example with different devices shown



Anglais	Français
SIS architecture and safety instrumented function example with different devices shown	Architecture SIS et exemple de fonction instrumentée de sécurité avec différents appareils
Sensors	Capteurs
Logic solver	Unité logique
Final elements	Éléments terminaux
NP	NP
PE	PE
H/W	matériel
S/W	logiciel

Figure 6 – Exemple d'architectures SIS comprenant trois sous-systèmes SIS

3.2.68

intégrité de sécurité

aptitude du SIS à exécuter la SIF exigée lorsque cela est exigé

Note 1 à l'article: Cette définition est équivalente à la sûreté de fonctionnement du SIS au regard de la SIF exigée. Pour éviter toute confusion, le terme "sûreté de fonctionnement", qui est souvent considéré au sens économique plutôt qu'en tant que concept de sécurité, n'a pas été utilisé.

Note 2 à l'article: L'aptitude inclut à la fois la réponse fonctionnelle (p. ex.: fermeture d'une vanne spécifiée dans un intervalle de temps spécifié) et la probabilité que le SIS agisse comme cela est exigé.

Note 3 à l'article: L'évaluation de l'intégrité de sécurité peut prendre en compte toutes les causes des défaillances aléatoires du matériel et des défaillances systématiques conduisant à un état de non-sécurité (p. ex.: défaillances de matériel, défaillances induites du logiciel et défaillances dues aux perturbations électriques). Certaines de ces défaillances, en particulier les défaillances aléatoires du matériel, peuvent être quantifiées à l'aide de mesures telles que la fréquence moyenne de défaillance dangereuse ou la probabilité de défaillance en cas de sollicitation. Cependant, l'intégrité de sécurité dépend également de plusieurs facteurs systématiques, qui ne peuvent pas être précisément quantifiés, mais simplement considérés d'un point de vue qualitatif tout au long du cycle de vie. La probabilité que les défaillances systématiques conduisent à une défaillance dangereuse du SIS est réduite par le biais de la tolérance aux défauts du matériel (voir 11.4) ou d'autres méthodes et techniques.

Note 4 à l'article: L'intégrité de sécurité comprend l'intégrité de sécurité du matériel (voir 3.2.26) et l'intégrité de sécurité systématique (voir 3.2.82), mais les défaillances complexes engendrées par la conjonction des défaillances du matériel et des défaillances systématiques peuvent également être prises en compte.

3.2.69

niveau d'intégrité de sécurité

SIL

niveau discret (parmi quatre possibles) affecté à la SIF permettant de spécifier les exigences concernant l'intégrité de sécurité devant être réalisées par le SIS

Note 1 à l'article: Plus le SIL est élevé, ~~plus la PFD_{avg} attendue en mode sollicitation ou la fréquence moyenne d'une défaillance dangereuse causant un événement dangereux en mode continu est faible~~ plus la PFD_{avg} attendue ou la fréquence moyenne d'une défaillance dangereuse causant un événement dangereux est faible.

Note 2 à l'article: Les relations entre le niveau objectif de défaillances et le SIL sont données dans les Tableaux 4 et 5.

Note 3 à l'article: Le SIL 4 possède le plus haut niveau d'intégrité de sécurité; le SIL 1 possède le niveau le plus bas

Note 4 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

Note 5 à l'article: L'abréviation «SIL» est dérivée du terme anglais développé correspondant «safety integrity level»

3.2.69.1

exigences concernant l'intégrité de sécurité, pl

ensemble des exigences de l'IEC 61511 devant être satisfaites par un SIS afin de revendiquer un SIL donné pour une SIF mise en œuvre par ce SIS

Note 1 à l'article: Les exigences concernant l'intégrité de sécurité sont renforcées lorsque le SIL associé augmente.

3.2.70

cycle de vie de sécurité du SIS

activités nécessaires à la mise en œuvre de SIF, se déroulant au cours d'une période de temps, qui commence à la phase de conception d'un projet et se termine lorsque toutes les SIF ne sont plus disponibles à l'utilisation

Note 1 à l'article: Le terme "cycle de vie de sécurité fonctionnelle" est strictement plus précis, mais l'adjectif "fonctionnelle" n'est pas considéré comme étant nécessaire dans ce cas, c'est-à-dire dans le contexte de la série IEC 61511.

Note 2 à l'article: Le modèle de cycle de vie de sécurité du SIS utilisé dans l'IEC 61511 est donné par la Figure 7.

3.2.71

manuel de sécurité

manuel de sécurité fonctionnelle

informations qui définissent comment un appareil, un sous-système ou un système SIS peuvent être appliqués sans risque

Note 1 à l'article: Le manuel de sécurité peut comporter des données d'entrée du fabricant, mais également de l'utilisateur.

Note 2 à l'article: Concernant les appareils conformes à l'IEC 61508, les données d'entrée du fabricant correspondent au manuel de sécurité.

Note 3 à l'article: Ce terme pourrait recouvrir un document autonome générique ou un ensemble de documents.

Note 4 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.72

spécification des exigences de sécurité

SRS

spécification qui contient les exigences fonctionnelles pour les SIF et leurs niveaux d'intégrité de sécurité associés

Note 1 à l'article: L'abréviation «SRS» est dérivée du terme anglais développé correspondant «safety requirements specification»

[SOURCE: IEC 61508-4:2010, 3.5.11, modifiée – Alignée sur la terminologie de l'IEC 61511]

3.2.73

capteur

partie du BPCS ou du SIS qui mesure ou détecte la condition du processus

Note 1 à l'article: Des exemples incluent les transmetteurs, les transducteurs, les interrupteurs de processus et les interrupteurs de position.

3.2.74

logiciel

programmes, procédures, données, règles, ainsi que toute documentation se référant au fonctionnement d'un système de traitement de données

Note 1 à l'article: Le logiciel est indépendant du support sur lequel il a été enregistré.

Note 2 à l'article: Pour des exemples des différents types de logiciels, voir 3.2.75 et 3.2.76.

3.2.75

langages de programmation d'application

3.2.75.1

langage de programme figé

FPL

langage dans lequel l'utilisateur est limité à l'ajustement de quelques jeux de paramètres prédéfinis et figés

Note 1 à l'article: Des exemples représentatifs d'applications d'appareil avec FPL sont: les capteurs intelligents (p. ex.: transmetteur de pression sans algorithmes de commande), les éléments terminaux intelligents (p. ex.: vannes sans algorithmes de commande), les séquences d'un enregistreur d'événements, les points de consigne d'un boîtier d'alarme intelligent. L'utilisation de FPL est souvent nommée "configuration de l'appareil".

Note 2 à l'article: L'abréviation «FPL» est dérivée du terme anglais développé correspondant «fixed program language»

3.2.75.2

langage de variabilité limitée

LVL

langage de programmation destiné aux automates programmables industriels du commerce dont les capacités sont limitées à leur mise en oeuvre, telle que définie par le manuel de sécurité associé. La notation de ce langage peut être textuelle, graphique ou présenter les caractéristiques des deux.

Note 1 à l'article: Ce type de langage est conçu pour être aisément compris par les utilisateurs du secteur des industries de transformation, et permet de combiner des fonctions de bibliothèque, prédéfinies, spécifiques à une application, pour mettre en oeuvre les SRS. Les LVL fournissent une correspondance fonctionnelle étroite avec les fonctions exigées pour réaliser l'application.

Note 2 à l'article: L'IEC 61511 part du principe que les contraintes nécessaires à l'obtention des propriétés de sécurité sont le résultat de la combinaison du manuel de sécurité, de la proximité de la notation avec les fonctions dont le programmeur d'application a besoin pour définir les algorithmes de commande de processus et du temps de compilation et des vérifications d'exécution que le fournisseur de l'unité logique intègre dans le logiciel de base de l'unité logique et son environnement de développement. Les contraintes identifiées dans le rapport de certification et le manuel de sécurité peuvent garantir que les exigences de l'IEC 61508-3:2010 sont satisfaites.

Note 3 à l'article: Le LVL est le langage le plus fréquemment utilisé lorsque la série IEC 61511 fait référence au terme "programme d'application".

Note 4 à l'article: L'abréviation "LVL" est dérivée du terme anglais développé correspondant "limited variability language".

3.2.75.3

langage de variabilité totale

FVL

langage conçu pour être compréhensible par les informaticiens (programmeurs), et qui permet de mettre en oeuvre une plage étendue de fonctions et d'applications

Note 1 à l'article: Un exemple type de système utilisant le FVL est l'ordinateur d'usage général.

Note 2 à l'article: Dans le secteur des industries de transformation, le FVL se trouve dans les logiciels intégrés et rarement dans la programmation d'application.

Note 3 à l'article: Des exemples de FVL incluent: l'Ada, le C, le Pascal, le langage Liste d'instructions, les langages d'assemblage, le C++, le Java et le SQL.

Note 4 à l'article: L'abréviation «FVL» est dérivée du terme anglais développé correspondant «full variability language»

3.2.76

types de logiciels et de programmes

3.2.76.1

programme d'application

programme spécifique à l'application de l'utilisateur contenant, en général, des séquences logiques, des autorisations, des limites et des expressions qui contrôlent l'entrée, la sortie, les calculs et les décisions nécessaires pour satisfaire aux exigences fonctionnelles des SIS

3.2.76.2

logiciel intégré

logiciel qui fait partie du système fourni par le fabricant et qui n'est pas accessible pour des modifications par l'utilisateur final

Note 1 à l'article: Le logiciel intégré est également désigné sous le nom de microprogramme ou de logiciel système. Voir 3.2.75.3 "langage de variabilité totale".

3.2.76.3

logiciel utilitaire

outils logiciels pour la création, la modification et la documentation des programmes d'application

Note 1 à l'article: Ces outils logiciels ne sont pas exigés pour le fonctionnement du SIS.

3.2.77

cycle de vie du programme d'application

ensemble d'activités qui se déroulent au cours d'une période de temps débutant lorsque le programme d'application est conçu et se terminant lorsque le programme d'application est retiré du service

Note 1 à l'article: Le cycle de vie d'un programme d'application inclut habituellement une phase de définition d'exigences, une phase de développement, une phase d'essai, une phase d'intégration, une phase d'installation et une phase de modification.

Note 2 à l'article: Le logiciel (notamment le programme d'application) ne peut pas être entretenu; au lieu de cela, il est modifié.

3.2.78

sous-système SIS

partie indépendante d'un SIS dont une défaillance dangereuse invalidante donne lieu à une défaillance dangereuse invalidante du SIS

Note 1 à l'article: La Figure 6 présente un SIS composé de trois sous-systèmes SIS.

Note 2 à l'article: Concernant l'approche de coupe (voir IEC 61025), une coupe minimale d'un sous-système SIS est également une coupe minimale du SIS global. Par conséquent, les SIF mises en œuvre au sein d'un SIS dépendent totalement des sous-systèmes SIS de ce SIS (autrement dit lorsqu'un sous-système SIS est défaillant, les SIF associées sont également défaillantes).

3.2.79

système

ensemble d'appareils qui interagissent selon une spécification

Note 1 à l'article: Une personne peut faire partie d'un système.

Note 2 à l'article: Cette définition diffère de celle donnée par l'IEC 61508 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.80

capabilité systématique

mesure (exprimée sur une échelle de SC 1 à SC 4) de la confiance dans le fait que l'intégrité de sécurité systématique d'un appareil satisfait aux exigences du SIL spécifié, par rapport à la fonction de sécurité spécifiée, lorsque l'appareil est appliqué conformément aux instructions spécifiées dans le manuel de sécurité de l'appareil

Note 1 à l'article: La capabilité systématique est déterminée par référence aux exigences concernant l'évitement et la maîtrise des défaillances systématiques dans l'IEC 61508-2:2010 et l'IEC 61508-3:2010.

Note 2 à l'article: Le mécanisme de défaillance systématique dépend de la nature de l'appareil. Pour un appareil comprenant uniquement du matériel, seuls les mécanismes de défaillance du matériel sont considérés. Pour un appareil comprenant du matériel et du logiciel, les interactions entre les mécanismes de défaillance du matériel et du logiciel doivent être considérées.

Note 3 à l'article: Une capabilité systématique de SC N pour un appareil signifie que l'intégrité de sécurité systématique de SC N a été satisfaite lorsque l'appareil est appliqué conformément aux instructions spécifiées dans le manuel de sécurité de l'appareil par rapport au SC N.

3.2.81

défaillance systématique

défaillance relative à une anomalie préexistante, qui survient systématiquement dans des conditions particulières, ne pouvant être éliminée qu'en supprimant l'anomalie par une modification de la conception ou du processus de fabrication, des procédures de fonctionnement, de la documentation ou d'autres facteurs appropriés

Note 1 à l'article: La cause des défaillances systématiques du logiciel peut être désignée sous le nom de "bogues".

Note 2 à l'article: La maintenance corrective sans modification n'éliminerait pas, habituellement, la cause de la défaillance qui implique la défaillance dans des conditions particulières.

Note 3 à l'article: Une défaillance systématique peut être reproduite en appliquant délibérément les mêmes conditions, même si toutes les défaillances reproductibles ne sont pas systématiques.

Note 4 à l'article: Des exemples d'erreurs conduisant à une défaillance systématique incluent l'erreur humaine survenant dans:

- la SRS;
- la conception, la fabrication, l'installation, le fonctionnement ou la maintenance du matériel;
- la conception ou la mise en œuvre du logiciel (notamment le programme d'application).

Note 5 à l'article: Des appareils similaires conçus, installés, mis en fonctionnement, mis en œuvre ou entretenus de la même façon sont susceptibles de contenir les mêmes anomalies. Par conséquent, ils font l'objet de défaillances de cause commune lorsque les conditions particulières surviennent.

3.2.82

intégrité de sécurité systématique

partie de l'intégrité de sécurité des SIS qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux

Note 1 à l'article: L'intégrité de sécurité systématique ne peut normalement pas être quantifiée (à la différence de l'intégrité de sécurité du matériel).

Note 2 à l'article: Voir également 3.2.26.

3.2.83

niveau objectif de défaillances

performance exigée de la SIF et spécifiée en termes de probabilité moyenne de défaillance lors du fonctionnement de la SIF en mode sollicitation (fonctionnement en mode sollicitation) ou de fréquence moyenne d'une défaillance dangereuse (fonctionnement en mode continu)

Note 1 à l'article: Les relations entre les niveaux objectifs de défaillances et le SIL sont données dans les Tableaux 4 et 5.

3.2.84 **risque tolérable**

niveau de risque accepté dans un certain contexte et fondé sur les valeurs admises par la société

Note 1 à l'article: Voir l'IEC 61511-3:2016, Annexe A.

[SOURCE: ISO/IEC Guide 51:2014, 3.15]

3.2.85 **non détecté** **non révélé** **non déclaré**

qui n'est pas détecté, ni révélé, ni déclaré

Note 1 à l'article: Dans l'IEC 61511 et excepté lorsque le contexte suggère une autre signification, le terme "défaillances/erreurs non détectées dangereuses" se rapporte aux défaillances/erreurs dangereuses non détectées par les essais de diagnostic.

3.2.86 **validation**

confirmation par examen et apport de preuves objectives que les exigences particulières à une utilisation prévue spécifique sont satisfaites

Note 1 à l'article: Dans la série IEC 61511, cela signifie démontrer que la ou les SIF et le SIS après installation satisfont en tous points à la SRS.

3.2.87 **vérification**

confirmation par examen et apport de preuves objectives que les exigences ont été satisfaites

Note 1 à l'article: Dans la série IEC 61511, cela désigne l'activité qui consiste, pour chaque phase du cycle de vie de sécurité du SIS correspondant, à démontrer par analyse et/ou par essais que, pour les entrées spécifiques, les sorties satisfont en tous points aux objectifs et aux exigences fixés pour la phase spécifique.

Note 2 à l'article: Des exemples incluent les activités de vérification qui suivent:

- les revues relatives aux sorties (documents concernant toutes les phases du cycle de vie de sécurité) destinées à assurer la conformité avec les objectifs et exigences de la phase, et prenant en compte les entrées spécifiques à cette phase;
- les revues de conception;
- les essais réalisés sur les produits conçus, afin d'assurer que leur fonctionnement est conforme à leur spécification;
- les essais d'intégration réalisés lors de l'assemblage de différentes parties d'un système, élément par élément, et par la réalisation d'essais d'environnement, afin d'assurer que toutes les parties fonctionnent les unes avec les autres conformément à ce qui est spécifié.

3.2.88 **chien de garde**

combinaison de diagnostics et d'un appareil de sortie (typiquement un commutateur) pour effectuer la surveillance du bon fonctionnement de l'appareil électronique programmable (PE) et entreprendre une action lors de la détection d'un fonctionnement incorrect

Note 1 à l'article: Le chien de garde confirme que le système logiciel fonctionne correctement en réinitialisant régulièrement un appareil externe (p. ex.: temporisateur électronique de chien de garde matériel), par un appareil de sortie commandé par le logiciel.

Note 2 à l'article: Le chien de garde peut être utilisé pour mettre hors tension un groupe de sorties de sécurité, lorsque des défaillances dangereuses sont détectées, afin d'atteindre ou de maintenir un état de sécurité du processus par rapport à l'événement dangereux. Le chien de garde est utilisé pour augmenter la couverture du diagnostic en ligne de l'unité logique PE (voir 3.2.13 et 3.2.15).

3.3 Abréviations

Les abréviations utilisées tout au long de l'IEC 61511 sont données au Tableau 1. Sont également incluses certaines abréviations communes relatives à la sécurité fonctionnelle du secteur des industries de transformation.

Tableau 1 – Abréviations utilisées dans l'IEC 61511

Abréviation	Expression développée
AC/DC	Alternating current/direct current, Courant alternatif/Courant continu (CA/CC)
AIChE	American Institute of Chemical Engineers
ALARP	As low as reasonably practicable, Aussi faible que raisonnablement possible
ANSI	American National Standards Institute, Organisme national de normalisation américain
AP	Application program, Programme d'application
BPCS	Basic process control system, Système de commande de processus de base
CCPS	Centre for Chemical Process Safety (AIChE), Centre pour la sécurité des processus chimiques
DC	Diagnostic coverage, Couverture du diagnostic
E/E/PE	Electrical/electronic/programmable electronic, Electrique/électronique/électronique programmable
EMC	Electro-magnetic compatibility, Compatibilité électromagnétique (CEM)
FAT	Factory acceptance test, Essai de réception en usine (ERU)
FPL	Fixed program language, Langage de programme figé
FSA	Functional safety assessment, Evaluation de la sécurité fonctionnelle
FSMS	Functional safety management system, Système de gestion de la sécurité fonctionnelle
FTA	Fault tree analysis, Analyse par arbre des défaillances
FVL	Full variability language, Langage de variabilité totale
HFT	Hardware fault tolerance, Tolérance aux défauts du matériel
H&RA	Hazard & risk assessment, Analyse de danger et de risque
HMI	Human Machine Interface, Interface homme-machine (IHM)
IEC	International Electrotechnical Commission, Commission Electrotechnique Internationale
ISA	International Society of Automation, Société internationale d'automatisation
ISO	International Organization for Standardization, Organisation internationale de normalisation
LVL	Limited variability language, Langage de variabilité limitée
MooN	"M" out of "N" channel architecture, Architecture de "M" pour "N" canaux
MPRT	Maximum permitted repair time, Temps de dépannage maximal admis
MRT	Mean repair time, Temps moyen de dépannage
MTTR	Mean time to restoration, Durée moyenne de rétablissement
NFPA	National Fire Protection Association(US), National Fire Protection Association (Etats-Unis)
NP	Non-programmable, Non programmable
OEM	Original Equipment Manufacturer, Fabricant original de l'équipement
PE	Programmable electronics, Electronique programmable
PES	Programmable electronic system, Système électronique programmable

Abréviation	Expression développée
PFD	Probability of dangerous failure on demand, Probabilité de défaillance dangereuse en cas de sollicitation
PFD _{avg}	Average probability of dangerous failure on demand, Probabilité moyenne de défaillance dangereuse en cas de sollicitation
PFH	Probability (average frequency of dangerous failures) of failure per hour, Probabilité (fréquence moyenne de défaillance dangereuse) de défaillance par heure
pl	Plural, Pluriel
PLC	Programmable logic controller, Automate programmable
SAT	Site acceptance test, Essai de réception sur site (ERS)
SC	Systematic capability, Capabilité systématique
SIF	Safety instrumented function, Fonction instrumentée de sécurité
SIL	Safety integrity level, Niveau d'intégrité de sécurité
SIS	Safety instrumented system, Système instrumenté de sécurité
SRS	Safety requirement specification, Spécification des exigences de sécurité

4 Conformité à l'IEC 61511-1:2016

Afin de se conformer à l'IEC 61511-1:2016, il doit être démontré que chacune des exigences décrites de l'Article 5 à l'Article 19 a été satisfaite eu égard aux critères définis, et que le ou les objectifs spécifiés dans ces articles ont donc été atteints.

5 Gestion de la sécurité fonctionnelle

5.1 Objectif

L'objectif des exigences de l'Article 5 est d'identifier les activités de gestion nécessaires pour s'assurer que les objectifs de sécurité fonctionnelle sont bien atteints.

NOTE 1: L'Article 5 a seulement pour but la réalisation et la maintenance de la sécurité fonctionnelle des SIS. Il est dissocié et distinct des mesures générales concernant la santé et la sécurité nécessaires à l'obtention de la sécurité sur le lieu de travail.

5.2 Exigences

5.2.1 Généralités

La politique et la stratégie pour atteindre la sécurité fonctionnelle doivent être identifiées, ainsi que les méthodes utilisées pour évaluer leur réalisation, et doivent être communiquées au sein de l'organisation.

5.2.2 Organisation et ressources

5.2.2.1 Les personnes, services, organisations ou autres unités qui sont responsables de l'exécution et de la revue de chacune des phases du cycle de vie de sécurité du SIS doivent être identifiés et être informés des responsabilités qui leur sont affectées.

5.2.2.2 Les personnes, les services ou les organisations impliqués dans les activités du cycle de vie de sécurité du SIS doivent être compétents pour conduire les activités dont ils sont responsables.

Les points suivants doivent être traités et documentés en considérant la compétence des personnes, services, organisations ou autres unités impliqués dans les activités du cycle de vie de sécurité du SIS:

- a) connaissances techniques, formation et expérience appropriées concernant l'application de processus;
- b) connaissances techniques, formation et expérience appropriées concernant la technologie applicable utilisée (p. ex.: électrique, électronique ou électronique programmable);
- c) connaissances techniques, formation et expérience appropriées concernant les capteurs et les éléments terminaux;
- d) connaissances techniques en matière de sécurité (p. ex.: analyse de processus de sécurité);
- e) connaissances des exigences de sécurité fonctionnelle légales et réglementaires;
- f) compétences adéquates en matière de gestion et d'encadrement appropriées à leur rôle dans les activités du cycle de vie de sécurité du SIS;
- g) compréhension de la conséquence potentielle d'un événement;
- h) SIL du SIF;
- i) nouveauté et complexité de l'application et de la technologie.

5.2.2.3 Une procédure doit être en place pour gérer les compétences de toutes les parties impliquées dans le cycle de vie du SIS. Des évaluations périodiques doivent être réalisées pour documenter les compétences des individus par rapport aux activités qu'ils accomplissent et en cas de changement d'un individu à un rôle.

5.2.3 Evaluation et gestion des risques

Les dangers doivent être identifiés, les risques évalués et la réduction de risque nécessaire déterminée, comme cela est défini à l'Article 8.

NOTE Pour des raisons économiques, il peut être judicieux de considérer également les pertes potentielles en capital.

5.2.4 Planification de la sécurité

Une planification de la sécurité doit être mise en place pour définir les activités devant être réalisées avec les personnes, services, organisations ou autres unités responsables de l'exécution de ces activités. Cette planification doit être mise à jour lorsque cela est nécessaire tout au long du cycle de vie de sécurité du SIS (voir l'Article 6) et réalisée selon un niveau d'activité détaillé conforme au rôle que l'individu ou l'organisation exerce au sein du cycle de vie de sécurité du SIS.

NOTE La planification de la sécurité peut être incorporée dans:

- une section du plan qualité, intitulée "plan du cycle de vie de sécurité du SIS"; ou
- un document distinct, intitulé "plan du cycle de vie de sécurité du SIS"; ou
- plusieurs documents qui peuvent comprendre des procédures ou des méthodes de travail propres à l'entreprise.

5.2.5 Mise en œuvre et surveillance

5.2.5.1 Des procédures doivent être mises en œuvre pour assurer le suivi rapide et une prise en compte satisfaisante des recommandations ayant trait au SIS et provenant

- a) de l'analyse de danger et l'évaluation du risque;
- b) des activités d'assurance;
- c) des activités de vérification;
- d) des activités de validation;
- e) des FSA;
- f) des audits de la sécurité fonctionnelle;
- g) des activités post-incident et post-accident.

5.2.5.2 Tous les fournisseurs offrant des produits ou services à une organisation qui a une responsabilité globale pour l'une ou plusieurs des phases du cycle de vie de sécurité du SIS doivent délivrer leurs produits ou services comme cela est spécifié par cette organisation et doivent posséder un système de gestion de la qualité. Des procédures doivent être en place pour démontrer l'adéquation du système de gestion de la qualité.

Si un fournisseur fait des revendications concernant la sécurité fonctionnelle d'un produit ou service, qui sont utilisées par l'organisation pour démontrer la conformité aux exigences de la présente partie de l'IEC 61511, le fournisseur doit posséder un système de gestion de la sécurité fonctionnelle. Des procédures doivent être en place pour démontrer l'adéquation du système de gestion de la sécurité fonctionnelle.

Le système de gestion de la sécurité fonctionnelle doit satisfaire aux exigences de la norme de sécurité fondamentale IEC 61508-1:2010, Article 6, ou aux exigences de gestion de la sécurité fonctionnelle de la norme déduite de l'IEC 61508 à laquelle se rapportent les revendications concernant la sécurité fonctionnelle.

5.2.5.3 Des procédures doivent être mises en œuvre afin d'évaluer les performances du SIS vis-à-vis de ses exigences de sécurité pour:

- identifier et prévenir les défaillances systématiques qui pourraient compromettre la sécurité;
- surveiller et évaluer si les paramètres de fiabilité du SIS sont conformes à ceux qui ont été supposés lors de la conception;
- définir l'action corrective nécessaire à entreprendre si les taux de défaillance sont supérieurs à ceux qui ont été supposés lors de la conception;
- comparer le taux de sollicitation relatif aux SIF pendant le fonctionnement aux hypothèses formulées lors de l'évaluation du risque lorsque les exigences de SIL ont été déterminées.

5.2.5.4 Pour les SIS conçus et construits conformément aux codes, normes ou pratiques définis avant la publication de la présente norme, l'utilisateur doit s'assurer que l'équipement est conçu, entretenu, contrôlé, soumis à l'essai et fonctionne d'une façon sûre.

5.2.6 Evaluation, audits et révisions

5.2.6.1 Evaluation de la sécurité fonctionnelle (FSA)

5.2.6.1.1 Une procédure doit être définie et exécutée pour réaliser une FSA de telle sorte qu'un jugement puisse être porté concernant la sécurité fonctionnelle et l'intégrité de sécurité atteintes par chaque SIF du SIS. La procédure doit exiger la nomination d'une équipe de FSA qui possède l'expertise technique, l'expertise de l'application et du fonctionnement nécessaires à l'application concernée.

5.2.6.1.2 L'équipe de FSA doit comprendre au moins une personne compétente de haut niveau, non impliquée dans l'équipe de conception du projet (pour les étapes 1, 2 et 3) ou non impliquée dans le fonctionnement et la maintenance du SIS (pour les étapes 4 et 5).

5.2.6.1.3 Les points suivants doivent être pris en compte lors de la planification d'une FSA:

- le domaine d'application de la FSA;
- qui doit participer à la FSA;
- les compétences, les responsabilités et les pouvoirs de l'équipe de FSA;
- les informations qui seront générées en tant que résultat de l'activité de FSA;
- l'identité de tous les autres organismes de sécurité impliqués dans la FSA;
- les ressources exigées pour terminer l'activité de FSA;
- le niveau d'indépendance de l'équipe de FSA;

- les méthodes par lesquelles la FSA sera revalidée après modifications.

NOTE Si l'équipe de FSA est importante, le fait d'avoir plusieurs personnes de haut niveau et compétentes dans l'équipe, indépendantes de l'équipe de projet, peut être pris en compte.

5.2.6.1.4 Une équipe de FSA doit passer en revue le travail réalisé sur l'ensemble des phases du cycle de vie de sécurité avant l'étape couverte par l'évaluation, qui n'ont pas déjà été couvertes par les FSA précédentes. Si des FSA précédentes ont été réalisées, l'équipe de FSA doit prendre en considération les conclusions et recommandations des évaluations précédentes. Les étapes du cycle de vie de sécurité du SIS pour lesquelles les activités FSA doivent être réalisées doivent être identifiées lors de la planification de la sécurité.

NOTE 1 Des activités supplémentaires de FSA peuvent être introduites en tant que nouveaux dangers identifiés, après modification et à intervalles périodiques lors du fonctionnement.

NOTE 2 Une attention particulière peut être portée à la réalisation des activités de FSA aux étapes suivantes (voir Figure 7).

- Etape 1 – Après avoir procédé à l'analyse de danger et de risque, avoir identifié les couches de protection exigées et avoir développé la SRS.
- Etape 2 – Après avoir conçu le SIS.
- Etape 3 – Après avoir terminé l'installation, la préparation à la mise en service et la validation finale du SIS et avoir développé les procédures de fonctionnement et de maintenance.
- Etape 4 – Après avoir acquis de l'expérience en fonctionnement et en maintenance.
- Etape 5 – Après une modification et avant le déclassement d'un SIS.

NOTE 3 Le nombre, l'ampleur et le domaine d'application des activités de FSA peuvent dépendre de circonstances particulières. Les facteurs intervenant dans cette décision sont susceptibles d'inclure:

- la taille du projet;
- le degré de complexité;
- le SIL;
- la durée du projet;
- les conséquences en cas de défaillance;
- le degré de normalisation des particularités de conception;
- les exigences de réglementation de sécurité;
- l'expérience antérieure d'une conception de système similaire;
- en considération de facteurs pertinents tels que:
 - le temps de fonctionnement;
 - le nombre et la portée des changements au niveau du fonctionnement;
 - la fréquence des essais périodiques.

5.2.6.1.5 Avant que les dangers ne se présentent, l'équipe de FSA doit procéder à une/des évaluation(s) de la sécurité fonctionnelle et doit confirmer que:

- la H&RA a été réalisée (voir 8.1);
- les recommandations résultant de la H&RA qui s'appliquent au SIS ont été mises en œuvre ou prises en compte;
- les procédures de changement de conception du projet sont en place et ont été correctement mises en œuvre;
- les recommandations résultant d'une FSA ont été prises en compte;
- le SIS est conçu, construit et installé selon la SRS, toutes les différences ayant été identifiées et prises en compte;
- les procédures de sécurité, de fonctionnement, de maintenance et d'urgence, propres au SIS sont en place;
- la planification de la validation du SIS est appropriée et les activités de validation ont été réalisées;

- la formation du personnel a été achevée et les informations appropriées sur le SIS ont été fournies au personnel de maintenance et d'exploitation;
- les stratégies ou les plans de mise en œuvre d'autres FSA sont en place.

5.2.6.1.6 Lorsque des outils de conception, de développement et de production sont utilisés pour toute activité du cycle de vie de sécurité du SIS, ils doivent faire l'objet d'une évaluation démontrant qu'ils n'ont pas un impact négatif sur le SIS ou les résultats des outils doivent être confirmés par des procédures de vérification.

NOTE 1 L'ampleur à laquelle ces outils peuvent être utilisés dépendra de leur impact sur le niveau de risque à obtenir.

NOTE 2 Des exemples d'outils de développement et de production incluent les outils de simulation et de modélisation, les équipements de mesure, les équipements d'essai, les équipements utilisés pendant les activités de maintenance et les outils de gestion de configuration.

NOTE 3 L'assurance qualité des outils inclut, mais sans s'y limiter, la traçabilité vis-à-vis des normes d'étalonnage, l'historique de fonctionnement et la liste des défauts.

5.2.6.1.7 Les résultats de la FSA doivent être disponibles, ainsi que toutes les recommandations découlant de cette évaluation.

5.2.6.1.8 Toutes les informations pertinentes doivent être mises à la disposition de l'équipe de FSA à sa demande.

5.2.6.1.9 Dans les cas où une FSA est réalisée sur une modification, l'évaluation doit tenir compte de l'analyse d'impact effectuée sur la modification proposée et confirmer que le travail de modification réalisé est conforme aux exigences de l'IEC 61511.

NOTE Les exigences relatives au cycle de vie de sécurité (y compris la FSA) liées aux modifications du SIS peuvent être consultées en 17.2.3.

5.2.6.1.10 Une FSA doit également être réalisée régulièrement lors de la phase de fonctionnement et de maintenance. Il s'agit de s'assurer que la maintenance et le fonctionnement sont effectués conformément aux hypothèses formulées lors de la conception et que les exigences de l'IEC 61511 en matière de gestion et de vérification de la sécurité sont satisfaites.

5.2.6.2 Révision et audit de la sécurité fonctionnelle

5.2.6.2.1 L'audit a pour objet de passer en revue les documents d'information et les rapports afin de déterminer si le système de gestion de la sécurité fonctionnelle (FSMS) est en place, à jour et respecté. Si des écarts sont identifiés, des recommandations d'améliorations sont formulées.

5.2.6.2.2 Toutes les procédures identifiées comme étant nécessaires à partir de l'ensemble des activités du cycle de vie de sécurité doivent faire l'objet d'un audit de sécurité.

5.2.6.2.3 Un audit de la sécurité fonctionnelle doit être réalisé par une personne indépendante ne travaillant pas sur le SIS qui doit être audité. Des procédures doivent être définies et exécutées pour auditer la conformité aux exigences, y compris:

- la fréquence des activités d'audit de la sécurité fonctionnelle;
- le degré de l'indépendance entre les personnes, services, organisations ou d'autres unités effectuant le travail et ceux ou celles conduisant les activités d'audit de la sécurité fonctionnelle;
- les activités d'enregistrement et de suivi.

5.2.6.2.4 La gestion des procédures de changement doit être en place pour initier, documenter, passer en revue, mettre en œuvre et approuver les changements apportés

au SIS autres que le remplacement en nature (c'est-à-dire sur une base comparable, un double exact d'un élément ou une substitution approuvée n'exigeant pas de modification du SIS installé).

5.2.6.2.5 La gestion des procédures de changement doit être en place pour identifier les changements qui affecteront les exigences relatives au SIS (p. ex.: reconception du BPCS, changements apportés à l'agencement dans une certaine zone).

5.2.7 Gestion de configuration du SIS

5.2.7.1 Les procédures de gestion de configuration du SIS au cours d'une phase du cycle de vie de sécurité du SIS doivent être disponibles.

NOTE En particulier, les points suivants peuvent être spécifiés:

- l'étape à laquelle la gestion formelle de configuration doit être mise en œuvre;
- les procédures devant être utilisées pour identifier de manière unique tous les composants d'un SIS ou d'un sous-système SIS (p. ex.: appareils, programmation d'application);
- les procédures permettant d'éviter que des appareils non autorisés entrent en service.

5.2.7.2 Les logiciels et matériels du SIS, ainsi que les procédures utilisées pour développer et exécuter le programme d'application doivent faire l'objet d'une gestion de configuration et doivent être gérés dans le cadre d'un contrôle de révision.

NOTE Les logiciels du SIS incluent le programme d'application (p. ex.: dans les unités logiques), les logiciels intégrés (p. ex.: capteurs, unités logiques, éléments terminaux) et les logiciels utilitaires (p. ex.: outils).

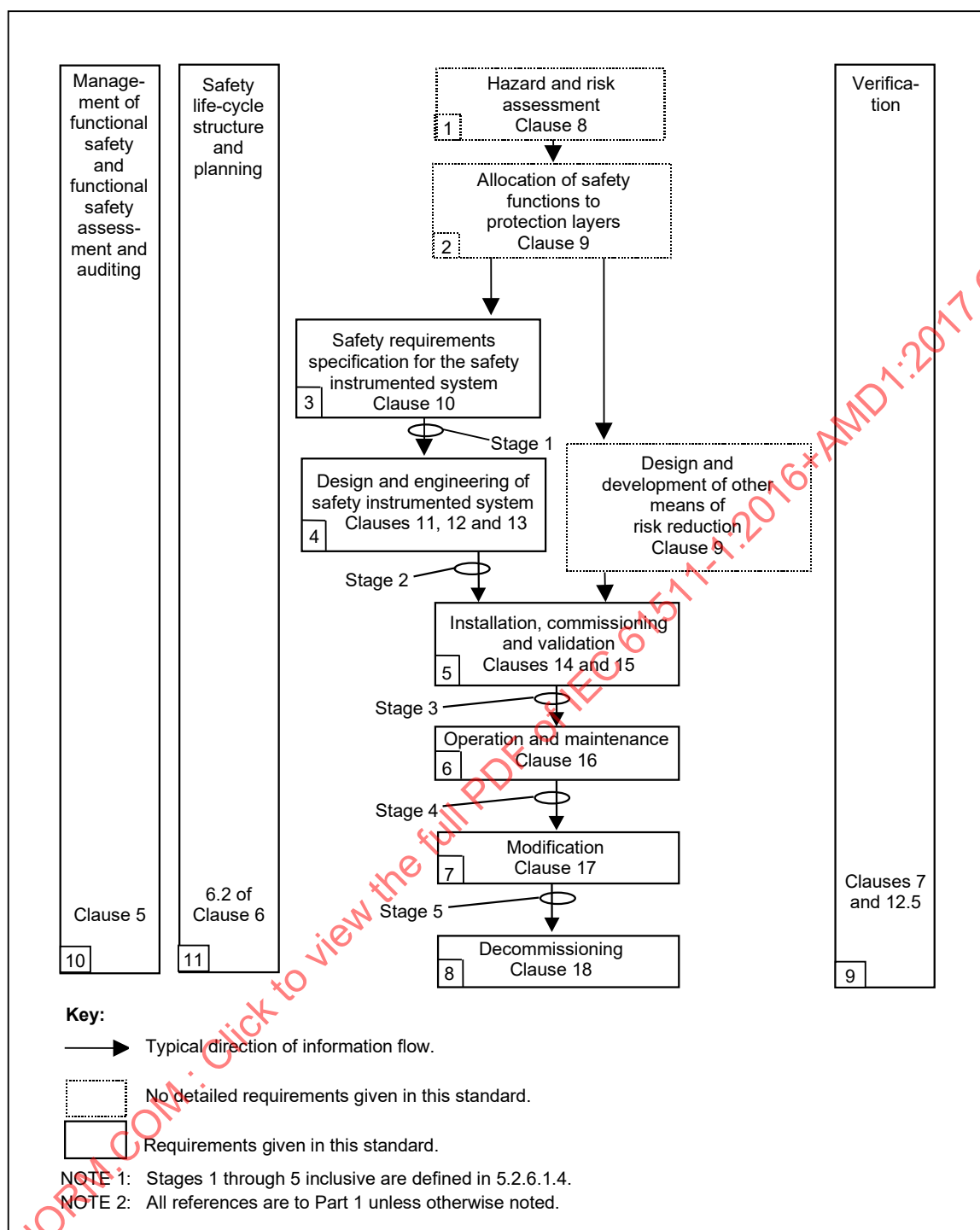
6 Exigences relatives au cycle de vie de sécurité

6.1 Objectifs

Les objectifs de l'Article 6 sont les suivants:

- définir les phases et établir les exigences relatives aux activités du cycle de vie de sécurité du SIS;
- définir et organiser les activités techniques dans le cycle de vie de sécurité du SIS;
- assurer qu'une planification adéquate existe (ou est développée), ce qui permet d'être certain que le SIS satisfait aux exigences de sécurité.

NOTE 1 L'approche globale de la série IEC 61511 est présentée à la Figure 7. Il peut être souligné que cette approche est donnée à titre indicatif et n'est censée indiquer que les activités typiques du cycle de vie de sécurité du SIS, de la conception initiale jusqu'au déclassement.



IEC

Anglais	Français
Management of functional safety and functional safety assessment and auditing Clause 5	Gestion, évaluation et audit de la sécurité fonctionnelle Article 5
Safety life-cycle structure and planning 6.2 of Clause 6	Structure et planification du cycle de vie de sécurité 6.2 de l'Article 6
Hazard and risk assessment Clause 8	Analyse de danger et de risque Article 8

Anglais	Français
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 Clause 10	Spécification des exigences de sécurité du système instrumenté de sécurité Article 10
Stage 1	Etape 1
Design and engineering of safety instrumented system Clauses 11, 12 and 13	Conception et ingénierie du système instrumenté de sécurité Articles 11, 12 et 13
Design and development of other means of risk reduction Clause 9	Conception et développement d'autres moyens de réduction de risque Article 9
Stage 2	Etape 2
Installation, commissioning and validation Clauses 14 and 15	Installation, mise en service et validation Articles 14 et 15
Stage 3	Etape 3
Operation and maintenance Clause 16	Fonctionnement et maintenance Article 16
Stage 4	Etape 4
Modification Clause 17	Modification Article 17
Stage 5	Etape 5
Decommissioning Clause 18	Déclassement Article 18
Verification Clauses 7 & 12.5	Vérification Articles 7 et 12.5
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 5.2.6.1.4.	NOTE 1 Les étapes 1 à 5 incluse sont définies en 5.2.6.1.4.
NOTE 2 All references are to Part 1 unless otherwise noted.	NOTE 2 Sauf indication contraire, toutes les références se rapportent à la Partie 1.

Figure 7 – Phases de cycle de vie de sécurité d'un SIS et étapes FSA

NOTE 2 Les informations de la Figure 7 peuvent découler du fonctionnement et de la maintenance et revenir à des étapes antérieures du cycle de vie afin de refléter le suivi des incidents et des défaillances, et de vérifier les hypothèses techniques.

6.2 Exigences

6.2.1 Le cycle de vie de sécurité d'un SIS incorporant les exigences de la série IEC 61511 doit être défini lors de la planification de la sécurité. Le cycle de vie de sécurité doit également couvrir la programmation d'application (voir 6.3.1).

6.2.2 Chaque phase du cycle de vie de sécurité du SIS doit être définie en termes de ses entrées, de ses sorties et de ses activités de vérification (voir Tableau 2).

Tableau 2 – Vue d'ensemble du cycle de vie de sécurité d'un SIS (1 de 2)

Phase ou activité du cycle de vie de sécurité		Objectifs	Exigences Article	Entrées	Sorties
Numéro de case de la Figure 7	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	Article 8	Conception du processus, agencement, équipes de personnel, cibles de sécurité	Description des dangers, des fonctions de sécurité exigées et de la réduction de risque associée
2	Affectation des fonctions de sécurité aux couches de protection	Affecter des fonctions de sécurité aux couches de protection et pour chaque SIF, le SIL associé	Article 9	Description des SIF exigées et des exigences associées concernant l'intégrité de sécurité	Description de l'allocation des exigences de sécurité
3	Spécification des exigences de sécurité d'un 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	Article 10	Description de l'allocation des exigences de sécurité	Exigences de sécurité du SIS; exigences de sécurité du programme d'application
4	Conception et ingénierie du SIS	Concevoir le SIS pour satisfaire aux exigences des SIF et leur intégrité de sécurité associée	Article 11, Article 12	Exigences de sécurité du SIS Exigences de sécurité du programme d'application	Conception du matériel et du programme d'application du SIS en conformité avec les exigences de sécurité du SIS; planification de l'essai d'intégration du SIS
5	Installation, mise en service et validation du SIS	Intégrer et soumettre à un essai le SIS Valider que le SIS satisfait, en tous points, aux exigences de sécurité en termes de SIF exigées et leur intégrité de sécurité associée	Article 14, Article 15	Conception du SIS Plan d'essai d'intégration du SIS Exigences de sécurité du SIS Plan de validation de sécurité du SIS	SIS fonctionnant entièrement en conformité avec les exigences de sécurité du SIS Résultats des essais d'intégration du SIS Résultats des activités d'installation, de mise en service et de validation

Tableau 2 (2 de 2)

Phase ou activité du cycle de vie de sécurité		Objectifs	Exigences Article	Entrées	Sorties
Numéro de case de la Figure 7	Titre				
6	Fonctionnement et maintenance du SIS	Assurer que la sécurité fonctionnelle du SIS est conservée pendant le fonctionnement et la maintenance	Article 16	Exigences de sécurité du SIS Conception du SIS Plan pour le fonctionnement et la maintenance du SIS	Résultats des activités de fonctionnement et de maintenance
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	Article 17	Exigences de sécurité du SIS révisées	Résultats des modifications du SIS
8	Déclassement	Assurer la revue, l'organisation sectorielle, mais également le caractère approprié de la SIF	Article 18	Exigences de sécurité et informations de processus conformes à la construction	SIF déclarée hors service
9	Vérification du SIS	Soumettre à un 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	Article 7, 12.5	Plan de vérification du SIS, pour chaque phase	Résultats de la vérification du SIS, pour chaque phase
10	FSA du SIS	Enquêter et arriver à un jugement sur la sécurité fonctionnelle obtenue par le SIS	Article 5	Planification pour la FSA du SIS Exigence de sécurité du SIS	Résultats de la FSA du SIS
11	Structure et planification du cycle de vie de sécurité	Etablir la manière dont les étapes du cycle de vie sont réalisées	6.2	Non applicable	Plan de sécurité

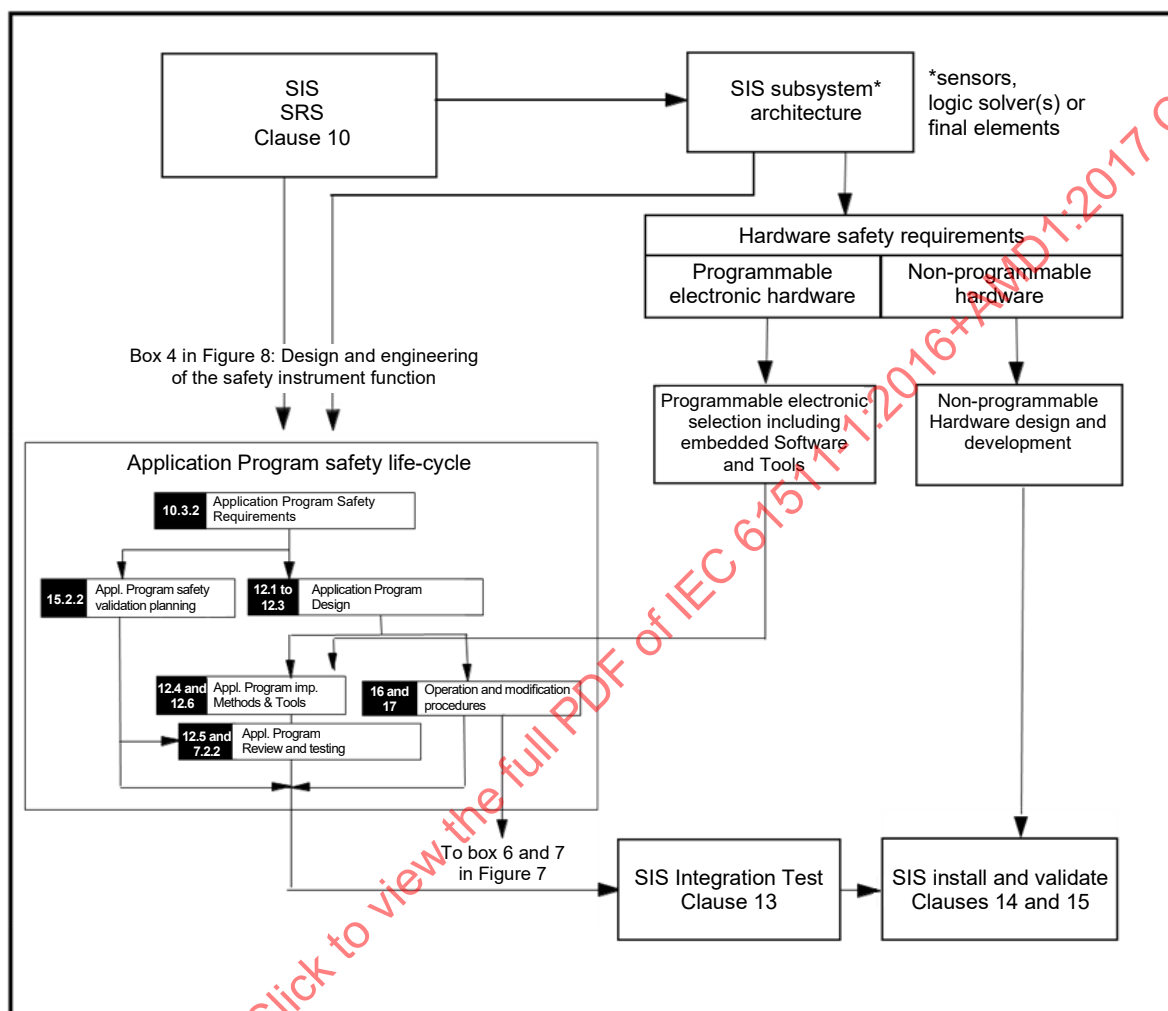
6.2.3 Pour toutes les phases du cycle de vie de sécurité du SIS, une planification de la sécurité doit avoir lieu pour définir les activités, les critères, les techniques, les mesures, les procédures, ainsi que les organisations/personnes responsables afin de:

- assurer que les exigences de sécurité du SIS sont réalisées pour tous les modes concernés du processus; cela inclut à la fois les exigences fonctionnelles et les exigences concernant l'intégrité de sécurité;
- assurer l'installation et la mise en service appropriées du SIS;
- assurer l'intégrité de la sécurité des SIF après l'installation;
- maintenir l'intégrité de sécurité lors du fonctionnement (p. ex.: essais périodiques, analyse des défaillances);
- gérer les dangers du processus pendant les activités de maintenance sur le SIS.

6.2.4 Si, à une étape quelconque du cycle de vie de sécurité, un changement est exigé sur une phase antérieure du cycle de vie, cette phase antérieure du cycle de vie de sécurité du SIS (ainsi que les phases suivantes) doivent être réexaminées, modifiées comme exigé et de nouveau vérifiées.

6.3 Exigences relatives au cycle de vie de sécurité du SIS du programme d'application

6.3.1 Chaque phase du cycle de vie de sécurité du programme d'application (voir Figure 8) doit être définie en termes de ses activités élémentaires, objectifs, informations d'entrée exigées, résultats de sortie et exigences de vérification (voir le Tableau 3).



IEC

Anglais	Français
SIS SRS Clause 10	SIS SRS Article 10
SIS subsystem* architecture	Architecture du sous-système* SIS
*sensors, logic solver(s) or final elements	*capteurs, unité(s) logique(s) ou éléments finaux
Hardware safety requirements	Exigences de sécurité du matériel
Programmable electronic hardware	Matériel électronique programmable
Non-programmable hardware	Matériel non programmable
Programmable electronic selection including embedded Software & Tools	Sélection de l'électronique programmable (logiciel intégré et outils inclus)
Non-programmable Hardware design and development	Conception et développement du matériel non programmable
Box 4 in Figure 8: Design and engineering of the safety instrument function	Case 4 de la Figure 8: Conception et ingénierie du système instrumenté de sécurité
Application Program safety life-cycle	Cycle de vie de sécurité du programme d'application

Anglais	Français
10.3.2 Application Program Safety Requirements	10.3.2 Exigences de sécurité du programme d'application
15.2.2 Appl. Program safety validation planning	15.2.2 Planification de la validation de la sécurité du programme d'application
12.1 to 12.3 Application Program Design	12.1 à 12.3 Conception du programme d'application
12.4 & 12.6 Appl. Program imp. Methods & Tools	12.4 & 12.6 Méthodes et outils de mise en œuvre du programme d'application
12.5 & 7.2.2 Appl. Program Review and testing	12.5 & 7.2.2 Revue et essai du programme d'application
16 & 17 Operation and modification procedures	16 & 17 Procédures de fonctionnement et de modification
To box 6 & 7 in Figure 7	Cases 6 et 7 de la Figure 7
SIS Integration Test Clause 13	Essai d'intégration du SIS (Article 13)
SIS install and validate Clauses 14 & 15	Installation et validation du SIS (Articles 14 et 15)
Box 5 in Figure 7	Case 5 de la Figure 7

**Figure 8 – Cycle de vie de sécurité du programme d'application
et ses relations avec le cycle de vie de sécurité du SIS**

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016+AMD1:2017 CSV

Tableau 3 – Cycle de vie de sécurité du programme d'application: vue d'ensemble
(1 de 2)

Phase du cycle de vie de sécurité		Objectifs	Exigences Article	Entrées	Sorties
Numéro de case de la Figure 8	Titre				
10.3.2	Exigences de sécurité du programme d'application	Spécifier les exigences de sécurité du programme d'application pour chaque SIS nécessaire pour mettre en œuvre les SIF exigées. Spécifier les exigences du programme d'application pour chacune des SIF allouées à ce SIS.	10.3 11.5	Exigences de sécurité du SIS. Manuels de sécurité du SIS choisis. Architecture du SIS.	Spécification des exigences de sécurité du programme d'application SIS. Informations de vérification.
15.2.2	Planification de la validation de la sécurité du programme d'application	Développer un plan de validation du programme d'application.	15.2.2, 15.2.5	Exigences de sécurité du programme d'application SIS.	Planification de la validation de sécurité du SIS. Informations de vérification.
12.1 à 12.3	Développement du programme d'application	Architecture. Créer une architecture de programme d'application qui satisfait aux exigences spécifiées pour la sécurité du programme d'application. Passer en revue et évaluer les exigences imposées au programme d'application par l'architecture matérielle du SIS. Spécifier les procédures de développement du programme d'application.	12.1 (également 10.3, 12.2)	Exigences de sécurité du programme d'application SIS. Contraintes de conception de l'architecture du matériel du SIS.	Description de la conception de l'architecture, p.ex.: ségrégation du programme d'application en sous-systèmes relatifs au processus et aux SIL, p.ex reconnaissance de modules de programme d'application communs, tels que les séquences de pompes ou de vannes. Exigences d'essai d'intégration de l'architecture et des sous-systèmes du programme d'application. Informations de vérification.
	Conception du programme d'application	Développer la conception du programme d'application. Identifier un ensemble pertinent d'outils de configuration, de bibliothèque, de gestion, de simulation et d'essai pour l'ensemble du cycle de vie de sécurité du programme d'application.	12.3	Exigences de sécurité du programme d'application SIS. Description de la conception de l'architecture. Manuels du SIS. Manuel de sécurité de l'unité logique du SIS choisie.	Conception du programme d'application. Procédures d'utilisation pendant la programmation. Description des fonctions de bibliothèque normalisées (fabricants) à utiliser. Informations de vérification.

Tableau 3 (2 de 2)

Phase du cycle de vie de sécurité		Objectifs	Exigences Article	Entrées	Sorties
Numéro de case de la Figure 8	Titre				
12.4 12.6	Mise en œuvre du programme d'application	Développer l'application et développer le module d'application. Mettre en œuvre le programme d'application qui satisfait aux exigences spécifiées pour la sécurité de l'application. Utiliser les outils de support et les langages de programmation appropriés.	12.4 12.3.4 12.6	Description de la conception. Liste des manuels et procédures de l'unité logique choisie pour l'utilisation avec le programme d'application.	Programme d'application (p.ex.: diagrammes de blocs fonctionnels, diagrammes à contacts). Simulation du programme d'application et essai d'intégration. Spécification des exigences de sécurité spéciales du programme d'application. Informations de vérification.
12.5 7.2.2	Vérification du programme d'application	Vérifier que les exigences de sécurité du programme d'application ont été satisfaites. Montrer que tous les programmes d'application du SIS interagissent correctement pour exécuter leurs fonctions prévues et n'exécutent aucune fonction non prévue.	12.5 7.2.2	Exigences d'essai de simulation et d'intégration du programme d'application (essais structurels). Exigences d'essai d'intégration de l'architecture du programme d'application.	Résultats d'essai du programme d'application. Programme d'application vérifié et soumis à l'essai. Informations de vérification.
13	Essai d'intégration du SIS	Intégrer le programme d'application sur l'unité logique cible, y compris l'interaction avec un groupe d'échantillons d'appareils de terrain et/ou un simulateur.	Article 13	Exigences d'essai d'intégration du programme d'application et de l'unité logique.	Résultats d'essai d'intégration du programme d'application et de l'unité logique.

6.3.2 Les méthodes, les techniques et les outils doivent être appliqués pour chaque phase du cycle de vie selon 12.6.2.

6.3.3 Chaque phase du cycle de vie de sécurité du SIS pour laquelle la planification de la sécurité a été réalisée doit être vérifiée (voir Article 7) et les résultats doivent être disponibles comme indiqué à l'Article 19.

7 Vérification

7.1 Objectif

L'Article 7 a pour objet de démontrer, par revue, analyse et/ou essais, que les sorties exigées satisfont aux exigences définies pour les phases appropriées (voir la Figure 7) identifiées par la planification de la vérification.

7.2 Exigences

7.2.1 La planification de la vérification doit être effectuée tout au long du cycle de vie de sécurité du SIS et doit définir l'ensemble des activités exigées pour la phase adéquate (voir Figure 7) du cycle de vie de sécurité, y compris le programme d'application. La planification de la vérification doit se conformer à la série IEC 61511 en abordant les points suivants:

- les activités de vérification;
- les procédures, les mesures et les techniques devant être utilisées pour la vérification, comprenant la mise en œuvre et la prise en compte des recommandations résultantes;
- le moment où ces activités auront lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités, y compris les niveaux d'indépendance;
- l'identification des éléments devant être vérifiés;
- l'identification des informations vis-à-vis desquelles la vérification est effectuée;
- l'adéquation des sorties par rapport aux exigences relatives à la phase en question;
- l'exactitude des données;
- la manière de traiter les non-conformités;
- les outils et l'analyse justificative;
- l'exhaustivité de la mise en œuvre du SIS et la traçabilité des exigences;
- la lisibilité et l'aptitude aux audits de la documentation;
- l'aptitude aux essais de la conception.

7.2.2 Lorsque la vérification inclut des essais, la planification de la vérification doit également aborder les points suivants:

- la stratégie d'intégration du programme d'application, du matériel et des appareils de terrain, y compris l'intégration des sous-systèmes devant satisfaire à d'autres normes (machines, brûleur, etc.);
- le domaine d'application de l'essai (description du montage d'essai et du type d'essai à réaliser, du matériel, de la programmation d'application et des appareils de programmation à inclure);
- les cas d'essai et les données d'essai (ces détails correspondront à des scénarios spécifiques avec les données associées);
- les types d'essais à exécuter;
- l'environnement d'essai comprenant les outils, le matériel, l'ensemble des logiciels ainsi que la configuration exigée;
- les critères d'essai (p. ex.: critères de réussite/d'échec) selon lesquels les résultats de l'essai seront évalués;
- les procédures relatives aux actions correctives lors d'une défaillance pendant l'essai;
- le ou les lieux physiques (p.ex.: usine ou site);
- la dépendance à l'égard d'une fonctionnalité externe;
- le personnel approprié;
- la gestion des changements;
- les non-conformités.

7.2.3 Les fonctions non liées à la sécurité intégrées à des fonctions de sécurité doivent être vérifiées pour contrôler l'absence d'interférences avec les fonctions de sécurité.

7.2.4 La vérification doit être effectuée en accord avec la planification de la vérification.

7.2.5 Durant les essais, une modification doit faire l'objet d'une analyse d'impact, qui doit déterminer l'ensemble des composants du SIS impactés, ainsi que les activités de revérification nécessaires.

7.2.6 Les résultats du processus de vérification doivent être disponibles (voir Article 19), notamment le fait de savoir si l'objectif et les critères des essais ont été satisfaits.

NOTE 1 Le choix des techniques et des mesures concernant le processus de vérification et le degré d'indépendance dépend d'un certain nombre de facteurs, notamment le degré de complexité, d'innovation de la conception, d'innovation de la technologie et du SIL exigé.

NOTE 2 Les revues de conception, l'utilisation d'outils et de techniques (dont les outils de vérification de logiciel et les outils d'analyse de conception assistée par ordinateur) sont des exemples d'activités de vérification.

8 Analyse de danger et de risque du processus

8.1 Objectifs

Les exigences de l'Article 8 visent à déterminer:

- les dangers et les événements dangereux du processus et des équipements associés;
- l'enchaînement des événements conduisant à l'événement dangereux;
- les risques de processus, associés à l'événement dangereux;
- toutes les exigences concernant la réduction de risque;
- les fonctions de sécurité exigées pour atteindre la réduction de risque nécessaire;
- si certaines des fonctions de sécurité sont des SIF.

NOTE 1 L'Article 8 de la présente norme s'adresse aux ingénieurs de processus, aux spécialistes en danger et en risque, aux responsables de la sécurité, ainsi qu'aux ingénieurs instrumentistes. Son but est de prendre en compte l'approche multidisciplinaire habituellement exigée pour la détermination des SIF.

NOTE 2 Lorsque cela est raisonnablement réalisable, les processus peuvent être conçus pour présenter une sécurité intrinsèque. Si cela n'est pas réalisable, d'autres couches de protection (voir la Figure 9) peuvent être exigées. Dans certaines applications, les normes de l'industrie peuvent spécifier l'utilisation de couches de protection particulières.

NOTE 3 Le risque peut être réduit en utilisant plusieurs couches de protection, ~~lesquelles peuvent être indépendantes, suffisantes, fiables et audibles~~ (voir Article 9).

8.2 Exigences

8.2.1 Une H&RA doit être effectuée sur les matériaux, le processus et les équipements. Elle doit avoir pour résultat:

- une description de chaque événement dangereux identifié et des facteurs qui y contribuent;
- une description de la probabilité et des conséquences de chaque événement dangereux;
- la prise en compte des modes de fonctionnement du processus, tels que le fonctionnement normal, la mise en route, l'arrêt, la maintenance, la perte de contrôle du processus et l'arrêt d'urgence;
- la détermination de la réduction de risque supplémentaire nécessaire afin d'obtenir la sécurité fonctionnelle exigée;
- une description, ou des références à, des informations concernant les mesures prises pour réduire ou éliminer les dangers et le risque;
- une description détaillée des hypothèses faites pendant l'analyse des risques, incluant notamment les taux de sollicitation sur les couches de protection et la fréquence moyenne de défaillance dangereuse des sources de déclenchement, ainsi que toute prise en compte de contraintes de fonctionnement ou d'intervention humaine;
- l'identification de la ou des fonctions de sécurité appliquées en tant que SIF.

NOTE 1 Lors de la détermination des exigences concernant l'intégrité de sécurité, les effets de la cause commune entre les systèmes qui créent les sollicitations et les couches de protection qui ont vocation à y répondre peuvent être pris en compte. Un exemple serait le cas où des sollicitations peuvent être consécutives à une défaillance du BPCS et les équipements utilisés dans les couches de protection sont similaires ou identiques aux équipements utilisés dans le système BPCS. Dans de tels cas, une sollicitation causée par une défaillance d'équipement BPCS peut ne pas être répondue efficacement si une cause commune a rendu inefficace l'équipement similaire dans la couche de protection. Les problèmes de cause commune peuvent ne pas pouvoir être reconnus pendant l'identification initiale des dangers et l'analyse de risque, car la conception

des couches de protection ne sera pas nécessairement terminée à cette première étape. Dans de tels cas, il peut s'avérer nécessaire de reconsidérer les exigences concernant l'intégrité de sécurité et la SIF à l'issue de la conception du SIS et des autres couches de protection. En déterminant si la conception globale du processus et des couches de protection satisfait aux exigences, les défaillances de cause commune seront prises en compte.

NOTE 2 Les exemples de techniques qui peuvent être utilisées pour établir les SIL exigés des SIF sont présentés dans l'IEC 61511-3:2016.

8.2.2 La fréquence moyenne de défaillance dangereuse d'un BPCS en tant que source de déclenchement ne doit pas être supposée $< 10^{-5}$ par heure.

8.2.3 La H&RA doit être consignée de telle manière que les relations entre les éléments ci-dessus soient claires et traçables.

NOTE 1 Les exigences ci-dessus n'imposent pas de devoir attribuer les exigences concernant l'intégrité de sécurité sous forme de valeurs numériques. Des approches qualitatives ou semi-quantitatives (voir l'IEC 61511-3:2016, Annexe C, Annexe D et Annexe E) peuvent également être utilisées.

NOTE 2 Les exigences concernant l'intégrité de sécurité varient en fonction de l'application et des exigences nationales légales. Un principe admis dans de nombreux pays est que des mesures supplémentaires de réduction de risque peuvent être appliquées jusqu'à ce que le coût engagé devienne disproportionné par rapport à l'intégrité de sécurité obtenue.

8.2.4 Une évaluation du risque de sécurité doit être effectuée pour identifier les failles de sécurité du SIS. Elle doit avoir pour résultat:

- une description des appareils couverts par cette évaluation du risque (p. ex.: SIS, BPCS ou tout autre appareil connecté au SIS);
- une description des menaces identifiées qui pourraient exploiter des failles et engendrer des événements de sécurité (notamment des attaques intentionnelles visant le matériel, les programmes d'application et les logiciels associés), ainsi que des événements non prévus découlant d'une erreur humaine);
- une description des conséquences potentielles résultant des événements de sécurité et la probabilité d'occurrence de ces événements;
- la prise en compte des différentes phases telles que la conception, la mise en œuvre, la mise en service, le fonctionnement et la maintenance;
- la détermination des exigences relatives à la réduction de risque supplémentaire;
- une description, ou des références à, des informations concernant les mesures prises pour réduire ou éliminer les menaces.

NOTE 1 Des lignes directrices relatives à la sécurité du SIS sont données dans l'ISA TR84.00.09, l'ISO/IEC 27001:2013 et l'IEC 62443-2-1:2010.

NOTE 2 Les informations et le contrôle des conditions limites nécessaires pour l'évaluation du risque de sécurité relèvent habituellement de la société propriétaire/exploitante d'une installation, et non du fournisseur. Si c'est le cas, l'obligation de satisfaire à 8.2.4 peut revenir à la société propriétaire/exploitante de l'installation.

NOTE 3 L'évaluation du risque de sécurité du SIS peut être rattachée à une évaluation globale du risque de sécurité relative à l'automation de processus.

NOTE 4 L'évaluation du risque de sécurité du SIS peut porter sur des éléments allant d'une SIF individuelle à l'ensemble des SIS d'une entreprise.

9 Affectation des fonctions de sécurité aux couches de protection

9.1 Objectifs

Les exigences de l'Article 9 visent à:

- affecter les fonctions de sécurité aux couches de protection;
- déterminer les SIF exigées;
- déterminer les exigences concernant l'intégrité de sécurité pour chaque SIF.

NOTE 1 Les autres normes ou codes de l'industrie peuvent être pris en compte pendant le processus d'allocation.

NOTE 2 Les exigences concernant l'intégrité de chaque SIF peuvent inclure la réduction de risque associée, la PFD, la PFH ou le SIL.

9.2 Exigences relatives au processus d'allocation

9.2.1 Le processus d'allocation doit avoir comme résultat

- l'allocation des fonctions de sécurité exigées pour réaliser la réduction de risque nécessaire aux couches de protection spécifiques;
- l'allocation de réduction de risque ou la fréquence moyenne de défaillance dangereuse à chaque SIF.

NOTE Les exigences légales ou d'autres pratiques de l'industrie peuvent influencer le processus d'allocation.

9.2.2 Le SIL exigé doit être déduit en tenant compte de la PFD ou la PFH exigée qui doit être fournie par la SIF.

NOTE D'autres lignes directrices peuvent être consultées dans l'IEC 61511-3:2016.

9.2.3 Pour chaque SIF fonctionnant en mode sollicitation, le SIL exigé doit être spécifié conformément au Tableau 4 ou au Tableau 5.

9.2.4 Pour chaque SIF fonctionnant en mode continu, le SIL exigé doit être spécifié conformément au Tableau 5.

Tableau 4 – Exigences concernant l'intégrité de sécurité: PFD_{avg}

FONCTIONNEMENT EN MODE SOLLICITATION		
Niveau d'intégrité de sécurité (SIL)	PFD_{avg}	Réduction de risque exigée
4	$\geq 10^{-5}$ à $< 10^{-4}$	$> 10\ 000$ à $\leq 100\ 000$
3	$\geq 10^{-4}$ à $< 10^{-3}$	$> 1\ 000$ à $\leq 10\ 000$
2	$\geq 10^{-3}$ à $< 10^{-2}$	> 100 à $\leq 1\ 000$
1	$\geq 10^{-2}$ à $< 10^{-1}$	> 10 à ≤ 100

Tableau 5 – Exigences concernant l'intégrité de sécurité: fréquence moyenne de défaillance dangereuse de la SIF

FONCTIONNEMENT EN MODE CONTINU OU EN MODE SOLLICITATION	
Niveau d'intégrité de sécurité (SIL)	Fréquence moyenne de défaillances dangereuses (défaillances par heure)
4	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-6}$ à $< 10^{-5}$

NOTE 1 Des explications complémentaires relatives aux modes de fonctionnement peuvent être obtenues en 3.2.39.

NOTE 2 Le SIL est défini numériquement afin de fournir une mesure de comparaison objective des conceptions et solutions alternatives. Cependant, il est reconnu qu'étant donné l'état actuel des connaissances, de nombreuses causes systématiques de défaillance ne peuvent être évaluées que qualitativement.

NOTE 3 La fréquence moyenne exigée de défaillance dangereuse pour une SIF en mode continu ou sollicitation est déterminée en tenant compte du risque causé par une défaillance de la SIF en mode continu ou sollicitation,

ainsi que les défaillances d'autres appareils conduisant au même risque, tout en prenant en considération la réduction de risque fournie par d'autres couches de protection.

9.2.5 Si le processus d'allocation donne une exigence de réduction de risque $> 10\,000$ ou une fréquence moyenne de défaillance dangereuse $< 10^{-8}$ par heure pour un ou plusieurs SIS conjointement avec une couche de protection BPCS, l'application (p. ex.: processus, autres couches de protection) doit être reconsidérée afin de déterminer si l'un des paramètres de risque peut être modifié de manière à éviter l'exigence de réduction de risque de $> 10\,000$ ou de fréquence moyenne de défaillance dangereuse $< 10^{-8}$ par heure. La revue doit notamment considérer si:

- le processus ou les cuves/tuyauteries peuvent être modifiés pour éliminer ou diminuer les dangers à la source;
- des systèmes relatifs à la sécurité complémentaires ou d'autres moyens de réduction de risque (non basés sur l'instrumentation) peuvent être introduits;
- la gravité de la conséquence peut être réduite, par exemple en réduisant la quantité de substances dangereuses;
- la probabilité d'occurrence de la conséquence indiquée peut être réduite, par exemple en diminuant la probabilité d'occurrence de la source initiatrice de l'événement dangereux.

NOTE Les applications exigeant l'utilisation d'une seule SIF avec une exigence de réduction de risque $> 10\,000$ ou une fréquence moyenne de défaillance dangereuse $< 10^{-8}$ par heure nécessitent d'être évitées compte tenu de la difficulté à réaliser et maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité du SIS. L'exigence de réduction de risque $> 10\,000$ ou la fréquence moyenne de défaillance dangereuse $< 10^{-8}$ par heure peut exiger des niveaux élevés de compétence et des niveaux élevés de couverture pour tous les essais de réception en usine, essais périodiques, vérification et activités de validation.

9.2.6 Si un examen approfondi de l'application confirme qu'une exigence de réduction de risque $> 10\,000$ ou que la fréquence moyenne de défaillance dangereuse $< 10^{-8}$ par heure est toujours exigée, il convient d'envisager la réalisation de l'exigence concernant l'intégrité de sécurité à l'aide de couches de protection multiples (p. ex.: SIS ou BPCS) faisant l'objet d'exigences de réduction de risque inférieures. Si la réduction de risque est allouée à plusieurs couches de protection, ces couches de protection doivent être indépendantes les unes des autres ou l'absence d'indépendance doit être évaluée et démontrée comme suffisamment faible par rapport aux exigences de réduction de risque. Les facteurs suivants doivent être étudiés lors de cette évaluation:

- la cause commune de défaillance du SIS et la cause de la sollicitation;

NOTE 1 L'étendue de la cause commune peut être évaluée en tenant compte de la diversité de tous les appareils dont la défaillance pourrait entraîner une sollicitation et de tous les appareils de la couche de protection BPCS et/ou du SIS utilisés pour réaliser la réduction de risque.

NOTE 2 Un exemple de cause commune entre le SIS et la cause de la sollicitation est la perte de commande du processus suite à une anomalie ou une défaillance du capteur, ce qui peut entraîner une sollicitation, le type de capteur utilisé pour la commande étant le même que celui du capteur utilisé pour le SIS.

- la cause commune de défaillance avec d'autres couches de protection fournissant la réduction de risque;

NOTE 3 L'étendue de la cause commune peut être évaluée en tenant compte de la diversité de tous les appareils de la couche de protection BPCS et/ou du SIS utilisés pour réaliser les exigences de réduction de risque.

NOTE 4 Un exemple de cause commune entre les SIS fournissant la réduction de risque est lorsque deux SIS indépendants et séparés caractérisés par des mesures diversifiées et des unités logiques diversifiées sont utilisés, mais que les appareils actionneurs terminaux sont deux vannes d'arrêt de type similaire ou une seule vanne d'arrêt commandée par les deux SIS.

- la ou les dépendances pouvant être introduites par des activités communes d'exploitation, de maintenance, d'inspection ou d'essai ou encore par des procédures d'essai périodique et des horaires d'essai périodique communs.

NOTE 5 Même si les couches de protection sont diversifiées, les essais périodiques synchrones atténueront la réduction globale de risque obtenue, ce qui peut constituer un facteur important empêchant d'atteindre la réduction de risque nécessaire pour l'événement dangereux.

NOTE 6 Si des niveaux de réduction de risque élevés sont exigés et que les essais périodiques sont désynchronisés selon la Note 5, le facteur dominant est en principe une défaillance de cause commune, même si plusieurs couches de protection indépendantes sont utilisées pour réduire le risque. La dépendance au sein

et entre les couches de protection assurant la réduction de risque pour le même événement dangereux peut être évaluée et présentée comme étant suffisamment faible.

9.2.7 Si une exigence de réduction de risque $> 10\,000$ ou si la fréquence moyenne de défaillance dangereuse $< 10^{-8}$ par heure doit être mise en œuvre, qu'elle soit allouée à un ou plusieurs SIS ou à un SIS associé à une couche de protection BPCS, une autre évaluation du risque doit être réalisée par une méthodologie quantitative visant à confirmer que les exigences concernant l'intégrité de sécurité sont satisfaites. La méthodologie doit prendre en compte les défaillances dépendantes et les défaillances de cause commune entre le SIS et:

- une autre ou d'autres couches de protection dont la défaillance entraînerait une sollicitation de celle-ci;
- un autre ou d'autres SIS réduisant la probabilité d'occurrence de l'événement dangereux;
- un autre ou d'autres moyens de réduction de risque réduisant la probabilité d'occurrence de l'événement dangereux (p. ex.: alarmes de sécurité).

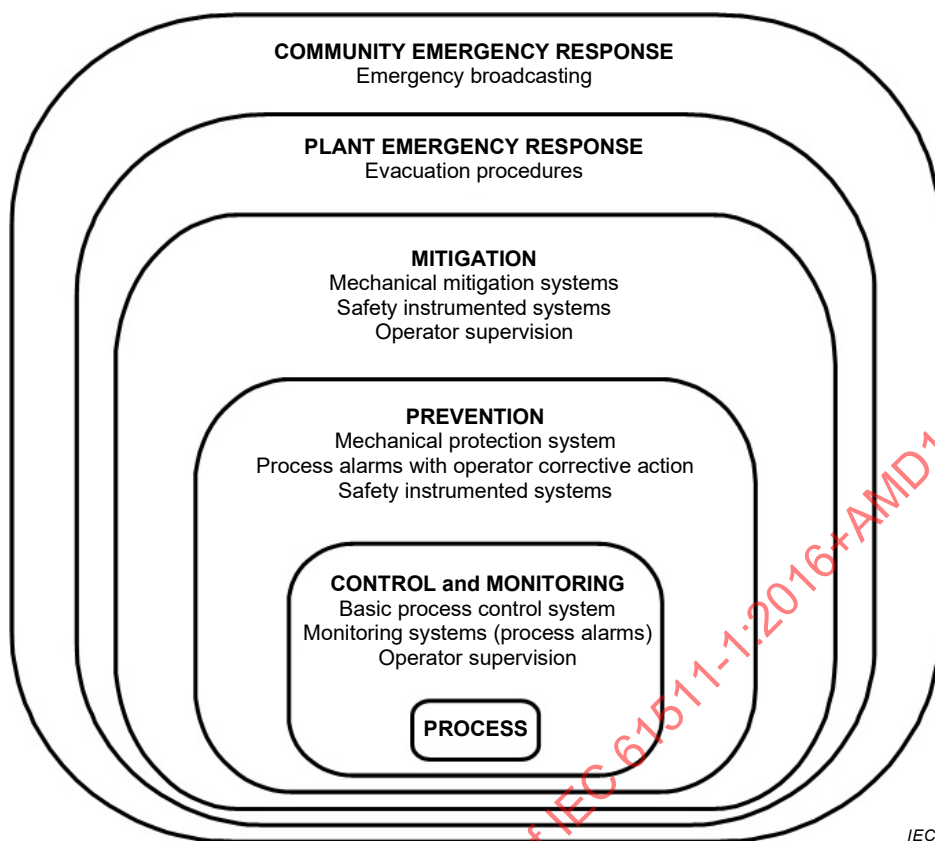
9.2.8 Si la réduction de risque exigée pour un événement dangereux est allouée à plusieurs SIF d'un même SIS, le SIS doit satisfaire à l'exigence de réduction de risque globale.

9.2.9 Les résultats du processus d'allocation doivent être consignés de manière à décrire les SIF en termes de besoins fonctionnels du processus (p. ex.: actions à entreprendre, points de consigne, temps de réaction, délais d'activation, traitement des anomalies, exigences de fermeture des vannes) et en termes d'exigences de réduction de risque.

NOTE Cette description peut se présenter sous une forme logique non ambiguë et peut être désignée comme la spécification des exigences de processus ou la description de sécurité. La description peut énoncer clairement le but et la démarche utilisée lors du processus d'allocation. La spécification des exigences de processus est utilisée comme information d'entrée pour la SRS abordée à l'Article 10. Elle peut être suffisamment détaillée pour assurer la spécification adéquate du SIS et de ses appareils. Par exemple, la description peut inclure les points de consigne relatifs aux capteurs, le temps de sécurité du processus disponible pour la réponse, ainsi que les exigences relatives à la fermeture des vannes.

9.3 Exigences relatives au système de commande de processus de base en tant que couche de protection

9.3.1 Le système de commande de processus de base peut être déclaré comme étant une couche de protection (voir la Figure 9).



IEC

Anglais	Français
COMMUNITY EMERGENCY RESPONSE	REPOSE D'URGENCE COLLECTIVE
Emergency broadcasting	Diffusion d'urgence
PLANT EMERGENCY RESPONSE	REPOSE D'URGENCE DE L'INSTALLATION
Evacuation procedures	Procédures d'évacuation
MITIGATION	ATTENUATION
Mechanical mitigation systems	Systèmes d'atténuation mécanique
Safety instrumented systems	Systèmes instrumentés de sécurité
Operator supervision	Supervision opérateur
PREVENTION	PREVENTION
Mechanical protection system	Système de protection mécanique
Process alarms with operator corrective action	Alarmes du processus avec action corrective de l'opérateur
CONTROL and MONITORING	CONTROLE et SURVEILLANCE
Basic process control system	Système de commande de processus de base
Monitoring systems (process alarms)	Systèmes de surveillance (alarmes du processus)
Operator supervision	Supervision opérateur
PROCESS	PROCESSUS

Figure 9 – Couches de protection types et moyens de réduction de risque

9.3.2 La réduction de risque revendiquée pour une couche de protection BPCS doit être ≤ 10 .

NOTE Le fait qu'un BPCS puisse également être une source initiatrice de sollicitation de la couche de protection peut également être pris en compte.

9.3.3 Si la réduction de risque revendiquée pour une couche de protection BPCS est > 10 , le BPCS doit être conçu et géré selon les exigences fournies dans la série IEC 61511.

9.3.4 S'il n'est pas prévu que le BPCS soit conforme à la série IEC 61511, alors:

- pas plus d'une couche de protection BPCS ne doit être revendiquée pour la même séquence d'événements donnant lieu à l'événement dangereux, lorsque le BPCS est la source initiatrice de la sollicitation sur la couche de protection; ou
- pas plus de deux couches de protection BPCS ne doivent être revendiquées pour la même séquence d'événements donnant lieu à l'événement dangereux, lorsque le BPCS n'est pas la source initiatrice de la sollicitation.

NOTE La couche de protection BPCS identifiée peut être composée d'un BPCS faisant office de source initiatrice de la sollicitation (voir 8.2.2) et d'une deuxième couche de protection BPCS indépendante (voir 9.3.2 et 9.3.3) ou d'au maximum deux couches de protection BPCS indépendantes lorsque la source initiatrice n'est pas liée à une défaillance du BPCS.

9.3.5 Si 9.3.4 s'applique, chaque couche de protection BPCS doit être indépendante et séparée de la source initiatrice et des autres couches de protection, dans la mesure où la réduction de risque revendiquée de chaque couche de protection BPCS n'est pas compromise.

NOTE 1 L'évaluation de la séparation et de l'indépendance peut s'appuyer sur les éléments nécessaires à la réduction de risque (p. ex.: les unités centrales de traitement ou CPU, les modules d'entrée/sortie, les relais, les appareils de terrain, la programmation d'application, les réseaux, la base de données de programme, les outils d'ingénierie, l'interface homme-machine, les outils de dérivation et autres appareils).

NOTE 2 Un contrôleur de sauvegarde à chaud n'est pas considéré comme étant indépendant du contrôleur principal, car il fait l'objet d'une défaillance de cause commune (p. ex.: les contrôleurs de sauvegarde à chaud sont dotés de composants qui sont communs au contrôleur principal et au contrôleur de sauvegarde, tels que le fond de panier, le microprogramme, le diagnostic, les mécanismes de transfert et les défaillances dangereuses non détectées).

9.4 Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes

9.4.1 La conception des couches de protection doit être évaluée pour s'assurer que la probabilité de cause commune, de mode commun et de défaillances dépendantes entre:

- les couches de protection;
- les couches de protection et le BPCS

est suffisamment faible comparée aux exigences concernant l'intégrité de sécurité globale des couches de protection. Sauf si 9.2.7 s'applique, l'évaluation peut être qualitative ou quantitative.

NOTE Une définition de la défaillance dépendante est donnée en 3.2.12.

9.4.2 L'évaluation doit prendre en compte les points suivants:

- l'indépendance entre les couches de protection;
- la diversité entre les couches de protection;
- la séparation physique entre les différentes couches de protection;
- les défaillances de cause commune entre les couches de protection et entre ces dernières et le BPCS.

NOTE 1 Les causes communes provenant du processus peuvent être prises en compte. Le blocage des vannes de limitation peut engendrer les mêmes problèmes que le blocage de capteurs dans un SIS.

NOTE 2 L'indépendance et la séparation physique peuvent être prises en compte. Une interface homme-machine, des réseaux SIS/BPCS ou des moyens de dérivation peuvent engendrer une défaillance de cause commune.

10 Spécification des exigences de sécurité (SRS) du SIS

10.1 Objectif

L'Article 10 a pour objet de spécifier les exigences relatives au SIS, y compris les programmes d'application et l'architecture du SIS.

10.2 Exigences générales

Les exigences de sécurité doivent résulter de l'allocation des SIF et des exigences identifiées lors de la H&RA. Les exigences du SIS doivent être exprimées et structurées de telle manière qu'elles soient:

- claires, précises, vérifiables, gérables et réalisables;
- écrites de manière à aider les personnes qui utiliseront les informations à bien les comprendre et les interpréter, à n'importe quelle phase du cycle de vie de sécurité.

10.3 Exigences de sécurité du SIS

10.3.1 L'objectif de 10.3 est d'aborder les questions qui doivent être prises en compte lors du développement des exigences de sécurité du SIS.

10.3.2 Ces exigences doivent suffire pour concevoir le SIS et doivent inclure une description du but et de l'approche appliquée lors du développement des exigences de sécurité du SIS le cas échéant:

- une description de toutes les SIF nécessaires afin d'obtenir la sécurité fonctionnelle exigée (p. ex.: diagramme de cause à effet, narrative logique);
 - une liste de l'ensemble des appareils d'entrée et de sortie de l'installation relatifs à chaque SIF, clairement identifiés par les moyens d'identification d'équipements de l'installation (p. ex.: liste d'étiquettes sur le terrain);
 - les exigences pour identifier et tenir compte des défaillances de cause commune;
 - une définition de l'état de sécurité du processus pour chaque SIF identifiée, par exemple un état stable a été atteint et l'événement dangereux spécifié a été éliminé ou suffisamment atténué;
 - une définition de tous les états du processus, individuellement sûrs, qui, en ayant lieu concurremment, créent un danger distinct (p. ex.: surcharge de stockage d'urgence, dégazage multiple par système à torche);
 - les sources supposées de sollicitation et le taux de sollicitation relatifs à chaque SIF;
 - les exigences relatives aux intervalles d'essais périodiques;
 - les exigences relatives à la mise en œuvre des essais périodiques;
 - les exigences de temps de réponse pour que chaque SIF conduise le processus à un état de sécurité dans le temps de sécurité du processus;
- NOTE Pour une discussion approfondie sur le temps de sécurité du processus, voir l'IEC 61511-2:2016.
- le SIL et le mode de fonctionnement (sollicitation/continu) exigés pour chaque SIF;
 - une description des mesures du processus du SIS, de la plage, de la précision et de leurs points de déclenchement;
 - une description des actions de sortie du processus de la SIF et des critères de bon fonctionnement (p. ex.: taux de fuite des vannes);
 - les relations fonctionnelles entre les entrées et les sorties du processus, y compris les fonctions logiques et mathématiques, ainsi que toutes les autorisations exigées pour chaque SIF;
 - les exigences relatives à l'arrêt manuel de chaque SIF;
 - les exigences relatives à la mise sous ou hors tension pour déclencher chaque SIF;
 - les exigences pour réinitialiser chaque SIF après un arrêt (p. ex.: exigences concernant la réinitialisation manuelle, semi-automatique ou automatique des éléments terminaux après des déclenchements);
 - le taux de déclenchement parasite permis maximal pour chaque SIF;
 - les modes de défaillance pour chaque SIF et la réponse désirée du SIS (p. ex.: alarmes, arrêt automatique);

- toutes les exigences spécifiques relatives aux procédures de démarrage et de redémarrage du SIS;
- toutes les interfaces entre le SIS et tout autre système (y compris le BPCS et les opérateurs);
- une description des modes de fonctionnement de l'installation et les exigences relatives au fonctionnement du SIF dans chaque mode;
- les exigences de sécurité du programme d'application telles que listées en 10.3.23;
- les exigences relatives aux dérivations, notamment les procédures écrites devant être appliquées à l'état dérivé qui décrivent la manière dont les dérivations seront commandées du point de vue administratif et éliminées ultérieurement;
- les spécifications de toute action nécessaire pour obtenir ou maintenir un état de sécurité du processus en cas d'anomalie(s) détectée(s) dans le SIS en tenant compte des facteurs humains pertinents;
- le temps moyen de dépannage qui est réalisable pour le SIS en tenant compte du temps du déplacement, du lieu, du stock de pièces de rechange, des contrats d'entretien, des contraintes environnementales;
- l'identification des combinaisons dangereuses des états de sortie du SIS, qui doivent être évitées;
- l'identification des valeurs extrêmes de toutes les conditions environnementales, qui sont susceptibles d'être rencontrées par le SIS pendant l'expédition, le stockage, l'installation et le fonctionnement. Cela peut exiger de tenir compte des éléments suivants: la température, l'humidité, les contaminants, la mise à la terre, les interférences électromagnétiques/les interférences dans les fréquences radio (IEM/IRF), les chocs/vibrations, les décharges électrostatiques, la classification en zones électriques, la submersion, la foudre, et tout autre facteur pertinent;
- l'identification des modes de fonctionnement normaux et anormaux du processus pour les procédures de fonctionnement, à la fois de l'installation industrielle dans son ensemble (p. ex.: mise en route de l'installation) et de l'installation individuelle (p. ex.: maintenance des équipements, étalonnage ou réparation des capteurs). Des SIF supplémentaires peuvent être exigées pour supporter ces modes de fonctionnement du processus;
- la définition des exigences pour toute SIF nécessaire pour survivre à un événement accidentel majeur (p. ex.: temps exigé pendant lequel une vanne reste opérationnelle en cas d'incendie).

10.3.3 Les exigences de sécurité du programme d'application doivent résulter de la SRS et de l'architecture du SIS choisie (disposition et structure interne). Les exigences de sécurité du programme d'application peuvent être indiquées dans la SRS ou dans un document séparé (p. ex.: spécification d'exigences du programme d'application). Les informations d'entrée pour les exigences de sécurité du programme d'application de chaque sous-système SIS doivent inclure:

- a) les exigences de sécurité spécifiées de chaque SIF, y compris le vote des capteurs, etc.;
- b) les exigences résultant de l'architecture du SIS et du manuel de sécurité (p. ex.: les limitations et les contraintes du matériel et des logiciels intégrés);
- c) toutes les exigences de la planification de la sécurité (découlant de 5.2.4).

10.3.4 Les exigences de sécurité du programme d'application doivent être spécifiées pour chaque appareil programmable du SIS nécessaire pour la mise en œuvre de la SIF exigée conformément à l'architecture du SIS.

10.3.5 La spécification des exigences de sécurité du programme d'application doit être suffisamment détaillée pour permettre à la conception et à la mise en œuvre d'obtenir la sécurité fonctionnelle exigée et de procéder à une évaluation de la sécurité fonctionnelle. Les points suivants doivent être considérés:

- les SIF prises en charge par le programme d'application et leur SIL;

- les paramètres de performances en temps réel (p. ex.: capacité de l'UC, bande passante du réseau, performances en temps réel acceptables en présence d'anomalies), ainsi que tous les signaux de déclenchement sont reçus dans un délai spécifié;
- le séquençement du programme et les retards temporels le cas échéant;
- les interfaces matérielles et opérateurs et leur efficacité opérationnelle;
- tous les modes de fonctionnement pertinents du processus, comme indiqué dans la SRS;
- les actions à prendre concernant les variables erronées du processus (p. ex.: valeur de capteur hors plage, plage de changement excessive, valeur figée, circuit ouvert détecté, court-circuit détecté);
- les fonctions permettant de procéder aux essais périodiques et aux essais de diagnostic automatiques des appareils externes (p. ex.: capteurs et éléments terminaux) dans le programme d'application;
- l'autosurveillance du programme d'application (p. ex.: chiens de garde pilotés par l'application et validation de la plage de données);
- la surveillance d'autres appareils faisant partie du SIS (p. ex.: capteurs et éléments terminaux);
- les exigences relatives aux essais périodiques de la SIF lorsque le processus est opérationnel;
- les références aux documents d'entrée (p. ex.: spécification de la SIF, configuration ou architecture du SIS, exigences concernant l'intégrité de sécurité du matériel du SIS);
- les exigences relatives aux interfaces de communication, y compris les mesures permettant de limiter leur utilisation et la validité des données et commandes reçues et transmises;
- les états dangereux du processus (p. ex.: la fermeture de deux vannes d'isolation de gaz en même temps qui pourrait entraîner des variations de pression et ainsi conduire à un état dangereux) générés par le programme d'application doivent être identifiés et évités;
- les définitions des critères de validation des variables de processus pour chaque SIF.

10.3.6 La spécification des exigences de sécurité du programme d'application doit être rédigée et structurée de manière à:

- décrire le but et l'approche déterminant les exigences de sécurité du programme d'application;
- être claire et compréhensible pour ceux qui utiliseront le document à n'importe quelle phase du cycle de vie de sécurité du SIS; cela inclut l'utilisation d'une terminologie et de descriptions non ambiguës et comprises par tous les utilisateurs (p. ex.: personnel d'exploitation et de maintenance de l'installation, programmeurs de l'application);
- être vérifiable, apte à l'essai, modifiable;
- être traçable jusqu'aux livrables, y compris les documents de conception détaillés, la SRS et l'analyse de danger et de risque qui identifie la SIF et le SIL exigés.

11 Conception et ingénierie du SIS

11.1 Objectif

Les exigences de l'Article 11 ont pour objet de concevoir un ou plusieurs SIS afin de fournir la SIF et de satisfaire aux exigences d'intégrité spécifiées (p. ex.: SIL, réduction de risque associée, PFD et/ou PFH).

11.2 Exigences générales

11.2.1 La conception du SIS doit être conforme aux spécifications des exigences de sécurité du SIS, et tenir compte de toutes les exigences de l'Article 11.

11.2.2 Si le SIS doit mettre en œuvre à la fois des SIF et des fonctions non SIF, tout le matériel, le logiciel intégré et le programme d'application pouvant avoir un impact négatif sur une SIF dans les conditions normales et en présence d'anomalies doivent être traités en tant qu'éléments du SIS et satisfaire aux exigences relatives au plus haut SIL des SIF qu'il peut impacter.

11.2.3 Si le SIS doit mettre en œuvre les SIF de différents SIL, le matériel, les logiciels intégrés et le programme d'application partagés et communs doivent être conformes au SIL le plus élevé.

NOTE Les logiciels intégrés ou les programmes d'application des différents SIL peuvent coexister dans le même appareil sous réserve de pouvoir démontrer que la SIF au SIL le plus bas ne puisse pas avoir un impact négatif sur la SIF au SIL le plus élevé.

11.2.4 S'il est prévu de ne pas qualifier le BPCS par rapport à la série IEC 61511, le SIS doit être conçu pour être distinct et indépendant du BPCS de manière à ne pas compromettre l'intégrité de sécurité du SIS.

NOTE 1 Des informations de fonctionnement peuvent être échangées, mais sans compromettre la sécurité fonctionnelle du SIS.

NOTE 2 Des appareils du SIS peuvent être également utilisés pour des fonctions du BPCS, s'il peut être démontré qu'une défaillance du BPCS ne compromet pas les SIF du SIS.

11.2.5 Les exigences concernant l'aptitude au fonctionnement, à la maintenance, aux diagnostics, aux inspections et aux essais doivent être prises en compte lors de la conception du SIS afin de réduire la probabilité de défaillances dangereuses.

11.2.6 La conception du SIS doit tenir compte des capacités et des limites humaines et être apte aux tâches assignées aux opérateurs et au personnel de maintenance. La conception des interfaces opérateur doit suivre la bonne pratique ergonomique et doit être adaptée au niveau probable de formation qu'il convient que les opérateurs reçoivent.

NOTE Par exemple, des études relatives aux facteurs humains peuvent s'avérer nécessaires si le fonctionnement exige la saisie régulière de données pour les limites ou d'autres entrées de l'opérateur.

11.2.7 Le SIS doit être conçu de telle sorte qu'après avoir placé le processus dans un état de sécurité, le processus doit rester à l'état de sécurité jusqu'à ce qu'une réinitialisation ait été lancée, sauf indication contraire dans la SRS.

11.2.8 Des moyens manuels (p. ex.: bouton poussoir d'arrêt d'urgence) indépendants de l'unité logique doivent être mis à disposition pour actionner les éléments terminaux du SIS, sauf indication contraire dans la SRS.

11.2.9 La conception du SIS doit prendre en considération tous les aspects de l'indépendance et de la dépendance entre le SIS et le BPCS et entre le SIS et les autres couches de protection.

11.2.10 Un appareil utilisé par le BPCS ne doit pas être utilisé par le SIS si une défaillance de cet appareil peut entraîner une sollicitation de la SIF et une défaillance dangereuse de la SIF, à moins qu'une analyse n'ait été réalisée pour confirmer que le risque global est acceptable.

NOTE Si une partie du SIS est également utilisée pour la commande et qu'une défaillance dangereuse des équipements communs provoquerait une sollicitation de la fonction exécutée par le SIS, un nouveau risque est alors introduit. Le risque supplémentaire dépend du taux de défaillances dangereuses de l'appareil partagé, car si l'appareil partagé subit une défaillance, une sollicitation sera créée immédiatement, à laquelle le SIS peut ne pas pouvoir répondre. C'est la raison pour laquelle une analyse supplémentaire peut s'avérer nécessaire dans ces cas, pour s'assurer que les taux de défaillances dangereuses des appareils partagés sont suffisamment bas. Les capteurs et les vannes sont des exemples où le partage des équipements avec le BPCS est souvent pris en compte.

11.2.11 S'agissant d'un appareil SIS qui, suite à une perte d'alimentation (alimentation électrique, air, hydraulique ou pneumatique), ne passe pas à l'état de sécurité, la perte d'alimentation et l'intégrité du circuit du SIS doivent être détectées et signalées (p. ex.: surveillance en bout de ligne, mesure de la pression d'alimentation, surveillance de la pression hydraulique ou pneumatique) et des actions doivent être prises conformément à 11.3.

NOTE 1 L'intégrité du réseau d'alimentation peut être améliorée grâce à une alimentation auxiliaire (p. ex.: batterie de secours, alimentations sans interruption, réservoir d'air, accumulateur hydraulique, seconde alimentation en gaz).

NOTE 2 La perte d'une alimentation est susceptible d'affecter plusieurs SIF et, éventuellement, plusieurs SIS. ~~C'est pourquoi la défaillance de cause commune de plusieurs SIF peut être prise en compte.~~

11.2.12 La conception du SIS doit permettre d'assurer la résilience nécessaire par rapport aux risques de sécurité identifiés (voir 8.2.4).

NOTE Des lignes directrices relatives à la sécurité du SIS sont données dans l'ISA TR84.00.09, l'ISO/IEC 27001:2013, et l'IEC 62443-2-1:2010.

11.2.13 Un manuel de sécurité couvrant le fonctionnement, la maintenance, la détection d'anomalie et les contraintes associées au SIS doit être disponible, portant sur les configurations prévues des appareils et sur l'environnement de fonctionnement prévu.

11.2.14 Toutes les communications utilisées pour mettre en œuvre une SIF doivent être établies au moyen de techniques appropriées pour les applications de sécurité, afin de satisfaire au SIL exigé.

11.3 Exigences relatives au comportement du système lors de la détection d'une anomalie

11.3.1 En cas de détection d'une défaillance dangereuse dans un SIS (par les essais de diagnostic, les essais périodiques ou d'autres moyens), des mesures compensatoires doivent être prises pour garantir un fonctionnement de sécurité. Si un fonctionnement de sécurité ne peut pas être assuré, une action spécifiée visant à obtenir ou maintenir un état de sécurité du processus doit être prise. Si les mesures compensatoires dépendent d'un opérateur qui entreprend une action spécifique en réponse à une alarme (p. ex.: ouverture ou fermeture d'une vanne), l'alarme doit alors être considérée comme faisant partie du SIS.

NOTE 1 L'action spécifiée (comportement sur détection d'anomalie) exigée pour obtenir ou maintenir un état de sécurité du processus peut être spécifiée dans la SRS (voir 10.3.1). Il peut s'agir d'un arrêt de sécurité du processus ou de la partie du processus qui s'appuie sur le SIS défaillant pour réduire le risque.

NOTE 2 Les mesures compensatoires exigées pour assurer un fonctionnement en toute sécurité peuvent dépendre des exigences concernant l'intégrité de sécurité, du risque tolérable lié à l'événement dangereux, de la tolérance aux défauts du matériel du SIS, du MRT anticipé et de la disponibilité des autres couches de protection. Dans certains cas, il peut être judicieux de veiller à entreprendre l'action de manière à réparer la défaillance dangereuse dans les limites du MPRT supposé dans le calcul de la PFD_{avg} , mais dans d'autres cas, il peut être jugé nécessaire de proposer d'autres mesures compensatoires de la réduction du risque tant que le SIS n'est pas intégralement rétabli. Voir également 16.2.3.

11.3.2 Lorsqu'une anomalie dangereuse dans un SIS est portée à l'attention d'un opérateur par une alarme, l'alarme doit être soumise à des essais périodiques et à une gestion des changements appropriés.

11.4 Tolérance aux défauts du matériel

11.4.1 Le SIS doit avoir une HFT minimale en ce qui concerne chaque SIF qu'il met en œuvre.

NOTE Cela n'exclut pas le fait que la HFT puisse être réduite en dessous de l'exigence minimale à certains moments du fonctionnement du système suite à l'occurrence d'anomalies.

11.4.2 Si le SIS peut être divisé en sous-systèmes SIS indépendants (p. ex.: capteurs, unités logiques et éléments terminaux), la HFT peut être attribuée au niveau du sous-système SIS.

11.4.3 La HFT du SIS ou de ses sous-systèmes SIS doit être conforme

- à 11.4.5 à 11.4.9 de l'Article 11; ou
- aux exigences de 7.4.4.2 (parcours 1H) de l'IEC 61508-2:2010; ou
- aux exigences de 7.4.4.3 (parcours 2H) de l'IEC 61508-2:2010.

NOTE L'itinéraire développé dans l'IEC 61511 est déduit du parcours 2_H de l'IEC 61508-2:2010.

11.4.4 Lors de la détermination de la HFT obtenue, certaines anomalies peuvent être exclues sous réserve que la probabilité de leur occurrence soit très faible par rapport aux exigences concernant l'intégrité de sécurité. Toute autre exclusion des anomalies doit être justifiée et documentée.

NOTE Pour plus d'informations sur l'exclusion des anomalies, l'ISO 13849-1:2006 et l'ISO 13849-2:2012 peuvent être consultées.

11.4.5 La HFT minimale d'un SIS (ou de ses sous-systèmes SIS) mettant en œuvre une SIF d'un SIL spécifié doit être conforme au Tableau 6 et à 11.4.6 et 11.4.7, selon le cas.

NOTE Les exigences de HFT du Tableau 6 représentent le système minimal ou, le cas échéant, la redondance du sous-système SIS. Selon l'application, le taux de défaillance des appareils et l'intervalle des essais périodiques, une redondance supplémentaire peut être exigée pour satisfaire au niveau de défaillances pour le SIL de la SIF conformément à 11.9.

Tableau 6 – Exigences de HFT minimale en fonction du SIL

SIL	HFT minimale exigée
1 (n'importe quel mode)	0
2 (mode à faible sollicitation)	0
2 (mode à sollicitation élevée ou continu)	1
3 (n'importe quel mode)	1
4 (n'importe quel mode)	2

11.4.6 Pour un SIS ou un sous-système SIS qui n'utilise pas d'appareils programmables FVL ou LVL, et si la HFT minimale spécifiée au Tableau 6 donne lieu à des défaillances supplémentaires et à une moindre sécurité du processus global, alors la HFT peut être réduite. Cela doit être justifié et documenté. La justification doit apporter la preuve que l'architecture proposée est apte à assurer son utilisation prévue et satisfait aux exigences concernant l'intégrité de sécurité.

NOTE La tolérance aux anomalies est la solution préférentielle pour atteindre la confiance exigée relative à l'obtention d'une architecture robuste. Lorsque 11.4.6 s'applique, la justification a pour but de démontrer que l'autre architecture proposée apporte une solution équivalente, voire meilleure. Cela peut varier en fonction de l'application et/ou de la technologie utilisée. Il s'agit, par exemple: des dispositions de sauvegarde (p. ex.: redondance analytique, remplacement de la sortie d'un capteur en défaut par les résultats de calculs physiques d'autres sorties de capteurs), 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 (p. ex.: pour les composants électroniques), la diminution de l'incertitude de fiabilité via le regroupement de plus d'informations de situation ou de jugements d'experts.

11.4.7 Si une tolérance aux anomalies nulle résulte de l'application de 11.4.6, la justification exigée par 11.4.6 doit apporter la preuve que les modes de défaillance dangereuse associés peuvent être exclus, selon 11.4.4, en tenant compte de la possibilité de défaillances systématiques.

11.4.8 Les couvertures du diagnostic des appareils programmables FVL et LVL doit être de 60 % au moins.

11.4.9 Les données de fiabilité dans le calcul du niveau de défaillance doivent être déterminées par une limite de confiance statistique supérieure d'au moins 70 %.

11.5 Exigences relatives au choix des appareils

11.5.1 Objectifs

Les exigences de 11.5 visent à:

- spécifier les exigences pour le choix des appareils qui doivent être utilisés dans le cadre du SIS;
- spécifier les exigences d'intégration d'un appareil dans l'architecture d'un SIS;
- spécifier les critères d'acceptation pour les appareils en termes de SIF associée et d'exigences concernant l'intégrité de sécurité.

11.5.2 Exigences générales

11.5.2.1 Les appareils choisis pour être utilisés dans le cadre d'un SIS avec un SIL spécifié doivent être conformes à l'IEC 61508-2:2010 et l'IEC 61508-3:2010 et/ou à 11.5.3 à 11.5.6, selon le cas.

NOTE Les appareils évalués selon l'IEC 61508-2:2010 et l'IEC 61508-3:2010 peuvent être appliqués conformément aux exigences de capacité systématique de l'IEC 61508-2:2010.

11.5.2.2 Tous les appareils doivent être aptes pour l'environnement de fonctionnement déterminé suite à l'examen de la documentation du fabricant, des contraintes spécifiées dans la SRS et des paramètres de fiabilité supposée à 11.9. L'aptitude des appareils sélectionnés doit toujours être examinée dans le contexte de l'environnement de fonctionnement.

NOTE Les appareils peuvent présenter différents taux de défaillance selon l'environnement de fonctionnement et le mode de fonctionnement. Les données de taux de défaillance disponibles auprès des fabricants peuvent ne pas être valides dans toutes les applications. Par exemple, le taux de défaillance et la distribution des modes de défaillance peuvent être différents entre une vanne fréquemment manœuvrée et une vanne demeurant immobile pendant de longues périodes.

11.5.3 Exigences relatives au choix des appareils basés sur l'utilisation préalable

11.5.3.1 Une preuve pertinente doit être disponible montrant que les appareils sont aptes à être utilisés dans le SIS.

NOTE 1 Le but principal de l'évaluation de l'utilisation antérieure est de rassembler des preuves que les erreurs systématiques dangereuses ont été réduites à un niveau suffisamment bas par rapport à l'intégrité de sécurité exigée.

NOTE 2 Le niveau de détail de la preuve peut être en adéquation avec la complexité de l'appareil concerné.

NOTE 3 L'évaluation de l'utilisation antérieure implique la collecte d'informations documentées concernant les performances des appareils dans un environnement de fonctionnement similaire. L'utilisation antérieure démontre les fonctionnalités et l'intégrité de l'appareil installé, y compris les interfaces du processus, les frontières complètes de l'appareil, les communications et les réseaux d'alimentation. Le but principal de l'évaluation de l'utilisation antérieure est de rassembler des preuves que les erreurs systématiques dangereuses ont été réduites à un niveau suffisamment bas par rapport à l'intégrité de sécurité exigée.

NOTE 4 Les données d'utilisation antérieure peuvent contribuer à une base de données pour le calcul des taux de défaillance du matériel (voir 11.9.3).

11.5.3.2 La preuve d'aptitude doit comprendre les points suivants:

- la prise en considération des systèmes de qualité, de gestion de personnel et de gestion de configuration du fabricant;
- l'identification et la spécification adéquates des appareils;

- la démonstration des performances des appareils dans des environnements de fonctionnement similaires;

NOTE 1 Dans le cas des appareils de terrain (p. ex.: capteurs et éléments terminaux) satisfaisant à une spécification donnée, le comportement de l'appareil dans l'environnement de fonctionnement est en général identique dans les applications de sécurité et dans les applications non liées à la sécurité. Par conséquent, la preuve des performances d'appareils similaires dans les applications non liées à la sécurité peut également être utilisée pour satisfaire à cette exigence.

- l'importance de l'expérience de fonctionnement.

NOTE 2 Pour des appareils de terrain, les informations relatives à l'expérience de fonctionnement figurent principalement dans les listes dressées par les utilisateurs d'équipements approuvés pour être utilisés dans leurs installations, selon un historique étendu de bon fonctionnement dans des applications de sécurité et dans des applications non liées à la sécurité, mais également sur l'élimination des équipements ne donnant pas entière satisfaction. La liste des appareils de terrain peut être utilisée à l'appui des requêtes d'expérience en fonctionnement, à condition que:

- la liste soit mise à jour et revue régulièrement;
- les appareils de terrain ne soient ajoutés que lorsqu'une expérience suffisante en fonctionnement a été acquise;
- les appareils de terrain soient retirés lorsqu'ils présentent un historique de fonctionnement non satisfaisant;
- l'environnement de fonctionnement est inclus dans la liste, si cela est pertinent.

NOTE 3 L'environnement de fonctionnement affecte de manière considérable les performances des appareils. Il est généralement recommandé de pouvoir appuyer le choix des appareils sur les performances adéquates d'un nombre suffisant d'appareils installés dans plusieurs installations pendant un temps de fonctionnement suffisant. L'expérience acquise peut laisser le temps de révéler des défaillances précoces, telles que celles liées à la spécification, la manutention, l'installation et la mise en service.

NOTE 4 Le volume d'expérience pratique nécessaire à l'obtention des données de fiabilité statistiques crédibles est en général largement supérieur comparé à l'expérience pratique nécessaire pour recueillir des preuves concernant l'utilisation antérieure.

11.5.3.3 Tous les appareils choisis sur la base de l'utilisation antérieure doivent être identifiés par un numéro de révision spécifié et doivent être commandés par une gestion de la procédure de changement. En cas de changement apporté à l'appareil, la validité perpétuelle de la preuve de l'utilisation antérieure doit être justifiée en procédant à une évaluation de la pertinence du changement effectué.

11.5.4 Exigences relatives au choix des appareils programmables FPL (p. ex.: appareils de terrain) basés sur l'utilisation préalable

11.5.4.1 Pour le SIL 1, le SIL 2 et le SIL 3, les exigences de 11.5.2 et de 11.5.3 s'appliquent, avec les paragraphes suivants.

11.5.4.2 Toutes les options de configuration de l'appareil pouvant influencer la sécurité doivent être identifiées et étudiées. Lorsque des réglages spécifiques ne sont pas définis, il est important de vérifier que les réglages par défaut de l'appareil sont confirmés comme étant adéquats. Les caractéristiques inutilisées des appareils doivent être identifiées en justifiant leur aptitude, et il doit être établi qu'elles sont peu susceptibles de compromettre les SIF exigées.

11.5.4.3 Pour la configuration et l'environnement de fonctionnement spécifiques de l'appareil, la preuve d'aptitude doit considérer:

- les caractéristiques des signaux d'entrée et de sortie;
- les modes d'utilisation;
- les fonctions et les configurations utilisées;
- l'utilisation antérieure dans des environnements de fonctionnement similaires.

11.5.4.4 En outre, pour les applications de SIL 3, l'appareil FPL doit être évalué pour démontrer que:

- l'appareil FPL peut exécuter les fonctions exigées et l'utilisation antérieure démontre qu'il existe une assez faible probabilité qu'il subisse une défaillance d'une manière qui pourrait

conduire à un événement dangereux lorsqu'il est utilisé dans le cadre du SIS, du fait de défaillances aléatoires du matériel ou d'erreurs systématiques du matériel ou du logiciel;

- les normes appropriées pour le matériel et le logiciel ont été appliquées;
- l'appareil de FPL a été utilisé ou soumis à un essai dans des configurations représentatives des profils de fonctionnement prévus.

11.5.5 Exigences relatives au choix des appareils programmables LVL basés sur l'utilisation préalable

11.5.5.1 Les exigences suivantes s'appliquent aux appareils PE utilisés dans des SIS qui mettent en œuvre des SIF de SIL 1 ou de SIL 2.

11.5.5.2 Les exigences de 11.5.4 s'appliquent.

11.5.5.3 En cas de différences entre l'environnement de fonctionnement d'un appareil comme indiqué précédemment et l'environnement de fonctionnement de l'appareil lorsqu'il est utilisé dans le SIS, ces différences doivent être identifiées et une évaluation basée sur une analyse et des essais doit être réalisée, selon le cas, pour démontrer que la probabilité des erreurs systématiques est suffisamment faible en cas d'utilisation dans le SIS.

11.5.5.4 L'expérience de fonctionnement, considérée comme étant nécessaire pour justifier l'aptitude, doit être déterminée en tenant compte:

- du SIL du SIF;
- de la complexité et de la fonctionnalité des appareils.

11.5.5.5 Pour des applications de SIL 1 ou 2, une unité logique PE configurée pour la sécurité peut être utilisée, à condition que toutes les dispositions complémentaires suivantes soient satisfaites:

- compréhension des modes de défaillance en non-sécurité;
- utilisation de techniques de configuration de la sécurité qui prennent en compte des modes de défaillance identifiés;
- logiciel intégré faisant preuve, en utilisation, d'un bon historique pour des applications de sécurité;
- protection contre les modifications non autorisées ou non prévues.

NOTE Une unité logique PE configurée pour la sécurité est une unité logique de catégorie "électronique programmable pour usage général industriel", spécifiquement configurée par l'OEM, un ingénieur système ou l'utilisateur final dans des applications de sécurité.

11.5.5.6 Une unité logique PE utilisée dans une application de SIL 2 doit faire l'objet d'une évaluation formelle pour démontrer que:

- elle peut exécuter les fonctions exigées et l'utilisation antérieure a démontré qu'il existe une assez faible probabilité qu'elle subisse une défaillance d'une manière qui pourrait conduire à un événement dangereux lorsqu'elle est utilisée dans le cadre du SIS, du fait de défaillances aléatoires du matériel ou d'erreurs systématiques du matériel ou du logiciel;
- des mesures sont mises en œuvre pour détecter des erreurs pendant l'exécution du programme et déclencher des réponses adéquates; ces mesures doivent comprendre l'ensemble des points suivants:
 - surveillance de la séquence du programme;
 - protection par code contre les modifications ou la détection des défaillances par surveillance en ligne;
 - programmation par assertion (technique d'affirmation) des défaillances ou diversité logicielle;

- vérification des plages de variables ou contrôle de la vraisemblance des valeurs;
- approche modulaire;
- les normes de codage appropriées ont été utilisées pour le logiciel intégré et utilitaire;
- elle a été soumise à des essais dans des configurations typiques, avec des scénarios d'essai représentatifs des profils de fonctionnement prévus;
- des modules logiciels et des composants éprouvés/vérifiés ont été utilisés;
- le système a subi une analyse et des essais dynamiques;
- le système n'utilise pas d'intelligence artificielle ni de reconfiguration dynamique;
- des essais documentés d'insertion d'erreur (essais négatifs) ont été réalisés.

11.5.6 Exigences relatives au choix des appareils programmables FVL

Si les applications sont programmées à l'aide d'un FVL, l'appareil PE doit être conforme à l'IEC 61508-2:2010 et l'IEC 61508-3:2010.

11.6 Appareils de terrain

11.6.1 Les appareils de terrain doivent être choisis et installés pour réduire au minimum les défaillances qui pourraient engendrer des informations imprécises du fait de circonstances provenant de l'environnement de fonctionnement. Les conditions qu'il convient de considérer comprennent: la corrosion, le gel des matériaux dans les tuyauteries, les solides en suspension, la polymérisation, la cuisson, les températures et pressions extrêmes, la condensation dans les colonnes sèches à action et réaction, ainsi que la condensation insuffisante dans les colonnes humides du même type.

11.6.2 La mise sous tension pour déclencher des circuits doit appliquer un moyen assurant l'intégrité du circuit et de l'alimentation.

NOTE 1 Il s'agit, par exemple, d'un moniteur de bout de ligne, où un courant pilote est surveillé en permanence pour détecter la continuité du circuit et où l'amplitude du courant pilote n'est pas suffisante pour avoir un impact sur le bon fonctionnement des entrées/sorties.

NOTE 2 Des exigences supplémentaires relatives à la perte de puissance peuvent être consultées en 11.2.11.

11.6.3 Les capteurs intelligents doivent être protégés en écriture pour prévenir une modification involontaire, sauf si une revue de sécurité appropriée permet l'utilisation de la lecture/écriture (p. ex.: H&RA).

NOTE La revue peut tenir compte des facteurs humains, tels que le non-respect des procédures.

11.7 Interfaces

11.7.1 Généralités

Les interfaces au SIS peuvent comprendre, mais sans s'y limiter:

- la ou les interfaces opérateur;
- la ou les interfaces de maintenance/d'ingénierie;
- la ou les interfaces de communication.

11.7.2 Exigences relatives à l'interface opérateur

11.7.2.1 Lorsque l'interface opérateur du SIS s'effectue par l'intermédiaire de l'interface opérateur du BPCS, il doit être tenu compte des défaillances prévisibles qui peuvent se produire au sein de l'interface opérateur du BPCS.

NOTE La préparation de plans visant à assurer un arrêt de sécurité correct en cas de défaillance totale des affichages de fonctionnement peut être incluse.

11.7.2.2 La conception du SIS doit minimiser la nécessité pour l'opérateur de faire des choix d'options et la nécessité de dériver le système alors que des dangers sont présents. Si la conception exige l'utilisation d'actions de la part de l'opérateur, il convient que la conception inclue des fonctions de protection contre les erreurs de l'opérateur.

NOTE Si l'opérateur doit choisir une option particulière, il peut y avoir une étape de confirmation.

11.7.2.3 Les commutateurs ou les moyens de dérivation doivent être protégés de manière à éviter toute utilisation non autorisée (p. ex.: des interrupteurs à clé ou des mots de passe, associés à des contrôles de gestion efficace).

NOTE L'application de délais concernant le fonctionnement en dérivation, ainsi que la limitation du nombre de dérivations pouvant être actives à un moment donné peuvent être envisagées.

11.7.2.4 Les informations d'état du SIS qui sont critiques pour maintenir la SIF doivent être disponibles, en tant qu'éléments de l'interface opérateur. Ces informations peuvent comprendre:

- où en est le processus dans sa séquence;
- l'indication qu'une action de protection du SIS a eu lieu;
- l'indication qu'une fonction de protection est dérivée;
- l'indication qu'une (des) action(s) automatique(s), comme la dégradation du vote majoritaire et/ou la gestion des anomalies, a eu lieu;
- l'état des capteurs et des éléments terminaux;
- la perte d'énergie, dans le cas où cette dernière affecte la sécurité;
- les résultats des diagnostics;
- les défaillances des équipements de conditionnement environnemental, qui sont nécessaires pour assister le SIS.

11.7.2.5 La conception de l'interface opérateur du SIS (voir 11.7.2.7) doit être telle qu'elle ne permet pas d'apporter des changements au programme d'application du SIS.

11.7.2.6 Si les informations sont transférées du BPCS vers le SIS, les systèmes, les équipements ou les procédures doivent être appliqués afin de confirmer que les bonnes informations ont été transférées et que l'intégrité de sécurité du SIS n'est pas compromise.

NOTE Les systèmes, équipements ou procédures utilisés peuvent inclure un contrôle de l'écriture sélective du BPCS dans des variables SIS spécifiques.

11.7.2.7 La conception de l'interface opérateur du SIS via l'interface opérateur du BPCS doit être prévue de sorte que la sécurité ne doit pas être compromise si le BPCS envoie des informations ou des données incorrectes au SIS.

11.7.3 Exigences relatives à l'interface de maintenance/d'ingénierie

11.7.3.1 La conception de l'interface de maintenance/d'ingénierie du SIS doit garantir qu'aucune défaillance de cette interface ne doit compromettre l'aptitude du SIS à réaliser les SIF exigées. Cela peut exiger la déconnexion des interfaces de maintenance/d'ingénierie, comme les appareils de programmation, pendant le fonctionnement normal du SIS.

11.7.3.2 L'interface de maintenance/d'ingénierie doit fournir la protection de sécurité des accès à chacune des fonctions suivantes:

- mode de fonctionnement du SIS, programme, données, moyens de désactiver la communication des alarmes, essai, dérivation, maintenance;
- diagnostics du SIS, services de vote majoritaire et de gestion des anomalies;
- ajout, suppression ou modification du programme d'application;

- données nécessaires pour dépanner le SIS;
- dans le cas où des dérivations sont exigées, il convient qu'elles soient installées de telle manière que les alarmes et les appareils manuels d'arrêt ne soient pas désactivés.

11.7.3.3 L'interface de maintenance/d'ingénierie ne doit pas être utilisée comme interface opérateur.

11.7.3.4 L'activation et la désactivation de l'accès en lecture/écriture ne doivent être réalisées que par un processus de gestion de configuration utilisant l'interface de maintenance/d'ingénierie avec la documentation et les mesures de sécurité appropriées, telles que l'authentification et les canaux sécurisés utilisateur.

11.7.4 Exigences relatives à l'interface de communication

11.7.4.1 La conception d'une interface de communication du SIS doit garantir qu'aucune défaillance de l'interface de communication ne doit compromettre l'aptitude du SIS à obtenir ou maintenir un état de sécurité du processus.

11.7.4.2 Lorsque le SIS peut communiquer avec le BPCS et les périphériques, l'interface de communication, le BPCS ou les périphériques ne doivent pas avoir un impact défavorable sur une ou plusieurs SIF du SIS.

11.7.4.3 L'interface de communication doit être suffisamment robuste pour résister aux interférences électromagnétiques, y compris les surtensions, sans entraîner une défaillance dangereuse du SIS.

11.7.4.4 L'interface de communication doit être apte à assurer la communication entre des appareils référencés à différents potentiels électriques de mise à la terre.

NOTE Un autre support (p. ex.: les fibres optiques) peut être exigé.

11.8 Exigences relatives à la maintenance ou à la conception des essais

11.8.1 La conception doit tenir compte des essais du SIS, dans sa globalité ou par segments. Dans le cas où l'intervalle entre les temps d'arrêt programmés du processus est plus grand que l'intervalle entre les essais périodiques, des fonctions d'essai en ligne sont exigées.

NOTE Le terme "de bout en bout" signifie le déroulement fluide du processus entre l'extrémité côté capteur et l'extrémité côté actionnement.

11.8.2 Lorsque des essais périodiques en ligne sont exigés, les installations d'essai doivent faire partie intégrante de la conception du SIS.

11.8.3 Lorsque des installations d'essai ou de dérivation sont incluses dans le SIS, elles doivent être conformes aux points suivants:

- le SIS doit être conçu selon les exigences de maintenance et d'essai définies dans la SRS;
- l'opérateur doit être alerté lors de la dérivation d'une partie du SIS par l'intermédiaire d'une alarme ou d'une procédure de fonctionnement.

11.8.4 La durée maximale pendant laquelle le SIS peut demeurer en dérivation (réparation ou essai) pendant la poursuite du fonctionnement en toute sécurité du processus doit être définie.

11.8.5 Des mesures compensatoires assurant un fonctionnement en toute sécurité doivent être fournies selon 11.3 lorsque le SIS est en dérivation (réparation ou essai).

11.8.6 Le forçage des entrées et des sorties dans le SIS PE ne doit pas être utilisé dans le cadre du/des programme(s) d'application, de la/des procédure(s) de fonctionnement et de la maintenance (sauf indication contraire ci-dessous).

Le forçage des entrées et des sorties ne doit pas être permis sans mettre le SIS hors service, sauf s'il est complété par des procédures et une sécurité d'accès. Ce forçage doit faire l'objet d'une annonce ou d'une alarme, suivant les cas.

11.9 Quantification de défaillance aléatoire

11.9.1 Le niveau calculé de défaillances de chaque SIF doit être supérieur ou égal au niveau objectif de défaillances relatif au SIL spécifié dans la SRS. Cela doit être déterminé par calcul.

NOTE Dans les applications complexes, la fréquence d'événements dangereux peut être utilisée comme alternative aux niveaux objectifs de défaillances (p. ex.: lorsque différentes causes de sollicitation font l'objet de différentes exigences concernant l'intégrité de sécurité ou lorsque des SIS non indépendants agissent de manière séquentielle).

11.9.2 Le niveau calculé de défaillances de chaque SIF dû à des défaillances aléatoires doit prendre en compte tous les facteurs de contribution, y compris:

- a) l'architecture du SIS et de ses sous-systèmes SIS, lorsque cela présente un intérêt en rapport avec chaque SIF à l'étude;
- b) le taux estimé de défaillances relatif à chaque mode de défaillance, du fait de défaillances aléatoires du matériel, qui contribueraient à une défaillance dangereuse du SIS, mais qui sont détectées par les essais de diagnostic;
- c) le taux estimé de défaillances relatif à chaque mode de défaillance, du fait de défaillances aléatoires du matériel, qui contribueraient à une défaillance dangereuse du SIS, non détectées par les essais de diagnostic, mais détectées par les essais périodiques;
- d) le taux estimé de défaillances relatif à chaque mode de défaillance, du fait de défaillances aléatoires du matériel, qui contribueraient à une défaillance dangereuse du SIS, non détectées par les essais de diagnostic, ni par les essais périodiques;
- e) la susceptibilité du SIS aux défaillances causées par les essais périodiques eux-mêmes;
- f) la susceptibilité du SIS aux défaillances de cause commune;
- g) la couverture du diagnostic de tous les essais périodiques de diagnostic, l'intervalle associé pour les essais de diagnostic et la probabilité de défaillance des installations de diagnostic;
- h) la couverture de tous les essais périodiques, la procédure d'essai périodique associée, ainsi que la fiabilité de la procédure et des installations d'essai périodique;
- i) les temps de réparation relatifs aux défaillances détectées et l'état du SIS pendant les réparations (en ligne ou hors ligne);
- j) le taux estimé de défaillance dangereuse des processus de communication dans tous les modes qui provoquerait une défaillance dangereuse du SIS (détectée et non détectée par les essais de diagnostic);
- k) la probabilité estimée que la réponse de l'opérateur provoquer une défaillance dangereuse du SIS (détectée et non détectée par les essais de diagnostic);
- l) la fiabilité d'un réseau d'alimentation nécessaire au SIS.

NOTE Plusieurs approches de modélisation sont disponibles, et il appartient à l'analyste de déterminer l'approche la plus appropriée, qui peut dépendre des circonstances. Les moyens disponibles comprennent (voir l'IEC 61508-6:2010, Annexe B):

- l'analyse cause-conséquence;
- les diagrammes de fiabilité;
- l'analyse par arbre de panne;
- les modèles de Markov;
- les modèles de réseaux de Petri.

Les calculs probabilistes peuvent être réalisés de manière analytique ou par simulation numérique (p. ex.: simulation de Monte-Carlo).

11.9.3 Les données de fiabilité utilisées lors de la quantification de l'effet des défaillances aléatoires doivent être crédibles, traçables, documentées, justifiées et doivent s'appuyer sur des informations de situation provenant d'appareils similaires utilisés dans un environnement de fonctionnement similaire.

NOTE 1 Cela inclut les données collectées par l'utilisateur, les données constructeur/fournisseur/utilisateur dérivées des données collectées à partir des appareils, les données provenant de bases de données de fiabilité générales basées sur les informations de situation, etc. Dans certains cas, le jugement technique peut être utilisé pour analyser les données de fiabilité manquantes ou évaluer l'impact sur les données de fiabilité collectées dans un environnement de fonctionnement différent.

NOTE 2 L'absence de données de fiabilité représentatives de l'environnement de fonctionnement est un défaut récurrent des calculs probabilistes. Les utilisateurs finaux peuvent organiser les ensembles de données de fiabilité d'appareils appropriés conformément à l'IEC 60300-3-2:2004 ou à l'ISO 14224:2006 pour améliorer la mise en œuvre de la série IEC 61511.

NOTE 3 Les données constructeur basées sur les retours peuvent être limitées à une population ayant une parfaite connaissance de l'environnement de fonctionnement, puis consignées intégralement conformément à l'IEC 60300-3-2:2004 ou à l'ISO 14224:2006. L'utilisateur peut également consigner l'environnement de fonctionnement de la SIF et être apte à démontrer que les données d'environnement de fonctionnement du constructeur correspondent à l'environnement de la SIF.

11.9.4 Les incertitudes concernant les données de fiabilité doivent être évaluées et prises en compte lors du calcul des niveaux de défaillance.

NOTE 1 Les incertitudes concernant les données de fiabilité peuvent être évaluées en fonction de la quantité d'informations de situation disponibles (moins il y a d'informations de situation, plus l'incertitude est grande) et/ou du jugement d'un expert. Les normes publiées (IEC 60605-4), les approches bayésiennes, les techniques de jugement technique, etc. peuvent être utilisées pour estimer les incertitudes concernant les données de fiabilité.

NOTE 2 Les techniques suivantes peuvent être utilisées pour calculer les niveaux de défaillance (de plus amples informations peuvent être consultées dans l'IEC 61511-2:2016):

- l'utilisation d'une limite de confiance supérieure de 70 % pour chaque paramètre de fiabilité d'entrée au lieu de sa moyenne afin d'obtenir des estimations ponctuelles conservatrices des niveaux de défaillance; ou
- l'utilisation des fonctions de distributions probabilistes des paramètres de fiabilité d'entrée, la réalisation de simulations de Monte-Carlo pour produire un histogramme représentant la distribution du niveau de défaillance et l'évaluation d'une valeur conservatrice de cette distribution (p. ex.: pour vérifier qu'il existe un niveau de confiance de 90 % que le véritable niveau de défaillance est meilleur que la valeur calculée).

11.9.5 Si, pour une conception particulière, le niveau objectif de défaillances de la SIF concernée n'est pas atteint, alors:

- a) identifier les appareils ou paramètres contribuant le plus au niveau de défaillances;
NOTE L'analyse de coupe par arbre des défaillances peut être utile ici.
- b) évaluer l'effet des mesures d'amélioration possibles sur les appareils ou paramètres identifiés (p. ex.: appareils plus fiables, défenses supplémentaires contre les défaillances de mode commun, couverture élargie des essais périodiques et des essais de diagnostic, redondance renforcée, rapprochement des essais périodiques, décalage des essais, etc.);
- c) sélectionner et mettre en œuvre des mesures d'amélioration visant à établir le nouveau résultat;
- d) comparer le nouveau résultat au niveau objectif de défaillances et répéter les étapes a) à d) jusqu'à ce que le niveau objectif de défaillances soit atteint de manière prudente.

12 Développement du programme d'application du SIS

12.1 Objectif

L'Article 12 a pour objet de définir les exigences relatives au développement du programme d'application.

12.2 Exigences générales

12.2.1 Le programme d'application du SIS doit satisfaire aux exigences de sécurité du programme d'application (voir 10.3.3) et à toutes les exigences du présent article pour tous les SIL jusqu'au SIL 3 inclus.

12.2.2 Le programmeur d'application doit passer en revue les informations de la SRS et les exigences de sécurité du programme d'application pour s'assurer que les exigences sont exhaustives, sans équivoque, compréhensibles et cohérentes. Toutes les insuffisances dans les exigences de sécurité du programme d'application doivent être identifiées et résolues, et une analyse d'impact doit être effectuée si ces exigences ont fait l'objet de changements.

12.2.3 La série IEC 61511 aborde la programmation en langage de variabilité limitée (LVL) et l'utilisation d'appareils utilisant les langages de programme figés (FPL). La série IEC 61511 n'aborde ni le langage de variabilité totale (FVL) ni la programmation d'application SIL 4. Si des blocs fonctionnels sont écrits en langage FVL, ils doivent être développés et modifiés conformément à l'IEC 61508-3:2010.

12.2.4 Si le programme d'application du SIS doit mettre en œuvre à la fois des fonctions de sécurité et des fonctions non liées à la sécurité, l'ensemble du programme d'application doit être traité comme faisant partie intégrante du SIS et doit satisfaire à la présente norme. En outre, une évaluation et un essai doivent permettre de démontrer que les fonctions non liées à la sécurité ne peuvent pas interférer avec les fonctions de sécurité.

12.2.5 Le programme d'application doit être conçu de manière à garantir que, après que le SIS a placé le processus dans un état de sécurité, le processus reste à l'état de sécurité, y compris dans des conditions de perte de puissance et à la restauration de l'alimentation, jusqu'à ce qu'une réinitialisation ait été lancée, sauf indication contraire dans la SRS.

NOTE 1 Si la SIF ne fait pas l'objet d'une réinitialisation, un argument technique peut être documenté, expliquant les raisons pour lesquelles il est acceptable de réinitialiser le processus sans exiger le délai de sécurité qu'une réinitialisation imposerait.

NOTE 2 De plus amples informations peuvent être consultées en 11.2.7.

12.2.6 Durant le démarrage (ou la mise sous tension) du SIS, le programme d'application doit garantir que les sorties de sécurité demeurent dans un état de sécurité (habituellement à l'état de mise hors tension) jusqu'à ce qu'une réinitialisation ait été déclenchée, sauf indication contraire dans la SRS.

12.2.7 Le programme d'application doit être conçu de telle sorte que toutes les parties du programme d'application soient exécutées à chaque analyse du programme d'application à moins qu'une autre exigence spécifique ne soit spécifiée dans le manuel de sécurité. Les exigences concernant le temps de sécurité du processus doivent être prises en compte lors de l'établissement des exigences d'analyse du programme d'application.

12.2.8 Le programme d'application et les données du SIS doivent être soumis aux procédures de modification, de contrôle de révision, de gestion de versions, de sauvegarde et de restauration.

12.2.9 ~~Le programme d'application spécifie les exigences relatives à la programmation d'application pour les intégrateurs et utilisateurs des SIS. En particulier, les exigences pour les points suivants sont spécifiées~~ La planification du cycle de vie de sécurité du programme d'application SIS doit aborder les aspects suivants:

- les phases et activités du cycle de vie de sécurité relatif au SIS devant être appliquées pendant la conception et le développement du programme d'application. Ces exigences incluent l'application de mesures et de techniques qui visent à éviter des erreurs dans le programme d'application et à contrôler les défaillances pouvant se produire;

- les informations relatives à la validation du programme d'application devant être transmises à l'organisme en charge de l'intégration du SIS;
- la préparation des informations et procédures ~~concernant le programme d'application~~ dont l'utilisateur a besoin pour le fonctionnement et la maintenance du SIS;
- les procédures et spécifications devant être satisfaites par l'organisme en charge des modifications du programme d'application.

12.3 Conception du programme d'application

12.3.1 Une conception de programme d'application doit gérer l'ensemble de la logique SIS, y compris tous les modes de fonctionnement du processus pour chaque SIF.

12.3.2 L'entrée pour la conception du programme d'application doit être la SRS qui inclut les exigences du programme d'application (voir l'Article 10), l'architecture du SIS (voir l'Article 11), ainsi que les méthodes et outils utilisés pour le développement de la conception du programme d'application (voir 12.6). La conception de programme d'application doit être cohérente avec la SRS et traçable jusqu'à celle-ci.

12.3.3 La conception de programme d'application doit permettre de réaliser une évaluation de la sécurité fonctionnelle.

12.3.4 La conception de programme d'application et sa décomposition en modules (si applicable) doivent traiter la manière dont les exigences doivent être mises en œuvre, ainsi que les points suivants selon le cas:

- les fonctions qui permettent au processus d'atteindre ou de maintenir un état de sécurité;
- la spécification de tous les composants du programme d'application identifiés, et la description des liaisons et interactions entre les composants identifiés;
- les contraintes de synchronisation associées aux fonctions du programme d'application et leur mise en œuvre dans la/les durée(s) d'analyse du programme;
- une description détaillée des modules de bibliothèque normalisés (blocs de fonctions) utilisés;
- une description détaillée des modules d'application spécifiques (blocs de fonctions) utilisés;
- une description de la manière dont l'allocation de mémoire a été réalisée;
- la liste des variables globales utilisées et la manière dont leur intégrité est protégée;
- l'identification de toutes les fonctions non SIF et des interfaces avec les parties non liées à la sécurité du programme d'application pour s'assurer qu'elles ne peuvent pas affecter le fonctionnement correct des SIF;
- la définition des interfaces d'entrée et de sortie, notamment les listes d'étiquettes et les types de données associés;
- les détails des données échangées entre le programme d'application SIS et les interfaces opérateur;
- les détails des données échangées entre le programme d'application SIS et le BPCS et les périphériques tels que des imprimantes, du stockage de données, etc.;
- la manière dont les informations de diagnostic internes et externes seront traitées et journalisées;
- une description détaillée de la manière dont les interfaces de fonctionnement et de maintenance sont mises en œuvre, notamment comment les alarmes sont priorisées, indiquées et acceptées;
- une description détaillée des diagnostics au niveau application qui peuvent être mis en œuvre, tels que les chiens de garde externes, la vérification de l'intégrité des données ou encore la validation des capteurs pour satisfaire au SIL exigé;

- les contrôles de configuration du système, comprenant l'existence et l'accessibilité des appareils matériels et modules logiciels attendus;
- la manière dont la complexité de la conception de programme d'application est minimisée (p. ex.: grâce à l'utilisation d'une conception modulaire et de fonctionnalités simples);
- les fonctions relatives à la détection, l'annonce et la gestion des anomalies des sous-systèmes SIS;
- les fonctions relatives aux essais périodiques des SIF en ligne;
- les fonctions relatives aux essais périodiques des SIF hors ligne;
- les fonctions permettant d'effectuer la maintenance du SIS en toute sécurité;
- les références aux documents sur lesquels est basée la spécification de la conception du programme d'application.

12.3.5 La conception du programme d'application doit garantir:

- la complétude par rapport à la SRS et son utilisation prévue;
- l'exactitude par rapport à la SRS et son utilisation prévue;
- l'absence d'ambiguïtés, c'est-à-dire que la conception soit claire pour ceux qui utiliseront le document à n'importe quelle étape du cycle de vie de sécurité du SIS; cela inclut l'utilisation d'une terminologie et de descriptions non ambiguës et comprises par le personnel d'exploitation de l'installation et le personnel de maintenance système, ainsi que les programmeurs d'application;
- l'absence d'erreurs de conception.

12.4 Mise en œuvre du programme d'application

12.4.1 La méthodologie de développement du programme d'application doit satisfaire aux outils et restrictions de développement formulés par le fabricant du sous-système PE SIS sur lequel le programme d'application doit être utilisé.

12.4.2 Les informations suivantes doivent être contenues dans le programme d'application ou la documentation associée:

- a) l'origine du programme d'application;
 - b) une description du but du programme d'application;
 - c) les versions des manuels de sécurité qui ont été utilisés;
 - d) l'identification des dépendances de chaque SIF sur les parties (modules) du programme d'application;
 - e) la traçabilité de la spécification des exigences de sécurité du programme d'application;
 - f) l'identification de chaque SIF et de son SIL;
 - g) l'identification et la description des symboles utilisés, notamment les conventions logiques, les fonctions de bibliothèque normalisées, les fonctions de bibliothèque d'applications;
 - h) l'identification des signaux d'entrée et de sortie de l'unité logique SIS;
 - i) lorsque le SIS global utilise des communications, une description du flux d'informations de communication;
- NOTE Il s'agit, par exemple, d'une SIF utilisant plusieurs unités logiques.
- j) une description de la structure du programme, notamment une description de l'ordre du traitement logique des données par rapport aux sous-systèmes d'entrée/de sortie ainsi que les limitations imposées par les durées d'analyse;
 - k) Si cela est exigé par la SRS, les moyens permettant d'assurer:
 - l'exactitude des données de terrain (p. ex.: comparaison entre les capteurs analogiques pour améliorer la couverture du diagnostic);

- l'exactitude des données envoyées via une liaison de communication (p. ex.: lors d'une communication à partir d'une IHM, avant la mise en œuvre d'une commande, un acquittement "ack" est transmis);
- les communications sont sécurisées (p. ex.: mesures de cybersécurité).

l) l'identification des versions et un historique des changements.

12.4.3 Si des fonctions de bibliothèque du programme d'application précédemment développé doivent être utilisées dans le cadre de la conception, leur aptitude doit être justifiée et basée sur les points suivants:

- la conformité à l'IEC 61508. Si une évaluation validée en utilisation pour le FVL conformément à l'IEC 61508-3:2010 est réalisée, les appareils programmables sur lesquels les fonctions de bibliothèque du programme d'application s'exécutent doivent également être évalués et validés en utilisation (voir l'IEC 61508-2:2010); ou
- la conformité aux exigences d'utilisation antérieure de l'IEC 61511 (voir 11.5.4 ou 11.5.5) lors de l'utilisation d'un FPL ou d'un LVL;
- dans tous les cas, la démonstration que les fonctions inutilisées n'ont pas d'impact négatif sur le programme d'application.

12.4.4 Le programme d'application doit être créé d'une manière structurée de manière à obtenir:

- une décomposition modulaire des fonctionnalités;
- maintenir la complexité du programme d'application de la SIF à un niveau minimal en cohérence avec la complexité de la SIF exigée;
- l'aptitude aux essais des fonctionnalités (y compris les fonctions de tolérance aux erreurs) et de la structure interne du programme d'application;
- la traçabilité vis-à-vis des fonctions de l'application et des contraintes associées et leur explicitation;
- le mapping un à un entre l'architecture matérielle et l'architecture du programme d'application.

12.5 Exigences relatives à la vérification du programme d'application (revue et essai)

12.5.1 La planification de la vérification doit être réalisée conformément à l'Article 7.

12.5.2 Le programme d'application (y compris sa documentation) doit faire l'objet d'une revue par une personne compétente non impliquée dans le développement d'origine. L'approche utilisée pour la revue et les résultats de la revue doivent être documentés.

12.5.3 Le programme d'application (y compris sa décomposition en modules, le cas échéant) doit faire l'objet d'une vérification grâce à des techniques de revue, d'analyse, de simulation et d'essai reposant sur des procédures et des spécifications d'essai écrites, qui doit être effectuée afin de confirmer que les fonctions du programme d'application satisfont à la SRS, qu'aucune fonction non prévue n'est exécutée et qu'il n'existe pas d'effets secondaires non prévus vis-à-vis de la SIF. Les points suivants doivent être considérés:

- la conformité à la spécification de la conception du programme d'application, aux moyens et procédures définis, ainsi qu'aux exigences de validation de la sécurité et de planification des essais;
- l'exercice de toutes les parties du programme d'application;
- l'exercice d'une plage représentative de conditions de données;
- l'essai des conditions de défaillance (p. ex.: essais négatifs);
- la synchronisation et la séquence d'exécution;
- l'essai des communications à destination et en provenance du SIS;

~~NOTE Dans la mesure du possible, la condition de surcharge des communications peut être vérifiée et soumise à l'essai.~~

- l'intégration du programme d'application hors ligne au matériel de l'unité logique et au PE sous-jacent;
- les contrôles de flux de données internes pour confirmer que l'unité logique ne fonctionne pas qu'en apparence, mais fonctionne comme prévu;
- lorsque cela est faisable, l'intégration du programme d'application et d'appareils tiers.

12.5.4 Le mapping des données d'E/S par rapport au programme d'application (notamment le type et la plage des données) doit être vérifié.

12.5.5 Durant les essais, les modifications apportées au programme d'application doivent faire l'objet d'une analyse d'impact afin de déterminer:

- l'ensemble des parties du programme d'application impactées;
- les activités de reconception et revérification nécessaires.

12.5.6 Les résultats des essais du programme d'application doivent être documentés et inclure:

- les versions du programme d'application ainsi que ses supports documentaires soumis à l'essai;
- les versions des logiciels de support et des outils d'essai;
- le nom de la ou des personnes qui ont effectué les essais et les revues, ainsi que les dates correspondantes;
- les descriptions des essais et des revues effectués, ainsi que les dates correspondantes;
- les résultats d'essai;
- si l'objectif et les critères des essais ont été satisfaits ou non;
- en cas de défaillance pendant l'essai, les raisons de cette dernière, l'analyse de la défaillance et les enregistrements relatifs à sa correction, ainsi que les exigences du nouvel essai.

12.6 Exigences relatives à la méthodologie et aux outils du programme d'application

12.6.1 Le développement du programme d'application doit satisfaire aux contraintes spécifiées dans le ou les manuels de sécurité applicables.

~~NOTE Le/les manuel(s) de sécurité peuvent faire l'objet d'une revue et~~ Lors de la revue du ou des manuels de sécurité, si cela est exigé pour une application spécifique, des procédures et/ou contraintes supplémentaires quant à l'utilisation des méthodologies et des outils peuvent être mises en œuvre.

12.6.2 Les méthodes, les techniques et les outils doivent être choisis et appliqués pour chaque phase de cycle de vie, de manière à:

- minimiser le risque d'introduire des erreurs dans le programme d'application;
- révéler et éliminer les erreurs qui existent déjà dans le programme d'application;
- s'assurer, dans la mesure du possible, que les erreurs persistant dans le programme d'application ne conduiront pas à des résultats inacceptables;
- améliorer les moyens de gestion des modifications du programme d'application pendant toute la vie du SIS;
- fournir la preuve que le programme d'application réunit la qualité exigée.

13 Essai de réception en usine (ERU)

13.1 Objectif

L'Article 13 a pour objet de soumettre à l'essai les appareils du SIS afin de s'assurer qu'ils satisfont aux exigences définies dans la SRS.

NOTE 1 Le fait de soumettre à l'essai l'unité logique, le logiciel et le matériel associés avant de les installer peut faciliter l'identification et la correction des erreurs.

NOTE 2 L'ERU est parfois considéré comme un essai d'intégration et peut faire partie de la validation.

NOTE 3 Il peut être recommandé de soumettre les éléments de terrain à l'essai avec l'unité logique en cas de besoin de niveau élevé de confiance en fonctionnement avant l'installation finale (p. ex.: applications sous-marines).

13.2 Recommandations

13.2.1 La nécessité de procéder à un ERU doit être spécifiée pendant la planification de sécurité d'un projet.

NOTE 1 Une collaboration étroite entre le fournisseur de l'unité logique et le contractant responsable de la conception peut être exigée afin de mettre au point les essais d'intégration.

NOTE 2 Ces activités suivent les phases de conception et de développement et précèdent l'installation et la mise en service.

NOTE 3 Ces activités sont applicables aux sous-systèmes SIS, avec ou sans électronique programmable.

NOTE 4 Il est habituel que l'ERU se déroule dans un environnement industriel avant l'installation et la mise en service à l'usine.

13.2.2 La planification d'un ERU doit spécifier les points suivants:

- Les types d'essais à exécuter, y compris les essais de fonctionnalité du système boîte noire, les essais de performance, les contrôles internes, les essais de fonctionnement, les essais d'environnement, les essais d'interface, les essais en conditions de fonctionnement dégradé ou anormales, les essais d'exceptions, les essais de réaction de sécurité en cas de défaillance du réseau (notamment le redémarrage de l'installation après restauration de l'alimentation) et l'application des manuels de fonctionnement et de maintenance du SIS;

NOTE 1 Les essais de fonctionnalité boîte noire désignent une méthode de conception d'essais qui traite le système comme une "boîte noire", ce qui fait qu'ils n'utilisent pas la connaissance de sa structure interne de manière explicite. La conception des essais boîte noire est habituellement décrite comme se concentrant sur les exigences de fonction d'essai. Des synonymes de boîte noire sont: essais comportementaux, fonctionnels, en boîte opaque et en boîte fermée.

NOTE 2 Les essais de fonctionnement déterminent si le système satisfait aux caractéristiques de synchronisation, de fiabilité et de disponibilité, d'intégrité, ainsi qu'aux objectifs et contraintes de sécurité.

NOTE 3 Les essais environnementaux incluent la CEM, ainsi que les essais de durée de vie et de contrainte.

NOTE 4 Les contrôles de flux de données internes peuvent être réalisés de manière à confirmer ce que le SIS traite les données d'entrée et génère la réponse de sortie comme spécifié.

- les scénarios d'essai, les descriptions des essais et les données d'essai;

NOTE 5 Il peut être très important de dire clairement qui est responsable du développement du scénario d'essai, qui va être responsable de l'exécution de l'essai et qui va être témoin de l'essai.

- la dépendance à l'égard des autres systèmes/interfaces;
- l'environnement d'essai et les outils;
- la configuration de l'unité logique, du capteur et de l'élément terminal;
- les critères d'essai sur lesquels la fin des essais doit être jugée;
- les procédures relatives aux actions correctives lors d'une défaillance pendant l'essai;
- les compétences du personnel d'essai;
- la localisation physique;

- les dangers posés par les essais, notamment ceux ayant trait à l'énergie stockée;
- un schéma clair du montage d'essai;
- l'enregistrement des essais réalisés, des données, des résultats et des observations pendant la réalisation des essais.

NOTE 6 Les essais ne pouvant pas être physiquement effectués sont normalement traités par une ligne de raisonnement formel montrant pourquoi le SIS satisfait à l'exigence, l'objectif ou la contrainte.

13.2.3 L'ERU doit être réalisé sur une version définie de l'unité logique.

13.2.4 L'ERU doit être réalisé selon la planification des ERU. Ces essais doivent montrer que toute la logique s'exécute correctement.

13.2.5 Pour chaque essai effectué, les points suivants doivent être traités:

- la version de la planification d'essai qui a été utilisée;
- la SIF et les caractéristiques de performances soumises à l'essai;
- les procédures d'essai détaillées et les descriptions des essais;
- l'enregistrement chronologique des activités d'essai;
- les outils, les équipements et les interfaces utilisés.

13.2.6 Les résultats des ERU doivent être documentés, en mentionnant:

- les scénarios d'essai;
- les résultats d'essai;
- si les objectifs et les critères d'essai ont été satisfaits ou non.

En cas de défaillance pendant l'essai, les raisons de cette dernière doivent être documentées et analysées et il convient que l'action corrective appropriée soit mise en œuvre.

13.2.7 Pendant les ERU, toute modification ou tout changement doit être soumis à une analyse de sécurité pour déterminer:

- l'étendue de l'impact sur chaque SIF;
- l'étendue de l'essai et de la vérification devant être définis et mis en œuvre.

NOTE En fonction des résultats de l'ERU, la mise en service peut commencer alors que l'action corrective est entreprise.

14 Installation et mise en service du SIS

14.1 Objectifs

Les exigences de l'Article 14 visent à:

- installer le SIS conformément aux spécifications et aux plans;
- mettre en service le SIS de manière à ce qu'il soit prêt pour la validation finale du système.

NOTE Le but de la mise en service est de s'assurer que chacun des appareils SIS est individuellement prêt à fonctionner, tel que spécifié pendant la phase de conception.

14.2 Exigences

14.2.1 La planification de l'installation et de la mise en service doit définir toutes les activités exigées pour l'installation et la mise en service. Elle doit être conforme à la présente norme, en fournissant les informations suivantes:

- les activités d'installation et de mise en service;
- les procédures, les mesures et les techniques devant être utilisées pour l'installation et la mise en service;
- le moment où ces activités doivent avoir lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités.

Le cas échéant, la planification de l'installation et de la mise en service peut être intégrée dans la planification globale du projet.

14.2.2 Tous les appareils du SIS doivent être correctement installés conformément au ou aux plans de conception et d'installation.

14.2.3 Le SIS doit être mis en service en accord avec la planification, en vue de la validation finale du système. Les activités de mise en service doivent inclure, sans s'y limiter, la confirmation des points suivants:

- la mise à la terre (la mise au conducteur de protection) a été correctement raccordée;
- les sources d'énergie ont été correctement connectées et sont opérationnelles;
- les appareils de blocage pour le transport et des matériaux d'emballage ont été retirés;
- aucun dommage physique n'est constaté;
- tous les instruments ont été correctement étalonnés et configurés;
- tous les appareils de terrain sont opérationnels;
- l'unité logique et les entrées/sorties sont opérationnelles;
- les interfaces vers d'autres systèmes et périphériques sont opérationnelles;
- toutes les communications entre les systèmes SIS distants sont opérationnelles.

14.2.4 Des enregistrements appropriés de la mise en service du SIS doivent être créés en mentionnant les résultats des activités et en indiquant si les objectifs et les critères identifiés pendant la phase de conception ont été satisfaits ou non. En cas de défaillance, les raisons de cette dernière doivent être enregistrées.

14.2.5 Dans le cas où il a été établi que l'installation réelle n'est pas conforme aux informations de conception, la différence doit être évaluée par une personne compétente et l'impact de la différence sur la sécurité doit être déterminé. S'il est établi que les différences n'ont aucun impact sur la sécurité, les informations de conception doivent alors être mises à jour suivant l'état "conforme à l'exécution". Si les différences ont un impact négatif sur la sécurité, l'installation doit alors être modifiée pour satisfaire aux exigences de conception.

15 Validation de sécurité du SIS

15.1 Objectif

Les exigences de l'Article 15 ont pour objet de valider, par examen et essais, que le SIS installé et mis en service ainsi que sa ou ses SIF associées satisfont aux exigences indiquées dans la SRS.

NOTE Cela est parfois désigné sous le terme d'essai de réception sur site (ERS).

15.2 Exigences

15.2.1 La planification de la validation du SIS doit être effectuée tout au long du cycle de vie de sécurité du SIS et doit définir l'ensemble des activités et équipements exigés pour la validation. Les points suivants doivent être inclus:

- les activités de validation dont la validation du SIS par rapport à la SRS, y compris la mise en œuvre et la résolution des recommandations qui en découlent;
- la validation de tous les modes de fonctionnement appropriés du processus et de ses équipements associés, notamment:
 - la préparation pour l'utilisation, notamment l'initialisation et le réglage;
 - le fonctionnement au démarrage, en automatique, en manuel, en semi-automatique, en régime établi;
 - la réinitialisation, l'arrêt, la maintenance;
 - les autres modes identifiés lors des phases antérieures du cycle de vie de sécurité du SIS;
- les procédures, les mesures et les techniques devant être utilisées pour la validation, notamment la manière dont les activités de validation peuvent être réalisées, sans exposer l'installation et le processus au risque des événements dangereux contre lesquels le SIS doit les protéger;
- le moment où ces activités doivent avoir lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités, et les niveaux d'indépendance pour les activités de validation;
- la référence aux informations par rapport auxquelles la validation doit être effectuée (p. ex.: diagramme de cause et d'effet);
- les équipements et installations qui ont besoin d'être installés ou mis en disponibilité (p. ex.: les vannes d'isolement et les équipements de détection de fuites qui seront nécessaires pour les essais des vannes).

NOTE Des exemples d'activités de validation incluent les essais en boucle, les essais logiques, les procédures d'étalonnage, la simulation du programme d'application.

15.2.2 La planification de la validation pour le programme d'application doit inclure les points suivants:

- l'identification du programme d'application qui nécessite d'être validé pour chaque mode de fonctionnement du processus avant de commencer la mise en service;
- la stratégie technique vis-à-vis de la validation qui inclut (selon le cas):
 - les techniques manuelles et automatisées;
 - les techniques statiques et dynamiques;
 - les techniques analytiques et statistiques;
- conformément au point ci-dessus, les mesures (techniques) et les procédures qui seront utilisées pour confirmer que chaque SIF est conforme aux exigences de sécurité spécifiées et au SIL spécifié;
- l'environnement exigé dans lequel les activités de validation doivent avoir lieu (p. ex.: pour les essais, cela inclurait des outils et des équipements étalonnés);
- le programme d'application;
- les critères de réussite/d'échec pour réaliser la validation notamment:
 - le processus exigé et les signaux d'entrée de l'opérateur avec leurs séquences et leurs valeurs;
 - les signaux de sortie anticipés avec leurs séquences et leurs valeurs;
 - d'autres critères d'acceptation, par exemple, l'utilisation de la mémoire, la synchronisation et les tolérances de valeur;
- les règles et les procédures concernant l'évaluation des résultats de la validation, en particulier les défaillances;
- tous les documents (voir Article 19) sont validés en termes d'exactitude, de cohérence et de traçabilité de la SIF, de son apparition à l'étape de la H&RA jusqu'à la SIF finale installée.

15.2.3 Dans le cas où la précision de mesure est exigée en tant qu'élément de la validation, il convient que les instruments utilisés pour cette fonction soient étalonnés en référence à une spécification se rapportant à une norme, dans les limites d'une incertitude appropriée à l'application. Si cet étalonnage n'est pas réalisable, une autre méthode doit être utilisée et documentée.

15.2.4 La validation du SIS et de sa ou ses SIF associées doit être effectuée selon la planification de la validation du SIS. Les activités de validation doivent inclure les points suivants, sans toutefois devoir être limitées à ces derniers:

- la confirmation que le SIS fonctionne sous des modes de fonctionnement normaux et anormaux du processus (p. ex.: démarrage, arrêt) tels qu'identifiés dans la SRS;
- la confirmation que l'interaction défavorable du BPCS et d'autres systèmes liés n'affectent pas le fonctionnement correct du SIS;
- le SIS communique correctement (lorsque cela est exigé) avec le BPCS ou avec tout autre système ou réseau, y compris au cours de conditions anormales telles qu'une surcharge de données;
- les capteurs, l'unité logique et les éléments terminaux fonctionnent selon la SRS (tous les canaux redondants inclus), y compris au cours de conditions anormales telles qu'une surcharge de données;

NOTE Si l'unité logique a fait l'objet d'un essai de réception en usine (ERU), comme cela est décrit à l'Article 13, la validation de l'unité logique par l'ERU peut être prise en compte. Une fois l'ensemble des équipements installés au sein de l'installation, la fonctionnalité de l'unité logique ainsi que ses liaisons avec d'autres sous-systèmes SIS seront soumises à l'essai dans le cadre d'une validation en boucle complète.

- la documentation de conception du SIS est cohérente avec le système installé;
- la confirmation que la SIF fonctionne comme cela est spécifié pour des valeurs de variables du processus invalides (p. ex.: hors plage);
- la séquence d'arrêt correcte est activée;
- le SIS donne une annonce et un affichage de fonctionnement appropriés;
- les calculs qui sont inclus dans le SIS sont corrects pour la plage attendue de valeurs, mais également aux limites et au-dessus des limites;
- les fonctions de réinitialisation du SIS fonctionnent comme cela est défini dans la SRS;
- les fonctions de dérivation fonctionnent correctement;
- les neutralisations de démarrage fonctionnent correctement;
- les systèmes d'arrêt manuel fonctionnent correctement;
- la politique d'essais périodiques est documentée dans les procédures de maintenance;
- les fonctions d'alarme de diagnostic fonctionnent comme cela est exigé;
- la confirmation que le SIS se comporte comme exigé lors d'une perte d'alimentation (p. ex.: alimentation électrique, pneumatique ou hydraulique) et la confirmation que le SIS revient à l'état souhaité lorsque l'alimentation est rétablie;
- la confirmation que l'immunité CEM a été obtenue, comme spécifié dans la SRS (voir 10.3).

15.2.5 La validation du programme d'application doit déterminer si:

- toutes les exigences de sécurité du programme d'application spécifiées (voir 10.3.2) sont correctement réalisées;
- le programme d'application ne compromet pas les exigences de sécurité en état d'anomalie du SIS et en conditions de fonctionnement dégradé, ni en état d'anomalie du BPCS pour une ou plusieurs interfaces entre le SIS et le BPCS;
- le programme d'application ne compromet pas les exigences de sécurité en exécutant des fonctionnalités "inutilisées" du logiciel, autrement dit des fonctionnalités non définies dans la spécification.

Les informations des activités de validation doivent être disponibles.

15.2.6 Les résultats des activités du plan de validation doivent représenter et couvrir l'ensemble du processus de validation du SIS. La documentation de validation du SIS doit indiquer:

- la version de la planification de la validation du SIS utilisée;
- la ou les SIF à l'essai (ou en analyse), ainsi que la référence spécifique à l'exigence identifiée lors de la planification de la validation du SIS;
- les outils et les équipements utilisés, avec leurs données d'étalonnage;
- les résultats de chaque essai;
- la version de la spécification d'essai qui a été utilisée;
- les critères d'acceptation des essais réalisés;
- la version du matériel, du ou des programmes d'application, ainsi que des autres logiciels du SIS soumis à l'essai;
- toute divergence constatée entre les résultats attendus et les résultats réels, ainsi que la résolution de cette divergence;
- l'analyse faite et les décisions permettant de déterminer si l'essai est poursuivi ou au contraire générer une demande de changement dans le cas où des divergences apparaissent.

15.2.7 Les résultats doivent être vérifiés par rapport aux résultats attendus. Toutes les divergences doivent être analysées, et les conclusions doivent être disponibles dans le cadre de la documentation de validation. Cela doit inclure l'analyse réalisée, ainsi que les décisions permettant de déterminer si la validation est poursuivie ou au contraire générer une demande de changement et revenir à une étape antérieure du cycle de vie de développement.

15.2.8 Après la validation du SIS et avant que les dangers identifiés ne se produisent, les activités suivantes doivent être effectuées:

- toutes les fonctions de dérivation (p. ex.: unité logique PE et forçages de capteur PE, alarmes désactivées) doivent être revenues à leur position normale;
- toutes les vannes d'isolement du processus doivent être paramétrées selon les exigences et les procédures du processus au démarrage;
- tous les matériaux d'essai (p. ex.: fluides) doivent être éliminés;
- toutes les neutralisations de mise en service, ainsi que les autorisations de forçage doivent être éliminées.

16 Fonctionnement et maintenance du SIS

16.1 Objectifs

Les exigences de l'Article 16 visent à s'assurer que:

- le SIL exigé de chaque SIF est maintenu pendant le fonctionnement et la maintenance;
- le SIS est mis en fonctionnement et entretenu de manière à préserver l'intégrité de sécurité exigée.

16.2 Exigences

16.2.1 Le fonctionnement et la planification de la maintenance du SIS doivent être effectués. Elles doivent traiter les points suivants:

- les activités de fonctionnement périodique et anormal;

- les activités de contrôle, d'essais périodiques, de maintenance préventive et de dépannage;
- les procédures, les mesures et les techniques devant être utilisées pour le fonctionnement et la maintenance;
- la réponse de fonctionnement aux anomalies et défaillances identifiées par les diagnostics, inspections ou essais périodiques;
- la vérification de la conformité aux procédures de fonctionnement et de maintenance;
- le moment où ces activités doivent avoir lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités;
- un plan de maintenance du SIS.

NOTE Le plan de maintenance du SIS peut mentionner différentes fonctions de maintenance selon le niveau SIL.

16.2.2 Les procédures de fonctionnement et de maintenance doivent être développées en accord avec la planification de la sécurité adéquate et doivent fournir les informations suivantes:

- a) les méthodes et procédure habituelles qui doivent être appliquées afin de maintenir la sécurité fonctionnelle du SIS "comme à la conception";
- b) les procédures utilisées pour garantir la qualité et la cohérence des essais périodiques et s'assurer que la validation appropriée a été réalisée suite au remplacement d'un appareil;
- c) les mesures et contraintes nécessaires pour prévenir un état de non-sécurité et/ou réduire les conséquences d'un événement dangereux pendant la maintenance ou le fonctionnement (p. ex.: lorsqu'un système doit être dérivé (shunté) pour les essais ou la maintenance, quelles étapes supplémentaires de réduction du risque doivent être mises en œuvre);
- d) les méthodes et procédures utilisées pour soumettre les diagnostics à l'essai;
- e) les informations qui nécessitent d'être maintenues lors d'une défaillance du SIS et les taux de sollicitation sur le SIS;
- f) les procédures de collecte de données en fonction du taux de sollicitation et des paramètres de fiabilité du SIS;

NOTE 1 La collecte et l'analyse des données de défaillance présentent de nombreux avantages, notamment celui de réduire les coûts de maintenance si les taux de défaillance au fonctionnement sont considérablement inférieurs à ceux qui avaient été prévus lors de la conception. Les coûts de mise en œuvre des nouvelles installations peuvent également être réduits, car les nouvelles conceptions peuvent reposer sur des taux de défaillance moins prudents.

- g) les informations qui nécessitent d'être conservées, montrant les résultats des audits et des essais effectués sur le SIS;
- h) les procédures de maintenance à suivre lorsque des anomalies ou des défaillances ont lieu dans le SIS, incluant:
 - les procédures de diagnostic et de réparation des anomalies;
 - les procédures de revalidation;
 - les exigences relatives au compte rendu de maintenance;
 - les procédures pour suivre l'exécution de maintenance.

NOTE 2 Les considérations incluent:

- les procédures de compte rendu de défaillances;
- les procédures d'analyse de défaillances systématiques;
- les actions permettant un arrêt en toute sécurité en cas de défaillance du BPCS;
- l'étalonnage et l'entretien corrects de l'équipement d'essai.

16.2.3 Les procédures de fonctionnement doivent être mises à disposition. Des mesures compensatoires garantissant une sécurité perpétuelle lorsque le SIS est désactivé ou en condition de fonctionnement dégradé dans le cadre d'une dérivation (réparation ou essai)

doivent être appliquées selon les limites de fonctionnement associées (durée, paramètres du processus, etc.). L'opérateur doit être informé des procédures à appliquer avant et pendant la dérivation, ainsi que de ce qu'il convient de faire avant le retrait de la dérivation et la durée maximale pendant laquelle le système peut demeurer à l'état de dérivation. Ces informations doivent être revues régulièrement.

NOTE Les procédures de fonctionnement et de maintenance peuvent inclure une vérification du retrait des dérivation après les essais périodiques.

16.2.4 Le fonctionnement continu d'un processus en présence d'un appareil SIS en dérivation doit uniquement être permis si une analyse des dangers a conclu que des mesures compensatoires sont en place et qu'elles assurent une réduction de risque appropriée. Les procédures de fonctionnement doivent être développées en conséquence.

16.2.5 Le fonctionnement et la maintenance doivent être mis en œuvre conformément aux procédures s'y référant.

16.2.6 Les opérateurs doivent être formés à la fonction et au fonctionnement du SIS, et dans leur domaine de compétence. Cette formation doit assurer qu'ils comprennent:

- le fonctionnement du SIS (les points de déclenchement et l'action résultante qui est prise par le SIS);

NOTE 1 Cela peut également inclure l'impact d'une action SIS sur le reste de l'installation de fonctionnement.

- le danger contre lequel le SIS assure une protection;
- le fonctionnement correct et la gestion de tous les commutateurs de dérivation/neutralisation et dans quelles circonstances ces dérivation doivent être utilisées;
- le fonctionnement de tous les commutateurs d'arrêt manuel, des activités de démarrage manuel et dans quelles circonstances ces commutateurs manuels doivent être activés;

NOTE 2 Cela peut inclure la "réinitialisation du système" et le "redémarrage du système".

- la conduite à tenir lors de l'activation d'une alarme de diagnostic (p. ex.: quelle action doit être prise lorsqu'une alarme du SIS est activée, indiquant qu'il y a un problème avec le SIS);
- la vérification adéquate des diagnostics.

16.2.7 L'état de toutes les dérivation doit être consigné dans un journal de dérivation. Toutes les dérivation nécessitent une autorisation et une indication.

16.2.8 Le personnel de maintenance doit être formé comme exigé pour entretenir les performances fonctionnelles globales du SIS (matériel et logiciel) afin de satisfaire au SIL objectif de chaque SIF.

16.2.9 Les divergences entre le comportement attendu et le comportement réel du SIS doivent être analysées et, en cas de besoin, des modifications doivent être faites de telle manière que la sécurité exigée soit maintenue. Cela doit inclure la surveillance des points suivants:

- le taux de sollicitation relatif à chaque SIF (voir 5.2.5.3);
- les actions prises après une sollicitation sur le système;
- les défaillances et modes de défaillance des équipements faisant partie du SIS, notamment ceux identifiés au cours du fonctionnement normal, de l'inspection, de l'essai ou de la sollicitation d'une SIF;
- la cause des sollicitations;
- la cause et la fréquence des déclenchements parasites;
- la défaillance de l'équipement faisant partie des mesures compensatoires.

16.2.10 Les procédures de fonctionnement et de maintenance peuvent exiger une révision, si besoin, en suivant:

- des audits de la sécurité fonctionnelle;
- les essais sur le SIS;
- l'expérience à partir d'événements de fonctionnement et de maintenance normaux ou anormaux.

16.2.11 Des procédures d'essais périodiques écrites doivent être développées pour chaque SIF, afin de révéler des défaillances dangereuses non détectées par les diagnostics. Ces procédures d'essai écrites doivent décrire chaque étape qui doit être exécutée, et doivent inclure:

- le fonctionnement correct de chaque capteur et élément terminal;
- l'action logique correcte;
- les alarmes et indications correctes.

NOTE Les méthodes suivantes peuvent être utilisées pour déterminer les défaillances non détectées devant être soumises à l'essai:

- examen des arbres de défaillances;
- analyse des modes de défaillance et de leurs effets;
- maintenance basée sur la fiabilité.

16.2.12 Les pièces de rechange du SIS doivent être identifiées et doivent être rendues disponibles afin de réduire la durée de la dérivation consécutivement à une indisponibilité des pièces de rechange du SIS.

NOTE Les remplacements autres que les remplacements en nature (c'est-à-dire sur une base comparable) peuvent être gérés comme s'il s'agissait d'une modification du SIS.

16.2.13 Les personnes chargées du fonctionnement et de la maintenance doivent passer en revue l'analyse de danger et de risque, ainsi que les processus d'allocation et de conception pour s'assurer que les hypothèses faites sont valides (p. ex.: hypothèses concernant l'occupation et la protection contre la corrosion).

16.3 Essais périodiques et inspection

16.3.1 Essais périodiques

16.3.1.1 Les essais périodiques doivent être réalisés en utilisant une procédure écrite afin de révéler les pannes non détectées qui empêchent le SIS de fonctionner selon la SRS.

NOTE 1 Une attention particulière peut être accordée à l'identification des causes de défaillances pouvant conduire à des défaillances de cause commune.

NOTE 2 Les procédures d'essai fonctionnel peuvent également souligner la nécessité d'éviter l'apparition de défaillances de cause commune.

16.3.1.2 Le SIS dans son ensemble doit être soumis à l'essai, y compris le ou les capteurs, unités logiques et éléments terminaux (p. ex.: vannes d'arrêt et moteurs).

NOTE Les essais du SIS peuvent être réalisés dans sa globalité ou par segments (voir 11.8.1).

16.3.1.3 Le programme des essais périodiques doit être en conformité avec la SRS. La fréquence des essais périodiques d'une SIF doit être déterminée par le biais d'un calcul de la PFD_{avg} ou de la PFH selon 11.9 pour le SIS tel qu'installé dans l'environnement de fonctionnement.

NOTE Les différentes parties du SIS peuvent exiger différents intervalles d'essai. Par exemple, l'unité logique peut exiger un intervalle d'essai différent de celui des capteurs ou des éléments terminaux.

16.3.1.4 Toutes les insuffisances trouvées pendant les essais périodiques doivent être réparées d'une façon sûre et rapide. Un essai périodique doit être répété à l'issue de la réparation.

16.3.1.5 Périodiquement (intervalle déterminé par l'utilisateur), la fréquence de l'essai doit être réévaluée sur la base de divers facteurs incluant les données d'essai antérieures, l'expérience en usine et la dégradation du matériel.

NOTE L'utilisateur peut ajuster la fréquence d'essai en fonction de ces données et d'une analyse de la base d'origine pour la fréquence d'essai.

16.3.1.6 Tout changement apporté au programme d'application exige une validation complète, ainsi qu'un essai périodique de toutes les SIF impactées par le changement. Des exceptions sont permises si une revue appropriée et des essais partiels portant sur les changements sont effectués pour s'assurer que les changements ont été conçus selon les exigences de sécurité et ont été correctement mis en œuvre.

16.3.1.7 Des procédures de gestion adéquates doivent être appliquées afin de passer en revue les reports et d'empêcher la survenue de retards importants dans les essais périodiques.

16.3.2 Inspection

Chaque SIS doit faire l'objet d'un examen visuel régulier pour s'assurer de l'absence de modification non autorisée et de détérioration observable (p. ex.: boulons ou capots d'instrument manquants, ferrures rouillées, fils ouverts, conduits cassés, réchauffage des conduites cassé et isolation manquante).

NOTE Ces problèmes pourraient indiquer une augmentation de la fréquence des anomalies.

16.3.3 Documentation des essais périodiques et de l'inspection

L'utilisateur doit conserver les enregistrements qui certifient que les essais périodiques et les inspections ont été réalisés comme cela est exigé. Ces enregistrements doivent inclure, au minimum, les informations suivantes:

- la description des essais et inspections réalisés, notamment l'identification de la procédure d'essai utilisée;
- les dates des essais et des inspections;
- le nom de la (des) personne(s) qui a (ont) effectué les essais et les inspections;
- le numéro de série ou tout autre identifiant unique du système soumis à un essai (p. ex.: numéro de ligne, numéro d'étiquette, numéro d'équipement et numéro de SIF);
- les résultats des essais et inspections, notamment l'état "tel que mesuré", toutes les anomalies trouvées (y compris le mode de défaillance) et l'état "tel qu'étalonné".

17 Modification du SIS

17.1 Objectifs

Les exigences de l'Article 17 visent à:

- assurer que les modifications apportées à un SIS sont correctement planifiées, revues, approuvées et documentées avant de procéder au changement;
- assurer que le niveau d'intégrité de sécurité exigé du SIS est maintenu malgré les changements apportés au SIS.

NOTE Les modifications apportées au BPCS, à d'autres équipements, au processus ou aux conditions de fonctionnement peuvent faire l'objet d'une revue afin de déterminer si elles seront susceptibles d'affecter la nature ou la fréquence des sollicitations vis-à-vis du SIS. Celles ayant un impact néfaste peuvent être considérées ultérieurement afin de déterminer si le niveau de la réduction de risque sera toujours suffisant.

17.2 Exigences

17.2.1 Avant d'apporter des modifications à un SIS, les procédures d'autorisation et de contrôle des changements doivent être en place.

17.2.2 Les procédures doivent inclure une méthode claire pour identifier et demander le travail devant être réalisé, ainsi que les dangers qui peuvent être affectés.

17.2.3 Avant d'apporter des modifications à un SIS (y compris le programme d'application), une analyse doit être effectuée pour déterminer l'impact sur la sécurité fonctionnelle du fait de la modification proposée. Lorsque l'analyse montre que la modification proposée pourrait avoir une incidence sur la sécurité, il doit y avoir un retour à la première phase du cycle de vie de sécurité du SIS affectée par la modification.

17.2.4 La planification de la sécurité relative à la modification et à la nouvelle vérification doit être disponible. Les modifications et les nouvelles vérifications doivent être effectuées conformément à la planification.

17.2.5 Toute la documentation affectée par la modification doit être mise à jour.

17.2.6 L'activité de modification ne doit pas commencer tant qu'une FSA n'a pas été réalisée selon 5.2.6.1.9 et après une autorisation adéquate.

17.2.7 Les informations adéquates doivent être gérées pour l'ensemble des changements apportés au SIS. Les informations doivent comprendre:

- une description de la modification ou du changement;
- la raison du changement;
- les dangers identifiés et les SIF pouvant être affectés;
- une analyse de l'impact de l'activité de modification sur le SIS;
- toutes les approbations exigées pour les changements;
- les essais utilisés pour vérifier que le changement a été correctement mis en œuvre et que le SIS fonctionne comme cela est exigé;
- les détails de toutes les activités de modification du SIS (p. ex.: journal des modifications);
- l'historique de configuration adéquat;
- les essais utilisés pour vérifier que le changement n'a pas entraîné d'effet néfaste sur des parties du SIS qui n'ont pas été modifiées.

17.2.8 La modification doit être effectuée avec du personnel qualifié, qui a été correctement formé. Il convient de notifier à tout le personnel concerné et adéquat la nature du changement et de le former à ce changement.

18 Déclassement du SIS

18.1 Objectifs

Les exigences de l'Article 18 visent à s'assurer:

- qu'une revue adéquate est réalisée avant le déclassement du service actif d'un SIS et que l'autorisation exigée est obtenue;
- que la ou les SIF exigées demeurent opérationnelles pendant les activités de déclassement.

18.2 Exigences

18.2.1 Avant d'effectuer un déclassement de tout ou partie d'un SIS ou d'une SIF, les procédures d'autorisation et de contrôle des changements doivent être en place.

18.2.2 Les procédures doivent inclure une méthode claire pour identifier et demander le travail devant être réalisé, ainsi que pour identifier les dangers qui peuvent être affectés.

18.2.3 Une analyse doit être effectuée pour déterminer l'impact sur la sécurité fonctionnelle, du fait de l'activité de déclassement proposée. L'évaluation doit inclure une mise à jour de la H&RA, suffisante pour déterminer l'étendue de l'impact sur le cycle de vie de sécurité du SIS. Les phases ultérieures du cycle de vie de sécurité du SIS doivent avoir besoin d'être réévaluées. L'évaluation doit également tenir compte de:

- la sécurité fonctionnelle pendant l'exécution des activités de déclassement;
- l'impact du déclassement du SIS sur les unités de fonctionnement et les services d'une installation adjacents.

18.2.4 Les résultats de l'analyse d'impact doivent être utilisés lors de la planification de la sécurité, pour remettre en œuvre les exigences appropriées de la série IEC 61511, y compris la revérification et la revalidation.

18.2.5 Les activités de déclassement ne doivent pas commencer sans une documentation, ni une autorisation adéquates.

19 Exigences relatives aux informations et à la documentation

19.1 Objectifs

Les exigences de l'Article 19 ont pour objet de s'assurer que les informations nécessaires sont disponibles et documentées afin que:

- toutes les phases du cycle de vie de sécurité du SIS puissent être réalisées de manière efficace;
- les activités de vérification, de validation et de FSA puissent être réalisées de manière efficace.

19.2 Exigences

19.2.1 La documentation exigée par la série IEC 61511 doit être mise à disposition du personnel chargé de la mise en œuvre des exigences de la série IEC 61511.

19.2.2 La documentation doit:

- décrire l'installation, le système ou les équipements, ainsi que leur utilisation;
- être précise et à jour;
- être facile à comprendre;
- répondre à l'objectif pour lequel elle est prévue;
- être disponible dans un format accessible, gérable et éditable de manière à ce que les documents adéquats et pertinents puissent être identifiés, localisés, récupérés et révisés de manière aisée et rapide.

NOTE D'autres détails des exigences concernant les informations sont inclus à l'Article 14 et à l'Article 15.

19.2.3 La documentation doit avoir des identités uniques, car toute personne doit pouvoir se référer aux différentes parties.

19.2.4 La documentation doit avoir des désignations indiquant le type d'informations.

19.2.5 La documentation doit être traçable par rapport aux exigences fonctionnelles et d'intégrité découlant de la présente norme, y compris l'analyse de danger et de risque.

19.2.6 La documentation doit avoir un index de révision (p. ex.: numéros de version) pour permettre l'identification des différentes versions des informations.

19.2.7 La documentation doit être structurée pour permettre de rechercher les informations voulues. La dernière révision (version) d'un document doit pouvoir être identifiée.

NOTE La structure physique de la documentation peut changer en fonction d'un certain nombre de facteurs, tels que la taille du système, sa complexité et les exigences d'organisation.

19.2.8 Toute documentation pertinente doit être mise à jour, modifiée, revue, approuvée et doit être placée sous la maîtrise d'un système de contrôle des informations approprié.

19.2.9 La documentation courante concernant les sujets suivants doit être maintenue:

- a) les résultats de la H&RA et les hypothèses associées;
- b) les équipements utilisés pour les SIF, ainsi que leurs exigences de sécurité;
- c) l'organisation responsable du maintien de la sécurité fonctionnelle;
- d) les procédures nécessaires pour obtenir et maintenir la sécurité fonctionnelle du SIS;
- e) les informations de modification, comme cela est défini en 17.2.5;
- f) le ou les manuels de sécurité;
- g) la conception, la mise en œuvre, les essais et la validation.

NOTE D'autres détails des exigences concernant les informations sont inclus en 12.4.2, à l'Article 14, à l'Article 15 et en 16.3.3.

Bibliographie

IEC 60050 (toutes les parties), *Vocabulaire Electrotechnique International* (disponible à l'adresse <<http://www.electropedia.org/>>)

ISO/IEC Guide 51:2014, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

IEC 60300-3-2:2004, *Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

IEC 60605-4:2001, *Essai de fiabilité des équipements – Partie 4: Méthodes statistiques de distribution exponentielle – Estimateurs ponctuels, intervalles de confiance, intervalles de prédiction et intervalles de tolérance*

IEC 60617-12:1997, *Symboles graphiques pour schémas – Partie 12: Opérateurs logiques binaires*¹

IEC TS 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena* (disponible en anglais seulement)

IEC 61025, *Analyse par arbre de panne (AAP)*

IEC 61131-3:2013, *Automates programmables – Partie 3: Langages de programmation*

IEC 61131-6:2012, *Automates programmables – Partie 6: Sécurité fonctionnelle*

IEC 61506:1997, *Mesure et commande dans les processus industriels – Documentation des logiciels d'application*

IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définition et abréviations*

IEC 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de l'IEC 61508-2 et de l'IEC 61508-3*

IEC 61511-2:2016, *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 61511-3:2016, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

IEC 61784-3:2010, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils*

IEC 62443-2-1:2010, *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles*

¹ Retirée.

IEC 62682:2014, *Gestion de systèmes d'alarme dans les industries de transformation*

ISO/IEC 2382:2006, *Technologies de l'information – Vocabulaire*

ISO/IEC 27001:2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*

ISO/IEC 90003:2014, *Ingénierie du logiciel – Partie 3: Lignes directrices pour l'application de l'ISO 9001:2000 aux logiciels informatiques*

ISO 2382-1:1993, *Technologies de l'information – Vocabulaire – Partie 1: Termes fondamentaux*

ISO 9000:2005, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

ISO 9001:2008, *Systèmes de management de la qualité – Exigences*

ISO TR 12489:2013, *Pétrole, pétrochimie et gaz naturel – Modélisation et calcul fiabilistes des systèmes de sécurité*

ISO 13849-1:2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*

ISO 14224:2006, *Industries du pétrole, de la pétrochimie et du gaz naturel – Recueil et échange de données de fiabilité et de maintenance des équipements*

ISA TR84.00.04 Part 1:2015, *Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)* (disponible en anglais seulement)

ISA TR84.00.09:2013, *Security Countermeasures Related to Safety Instrumented Systems (SIS)* (disponible en anglais seulement)

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016+AMD1:2017 CSV

FINAL VERSION

VERSION FINALE

Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and application programming requirements

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

CONTENTS

FOREWORD	5
INTRODUCTION	7
1 Scope	9
2 Normative references	12
3 Terms, definitions and abbreviations	13
3.1 Terms	13
3.2 Terms and definitions	13
3.3 Abbreviations	31
4 Conformance to the IEC 61511-1:2016	32
5 Management of functional safety	32
5.1 Objective	32
5.2 Requirements	33
5.2.1 General	33
5.2.2 Organization and resources	33
5.2.3 Risk evaluation and risk management	33
5.2.4 Safety planning	33
5.2.5 Implementing and monitoring	34
5.2.6 Assessment, auditing and revisions	34
5.2.7 SIS configuration management	37
6 Safety life-cycle requirements	37
6.1 Objectives	37
6.2 Requirements	38
6.3 Application program SIS safety life-cycle requirements	40
7 Verification	43
7.1 Objective	43
7.2 Requirements	43
8 Process H&RA	45
8.1 Objectives	45
8.2 Requirements	45
9 Allocation of safety functions to protection layers	46
9.1 Objectives	46
9.2 Requirements of the allocation process	46
9.3 Requirements on the basic process control system as a protection layer	49
9.4 Requirements for preventing common cause, common mode and dependent failures	50
10 SIS safety requirements specification (SRS)	50
10.1 Objective	50
10.2 General requirements	50
10.3 SIS safety requirements	51
11 SIS design and engineering	53
11.1 Objective	53
11.2 General requirements	53
11.3 Requirements for system behaviour on detection of a fault	54
11.4 Hardware fault tolerance	55
11.5 Requirements for selection of devices	56

11.5.1	Objectives	56
11.5.2	General requirements	56
11.5.3	Requirements for the selection of devices based on prior use	56
11.5.4	Requirements for selection of FPL programmable devices (e.g., field devices) based on prior use	57
11.5.5	Requirements for selection of LVL programmable devices based on prior use	58
11.5.6	Requirements for selection of FVL programmable devices	59
11.6	Field devices	59
11.7	Interfaces	59
11.7.1	General	59
11.7.2	Operator interface requirements	59
11.7.3	Maintenance/engineering interface requirements	60
11.7.4	Communication interface requirements	60
11.8	Maintenance or testing design requirements	61
11.9	Quantification of random failure	61
12	SIS application program development	63
12.1	Objective	63
12.2	General requirements	63
12.3	Application program design	64
12.4	Application program implementation	65
12.5	Requirements for application program verification (review and testing)	66
12.6	Requirements for application program methodology and tools	67
13	Factory acceptance test (FAT)	68
13.1	Objective	68
13.2	Recommendations	68
14	SIS installation and commissioning	69
14.1	Objectives	69
14.2	Requirements	69
15	SIS safety validation	70
15.1	Objective	70
15.2	Requirements	70
16	SIS operation and maintenance	73
16.1	Objectives	73
16.2	Requirements	73
16.3	Proof testing and inspection	75
16.3.1	Proof testing	75
16.3.2	Inspection	76
16.3.3	Documentation of proof tests and inspection	76
17	SIS modification	76
17.1	Objectives	76
17.2	Requirements	77
18	SIS decommissioning	77
18.1	Objectives	77
18.2	Requirements	78
19	Information and documentation requirements	78
19.1	Objectives	78
19.2	Requirements	78

Bibliography	80
Figure 1 – Overall framework of the IEC 61511 series	8
Figure 2 – Relationship between IEC 61511 and IEC 61508	10
Figure 3 – Detailed relationship between IEC 61511 and IEC 61508	11
Figure 4 – Relationship between safety instrumented functions and other functions	12
Figure 5 – Programmable electronic system (PES): structure and terminology	24
Figure 6 – Example of SIS architectures comprising three SIS subsystems	26
Figure 7 – SIS safety life-cycle phases and FSA stages	38
Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle	41
Figure 9 – Typical protection layers and risk reduction means	49
Table 1 – Abbreviations used in IEC 61511	31
Table 2 – SIS safety life-cycle overview (1 of 2)	39
Table 3 – Application program safety life-cycle: overview (1 of 2)	42
Table 4 – Safety integrity requirements: PFD_{avg}	47
Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF	47
Table 6 – Minimum HFT requirements according to SIL	55

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016+AMD1:2017 CSV

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: Framework, definitions, system, hardware and application programming requirements

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.

DISCLAIMER

This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 61511-1 bears the edition number 2.1. It consists of the second edition (2016-02) [documents 65A/777/FDIS and 65A/784/RVD], its corrigendum 1 (2016-09) and its amendment 1 (2017-08) [documents 65A/844/FDIS and 65A/848/RVD]. The technical content is identical to the base edition and its amendment.

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition constitutes a technical revision and includes the following significant technical changes with respect to the previous edition:

- references and requirements to software replaced with references and requirements to application programming;
- functional safety assessment requirements provided with more detail to improve management of functional safety.
- management of change requirement added;
- security risk assessment requirements added;.
- requirements expanded on the basic process control system as a protection layer;
- requirements for hardware fault tolerance modified and should be reviewed carefully to understand user/integrator options.

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

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 the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site 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.

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 and performance levels.

The IEC 61511 series addresses the application of SISs for the process industries. The IEC 61511 series also addresses a process Hazard and Risk Assessment (H&RA) to be carried out to enable the specification for SISs to be derived. Other safety systems' contributions are only considered with respect to the performance requirements for the SIS. The SIS includes all devices necessary to carry out each SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application: SIS safety life-cycle and safety integrity levels (SILs).

The IEC 61511 series addresses SISs which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of the IEC 61511 series should be applied to ensure the functional safety requirements are met. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. 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 principles. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. However in some instances this is not possible or not practical. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, and programmable electronic). To facilitate this approach, the IEC 61511 series:

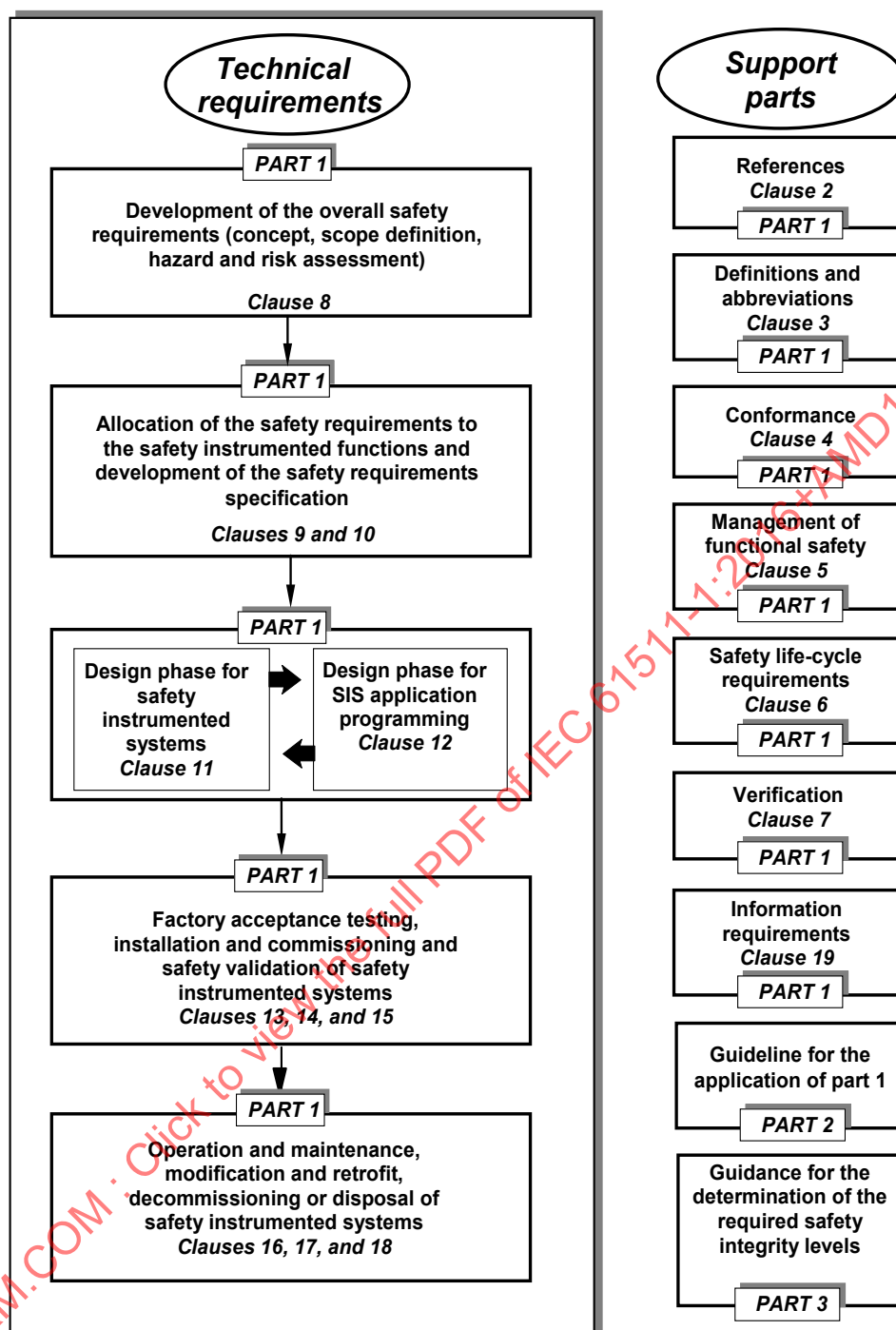
- addresses that a H&RA is carried out to identify the overall safety requirements;
- addresses that an allocation of the safety requirements to the SIS is carried out;
- works within a framework which is applicable to all instrumented means of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

The IEC 61511 series on SIS for the process industry:

- addresses all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (e.g., of underlying principles, terminology, and information) within the process industries. This should have both safety and economic benefits. Figure 1 below shows an overall framework of the IEC 61511 series.

In jurisdictions where the governing authorities (e.g., national, federal, state, province, county, city) have established process safety design, process safety management, or other regulations, these take precedence over the requirements defined in the IEC 61511 series.



IEC

Figure 1 – Overall framework of the IEC 61511 series

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

Part 1: Framework, definitions, system, hardware and application programming requirements

1 Scope

This part of IEC 61511 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to achieve or maintain a safe state of the process. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010.

In particular, IEC 61511-1:

- a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (e.g., designers, suppliers, owner/operating company, contractor). This responsibility will be assigned to different parties according to safety planning, project planning and management, and national regulations;
- b) applies when devices that meets the requirements of the IEC 61508 series published in 2010, or IEC 61511-1:2016 [11.5], is integrated into an overall system that is to be used for a process sector application. It does not apply to manufacturers wishing to claim that devices are suitable for use in SISs for the process sector (see IEC 61508-2:2010 and IEC 61508-3:2010);
- c) defines the relationship between IEC 61511 and IEC 61508 (see Figures 2 and 3);
- d) applies when application programs are developed for systems having limited variability language or when using fixed programming language devices, but does not apply to manufacturers, SIS designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3:2010);
- e) applies to a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation;

NOTE 1 Within the process sector some applications may have additional requirements that have to be satisfied.
- f) outlines the relationship between SIFs and other instrumented functions (see Figure 4);
- g) results in the identification of the functional requirements and safety integrity requirements for the SIF taking into account the risk reduction achieved by other methods;
- h) specifies life-cycle requirements for system architecture and hardware configuration, application programming, and system integration;
- i) specifies requirements for application programming for users and integrators of SISs.
- j) applies when functional safety is achieved using one or more SIFs for the protection of personnel, protection of the general public or protection of the environment;
- k) may be applied in non-safety applications for example asset protection;
- l) defines requirements for implementing SIFs as a part of the overall arrangements for achieving functional safety;
- m) uses a SIS safety life-cycle (see Figure 7) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the SIS;

- n) specifies that a H&RA is to be carried out to define the safety functional requirements and safety integrity levels (SIL) of each SIF;

NOTE 2 Figure 9 presents an overview of risk reduction means.

- o) establishes numerical targets for average probability of failure on demand (in demand mode) and average frequency of dangerous failures (in demand mode or continuous mode) for each SIL;
- p) specifies minimum requirements for hardware fault tolerance (HFT);
- q) specifies measures and techniques required for achieving the specified SIL;
- r) defines a maximum level of functional safety performance (SIL 4) which can be achieved for a SIF implemented according to IEC 61511-1;
- s) defines a minimum level of functional safety performance (SIL 1) below which IEC 61511-1 does not apply;
- t) provides a framework for establishing the SIL but does not specify the SIL required for specific applications (which should be established based on knowledge of the particular application and on the overall targeted risk reduction);
- u) specifies requirements for all parts of the SIS from sensor to final element(s);
- v) defines the information that is needed during the SIS safety life-cycle;
- w) specifies that the design of the SIS takes into account human factors;
- x) does not place any direct requirements on the individual operator or maintenance person:

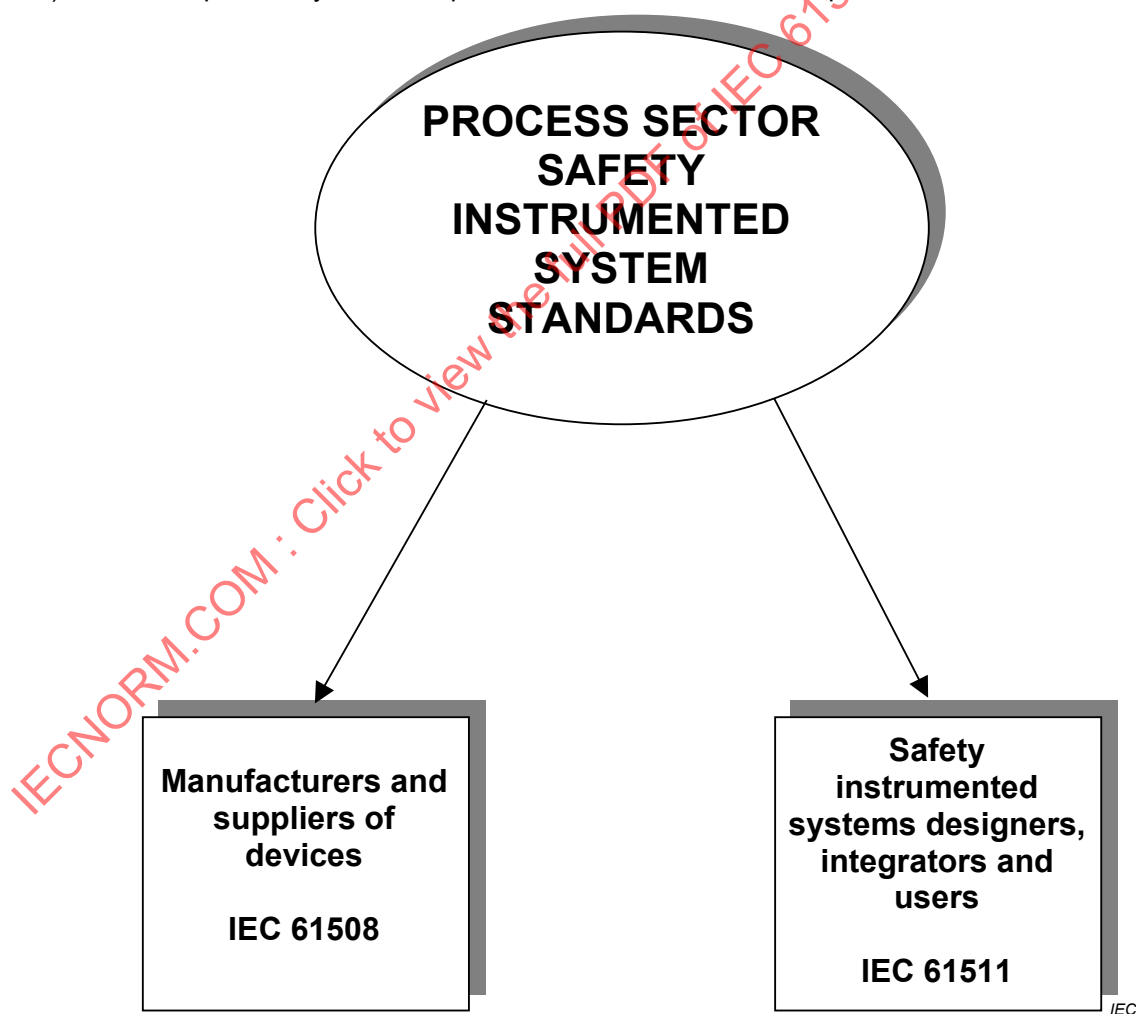


Figure 2 – Relationship between IEC 61511 and IEC 61508

NOTE 3 IEC 61508 is also used by safety instrumented designers, integrators and users where directed in IEC 61511.

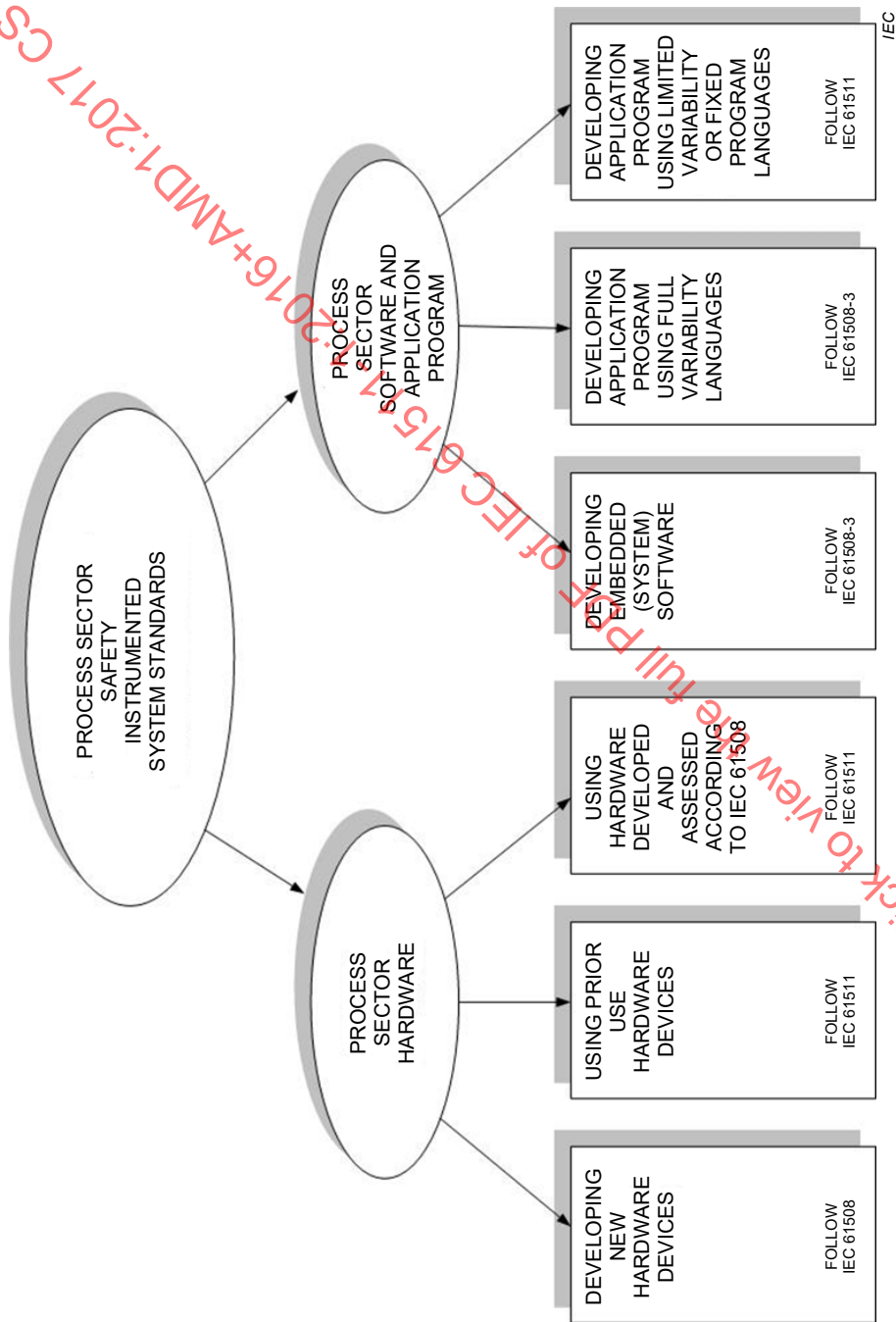
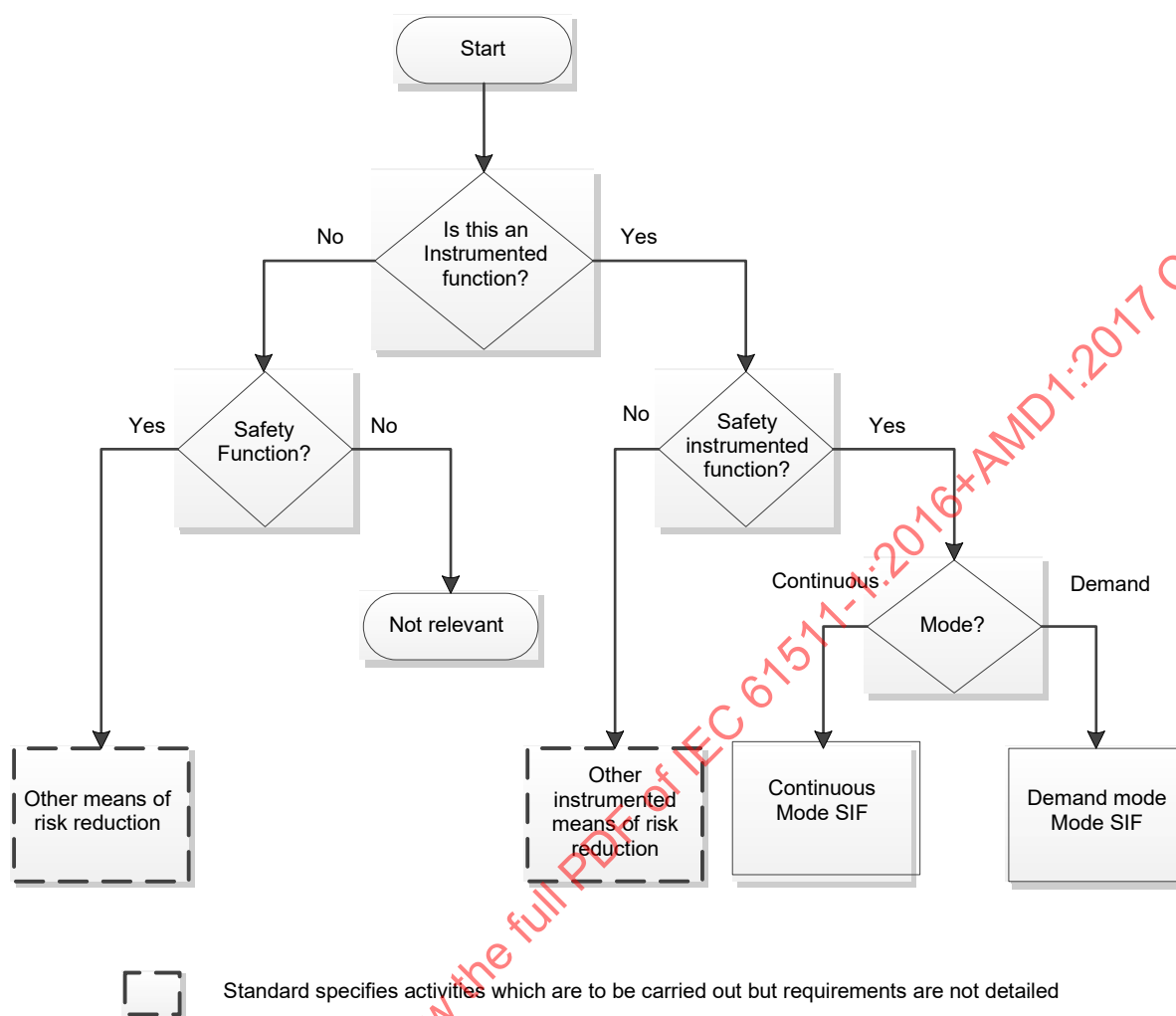


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

NOTE 4 Subclause 7.2.2 in IEC 61511-1:2016 and A.7.2.2 in IEC 61511-2:2016 contain guidance on handling integration of sub-systems that comply with other standards (such as machinery , burner, etc.).



IEC

Figure 4 – Relationship between safety instrumented functions and other functions

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 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General Requirements*

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*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

3 Terms, definitions and abbreviations

3.1 Terms

Terms are listed alphabetically in 3.2.

3.2 Terms and definitions

For the purposes of this document, the following definitions apply.

In some cases these definitions differ from the definitions of the same terms in IEC 61508-4:2010. In some cases this is due to the terminology used in the process sector. In other cases these definitions have been aligned with other relevant definitive references (e.g., IEC 60050 the International Electrotechnical Vocabulary, ISO/IEC Guide 51:2013). However, unless otherwise stated, there is no difference in the technical meaning between these definitions and the definitions of the same terms in IEC 61508-4:2010.

3.2.1

architecture configuration

specific configuration of hardware and software components in a system

Note 1 to entry: In the IEC 61511 series this can mean, for example, arrangement of SIS subsystems, the internal structure of a SIS subsystem or the internal structure of SIS application programs.

3.2.2

asset protection

function allocated to a system and designed for the purpose of preventing loss or damage to assets

3.2.3

basic process control system BPCS

system which responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any SIF

Note 1 to entry: A BPCS includes all of the devices necessary to ensure that the process operates in the desired manner.

Note 2 to entry: A BPCS typically may implement various functions such as process control functions, monitoring, and alarms.

3.2.4

bypass

action or facility to prevent all or parts of the SIS functionality from being executed

Note 1 to entry: Examples of bypassing include:

- the input signal is blocked from the trip logic while still presenting the input parameters and alarm to the operator;
- the output signal from the trip logic to a final element is held in the normal state preventing final element operation;
- a physical bypass line is provided around the final element;
- preselected input state (e.g., on/off input) or set is forced by means of an engineering tool (e.g., in the application program).

Note 2 to entry: Other terms are also used to refer to bypassing, such as override, defeat, disable, force, or inhibit or muting.

3.2.5

channel

device or group of devices that independently perform(s) a specified function

Note 1 to entry: The devices within a channel could include input/output (I/O) devices, logic solvers, sensors, and final elements.

Note 2 to entry: A dual channel (i.e., a two-channel) configuration is one with two channels that independently perform the same function. Channels may be identical or diverse.

Note 3 to entry: The term can be used to describe a complete system or a portion of a system (e.g., sensors or final elements).

Note 4 to entry: Channel describes SIS hardware architectural features often used to meet hardware fault tolerance requirements.

3.2.6 common cause

3.2.6.1

common cause failures, pl

concurrent failures of different devices, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: All the failures due to a common cause do not necessarily occur exactly at the same time and this may allow time to detect the occurrence of the common cause before a SIF is actually failed.

Note 2 to entry: Common cause failures can also lead to common mode failures.

Note 3 to entry: The potential for common cause failures reduces the effect of system redundancy or fault tolerance (e.g., increases the probability of failure of two or more channels in a multiple channel system).

Note 4 to entry: Common cause failures are dependent failures. They may be due to external events (e.g., temperature, humidity, overvoltage, fire, and corrosion), systematic fault (e.g., design, assembly or installation errors, bugs), human error (e.g., misuse), etc.

Note 5 to entry: By extension, a common cause failure (in singular form) is a failure belonging to a set of concurrent failures (plural form) according to 3.2.6.1 definition.

3.2.6.2

common mode failures, pl

concurrent failures of different devices characterized by the same failure mode (i.e., identical faults)

Note 1 to entry: Common mode failures may have different causes.

Note 2 to entry: Common mode failures can also be the result of common cause failures (3.2.6.1).

Note 3 to entry: The potential for common mode failures reduces the effectiveness of system redundancy and fault tolerance (e.g., failure of two or more channels in the same way, causing the same erroneous result).

Note 4 to entry: By extension, a common mode failure (in singular form) is a failure belonging to a set of concurrent failures (plural form) according to 3.2.6.2 definition.

3.2.7

compensating measure

temporary implementation of planned and documented methods for managing risks during any period of maintenance or process operation when it is known that the performance of the SIS is degraded

3.2.8

component

one of the parts of a system, SIS subsystem, or device performing a specified function

Note 1 to entry: Component may also include software.

3.2.9 configuration management

discipline of identifying the components and the arrangements of those components of an evolving system for the purposes of controlling changes to those components, and maintaining continuity of the system and traceability of any changes throughout the life-cycle

3.2.9.1 conservative approach cautious way of doing analysis and calculations

Note 1 to entry: In the safety field, each time an analysis, assumptions, or calculation has to be done (about models, input data, computations, etc.) it can be chosen in order to be sure to produce pessimistic results.

3.2.10 control system

system which responds to input signals from the process and/or from an operator and generates output signals causing the process to operate in the desired manner

Note 1 to entry: The control system includes sensors and final elements and may be either a BPCS or a SIS or a combination of the two.

3.2.11 dangerous failure failure which impedes or disables a given safety action

Note 1 to entry: A failure is "dangerous" only with regard to a given SIF.

Note 2 to entry: When fault tolerance is implemented, a dangerous failure can lead to either:

- a degraded SIF where the safety action is available but there is either a higher PFD or a PFH, or
- a disabled SIF where the safety action is completely disabled or the hazardous event has been induced.

Note 3 to entry: When no fault tolerance is implemented, all dangerous failures lead to a disabled SIF.

3.2.12 dependent failure

failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it

Note 1 to entry: Two events A and B are dependent if the probability of occurrence of A and B, $P(A \text{ and } B)$, is greater than $P(A) \times P(B)$.

Note 2 to entry: See 9.4.2 and IEC 61511-3:2016, Annex J for consideration of dependent failures between protection layers.

Note 3 to entry: Dependent failures include common cause.

3.2.13 detected revealed overt

relating to hardware and software failures or faults which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods

Note 1 to entry: There are some differences in the use of these terms:

- Overt is used for failures or faults which announce themselves when they occur (e.g., due to the change of state). The repair of such failures can begin as soon as they have occurred.
- Detected is used for failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, operator intervention like physical inspection and manual tests). The repair of such failures can begin only after they have been revealed. See Note 2 for the specific use of this term in IEC 61511.
- Revealed is used for failures or faults that become evident due to being overt or as a result of being detected.

Note 2 to entry: In IEC 61511 and except when the context suggests another meaning, the term *dangerous detected failures/faults* is related to dangerous failures detected by diagnostic tests.

Note 3 to entry: When the detection is very fast (e.g., by diagnostic tests) then the detected failures or faults can be considered to be overt failures or faults.

When the detection is not very fast (e.g., by proof tests) the detected failures or faults cannot be considered to be overt failures or faults when addressing safety integrity levels.

Note 4 to entry: A dangerous revealed failure can only be treated as a safe failure if effective measures, automatic or manual, are taken in a short enough time to maintain process safety.

3.2.14

device

hardware, with or without software, capable of performing a specified function

Note 1 to entry: Examples are sensors, logic solvers, final elements, operator interfaces, and field wiring.

3.2.14.1

field device

SIS or BPCS device connected directly to the process or located in close proximity to the process

Note 1 to entry: Examples are sensors, final elements and manual switches.

3.2.15

diagnostics

frequent (in relation to the process safety time) automatic test to reveal faults

3.2.15.1

diagnostic coverage

DC

fraction of dangerous failures rates detected by diagnostics. Diagnostic coverage does not include any faults detected by proof tests

Note 1 to entry: Diagnostic coverage is typically applied to SIS devices or SIS subsystems. E.g., the diagnostic coverage is typically determined for a sensor, final element or a logic solver.

Note 2 to entry: For safety applications the diagnostic coverage is typically applied to dangerous failures of SIS devices or SIS subsystems. For example, the diagnostic coverage for the dangerous failures of a device is $DC = \lambda_{DD} / \lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate. For a SIS subsystem with internal redundancy, DC is time dependant: $DC(t) = \lambda_{DD}(t) / \lambda_{DT}(t)$.

Note 3 to entry: When the diagnostic coverage (DC) and the total dangerous failure rate (λ_{DT}) are given, the detected (λ_{DD}) and undetected dangerous failures (λ_{DU}) can be computed as follows:

$$\lambda_{DD} = DC \times \lambda_{DT} \text{ and } \lambda_{DU} = (1-DC) \times \lambda_{DT}.$$

3.2.16

diversity

different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical means, different programming techniques, or different design approaches.

3.2.17

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.2.18

failure

loss of ability to perform as required

Note 1 to entry: A failure of a device is an event that results in a fault state of that device.

Note 2 to entry: When the loss of ability is caused by a latent fault, the failure occurs when a particular set of circumstances is encountered.

Note 3 to entry: Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

Note 4 to entry: Failures are either random or systematic (see 3.2.59 and 3.2.81).

[SOURCE: IEC 60050-192:2015, 192-03-01, modified – Notes to entry have been changed]

3.2.18.1

failure mode

manner in which failure occurs

Note 1 to entry: A failure mode may be defined by the function lost or the state transition that occurred.

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.2.19

fault

inability to perform as required, due to an internal state

Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life-cycle, such as specification, design, manufacture or maintenance.

Note 2 to entry: A fault of a device results in a failure when a particular set of circumstances is encountered.

[SOURCE: IEC 60050-192:2015, 192-04-01, modified – Some notes to entry have been changed, others have been deleted]

3.2.20

fault avoidance

use of techniques and procedures which aim to avoid the introduction of faults during any phase of the SIS safety life-cycle

3.2.20.1

fault exclusion

elimination from further consideration of faults due to improbable failure modes

Note 1 to entry: Further information about fault exclusion can be found in ISO 13849-1 and ISO 13849-2. After those standards fault exclusion can be based on

- the technical improbability of occurrence of some faults,
- generally accepted technical experience, independent of the considered application;
- technical requirements related to the application and the specific hazard.

Note 2 to entry: Failure modes, identified in the devices performing the safety function, can be excluded because their related dangerous failure rate(s) are very low compared to the target failure measure for the safety function under consideration. That is, the sum of the dangerous failure rates of all serial devices on which fault exclusion is being claimed, generally cannot exceed more than 1 % of the target failure measure.

3.2.21

fault tolerance

ability of a functional item to continue to perform a required function in the presence of faults or errors

3.2.22

final element

part of the BPCS or SIS that implements the physical action necessary to achieve or maintain a safe state

Note 1 to entry: Examples are valves, switch gear, and motors, including their auxiliary elements (such as solenoid valve and actuator used to operate a valve).

3.2.23

functional safety

part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers

3.2.24

functional safety assessment

FSA

investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers

3.2.25

functional safety audit

systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

Note 1 to entry: A functional safety audit may be carried out as part of a FSA.

3.2.26

hardware safety integrity

part of the safety integrity of the SIS relating to random hardware failures in a dangerous mode of failure

Note 1 to entry: The two failure measures that are relevant in this context are the average frequency of dangerous failure and the average probability of failure on demand.

Note 2 to entry: See 3.2.82.

Note 3 to entry: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.27

harm

injury or damage to the health of people, or damage to property or to the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.2.27.1

harmful event

hazardous event which has caused harm

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property, or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred. A hazardous event which has caused harm is termed a harmful event.

3.2.28

hazard

potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (e.g., fire and explosion) and also those that have a long-term effect on a person's health (e.g., release of a toxic substance or radioactivity).

[SOURCE: ISO/IEC Guide 51:2014, 3.2, modified – Note 1 to entry has been added]

3.2.28.1

hazardous event

event that can cause harm

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

[SOURCE: ISO/IEC Guide 51:2014: 3.3, modified – see Note 1]

3.2.28.2

hazardous situation

circumstance in which people, property or the environment are exposed to one or more hazards

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.2.29

human error

intended or unintended human action or inaction that produces an inappropriate result

Note 1 to entry: Mistakes, slips, and lapses are examples of human errors.

Note 2 to entry: This excludes malicious action.

3.2.30

impact analysis

activity of determining the effect that a change to a function or component will have to other functions or components in the system as well as in other systems

3.2.31

independent organization

organization that is separate and distinct, by management and other resources, from the organizations responsible for the activities that take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation

3.2.32

independent person

person who is separate and distinct from the activities which take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation and does not have direct responsibility for those activities

3.2.33

input function

function which monitors the process and its associated equipment in order to provide input information for the logic solver

Note 1 to entry: An input function could be a manual function.

3.2.34

instrument

apparatus used in performing an action (typically found in instrumented systems)

3.2.34.1

instrumented system

system composed of sensors (e.g., pressure, flow, temperature transmitters), logic solvers (e.g., programmable controllers, distributed control systems, discrete controllers), and final elements (e.g., control valves, motor control circuits)

Note 1 to entry: Instrumented systems perform instrumented functions including control, monitoring, alarm and protective functions. Instrumented systems can be SIS (see 3.2.67) or BPCS (see 3.2.3).

3.2.35

logic function

function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions)

Note 1 to entry: Logic functions provide the transformation from one or more input functions to one or more output functions.

Note 2 to entry: For further guidance, see IEC 61131-3:2012 and IEC 60617-12:1997.

3.2.36

logic solver

part of either a BPCS or SIS that performs one or more logic function(s)

Note 1 to entry: In IEC 61511 the following terms for logic solvers are used:

- electrical logic systems for electro-mechanical technology;
- electronic logic systems for electronic technology;
- PE logic system for programmable electronic systems.

Note 2 to entry: Examples are: electrical systems, electronic systems, programmable electronic systems, pneumatic systems, and hydraulic systems. Sensors and final elements are not part of the logic solver.

3.2.36.1

safety configured PE logic solver

general purpose industrial grade PE logic solver which is specifically configured for use in safety applications

Note 1 to entry: Further guidance can be found in 11.5.

3.2.37

maintenance/engineering interface

hardware and software provided to allow proper SIS maintenance or modification

Note 1 to entry: Maintenance/engineering interface can include instructions and diagnostics which may be found in software, programming terminals with appropriate communication protocols, diagnostic tools, indicators, bypass devices, test devices, and calibration devices.

3.2.37.1

mean repair time

MRT

expected overall repair time

Note 1 to entry: MRT encompasses the times (b), (c) and (d) of the times for MTTR (see 3.2.37.2).

3.2.37.2

mean time to restoration

MTTR

expected time to achieve restoration

Note 1 to entry: MTTR encompasses:

- the time to detect the failure (a);
- the time spent before starting the repair (b);
- the effective time to repair (c);
- the time before the component is put back into operation (d).

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

3.2.37.3

maximum permitted repair time

MPRT

maximum duration allowed to repair a fault after it has been detected

Note 1 to entry: The MRT may be used as MPRT but the MPRT may be defined without regards to the MRT:

- A MPRT smaller than the MRT can be chosen to decrease the probability of hazardous event.
- A MPRT greater than the MRT can be chosen if the probability of hazardous event can be relaxed.

Note 2 to entry: When a MPRT has been defined it can be used in place of the MRT for calculating the probability of random hardware failures.

3.2.38

mitigation

action that reduces the consequence(s) of a hazardous event

Note 1 to entry: Examples include emergency depressurization or closing ventilation dampers on detection or confirmed fire or gas leak or initiation of deluge on confirmed fire detection.

3.2.39

mode of operation (of a SIF)

way in which a SIF operates which may be either low demand mode, high demand mode or continuous mode

- a) **low demand mode:** mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year.
- b) **high demand mode:** mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year.
- c) **continuous mode:** mode of operation where the SIF retains the process in a safe state as part of normal operation.

3.2.39.1

demand mode SIF

SIF operating in low demand mode (3.2.39 a)) or high demand mode (3.2.39 b))

Note 1 to entry: In the event of a dangerous failure of the SIF, a hazardous event can only occur

- if the failure is undetected and a demand occurs before the next proof test;
- if the failure is detected by the diagnostic tests but the related process and its associated equipment has not been moved to a safe state before a demand occurs.

Note 2 to entry: In high demand mode, it will normally be appropriate to use the continuous mode criteria.

Note 3 to entry: The safety integrity levels for SIF operating in demand mode are defined in Tables 4 and 5.

3.2.39.2

continuous mode SIF

SIF operating in continuous mode (3.2.39 c))

Note 1 to entry: In the event of a dangerous failure of the SIF a hazardous event will occur without further failure unless action is taken to prevent it within the process safety time.

Note 2 to entry: Continuous mode covers those SIF which implement continuous control to maintain functional safety.

Note 3 to entry: The safety integrity levels for SIF operating in continuous mode are defined in Table 5.

3.2.40

module

self-contained part of a SIS application program (can be internal to a program or a set of programs) that performs a specified function (e.g., final element start/stop/test sequence, an application specific sequence within a SIF)

Note 1 to entry: In the context of IEC 61131-3:2012, a software module is a function or function block.

Note 2 to entry: Most modules have repetitive usage within an application program.

3.2.41

MooN

SIS, or part thereof, made up of “N” independent channels, which are so connected, that “M” channels are sufficient to perform the SIF

3.2.42

necessary risk reduction

risk reduction to be achieved by the SIS(s) and/or other protection layers to ensure that the tolerable risk is not exceeded

3.2.43

non-programmable system (NP) system

system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software)

Note 1 to entry: Examples would include hard-wired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

3.2.44

operating environment

conditions inherent to the installation of a device that potentially affects its functionality and safety integrity, such as:

- external environment, e.g. , winterization needs, hazardous area classification;
- process operating conditions, e.g., extremes in temperature, pressure, vibration;
- process composition, e.g., solids, salts, or corrosives;
- process interfaces;
- integration within the overall plant maintenance and operating management systems;
- communication through-put, e.g., electro-magnetic interference; and
- utility quality, e.g., electrical power, air, hydraulics.

Note 1 to entry: Some process applications may have special operating environment requirements necessary to survive a major accident event. For example some equipment requires special enclosures, purging, or fire protection.

3.2.45

operating mode

process operating mode

any planned state of process operation, including modes such as start-up after emergency shutdown, normal start-up, operation, and shutdown, temporary operations, and emergency operation and shutdown

3.2.46

operator interface

means by which information is communicated between a human operator and the SIS (e.g., display interfaces, indicating lights, push-buttons, horns, alarms)

Note 1 to entry: The operator interface is sometimes referred to as the human-machine interface (HMI).

3.2.47

output function

function which controls the process and its associated equipment according to output information from the logic function

3.2.48

performance

accomplishment of a given action or task measured against the specification and the IEC 61511 series

3.2.49

phase

period within the SIS safety life-cycle where activities described in the IEC 61511 series take place

3.2.50 **prevention**

action that reduces the likelihood of occurrence of a hazardous event

3.2.51 **prior use**

documented assessment by a user that a device is suitable for use in a SIS and can meet the required functional and safety integrity requirements, based on previous operating experience in similar operating environments

Note 1 to entry: To qualify a SIS device on the basis of prior use, the user can document that the device has achieved satisfactory performance in a similar operating environment. Understanding how the equipment behaves in the operating environment is necessary to achieve a high degree of certainty that the planned design, inspection, testing, maintenance, and operational practices are sufficient.

Note 2 to entry: Proven in use is based on the manufacturer's design basis (e.g., temperature limit, vibration limit, corrosion limit, desired maintenance support) for his device. Prior use deals with device's installed performance within a process sector application in a specific operating environment which is often different than the manufacturer's design basis.

3.2.52 **process risk**

risk arising from the process conditions caused by abnormal events (including BPCS malfunction)

Note 1 to entry: The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e., the risk associated with functional safety).

Note 2 to entry: Process risk analysis is described in IEC 61511-3:2016. The main purpose of determining the process risk is to establish a reference point for the risk without taking into account the protection layers.

Note 3 to entry: Assessment of this risk can include associated human factor issues.

Note 4 to entry: This term equates to "EUC risk" in IEC 61508-4:2010.

3.2.52.1 **process safety time**

time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed

Note 1 to entry: This is a property of the process only. The SIF has to detect the failure and complete its action soon enough to prevent the hazardous event taking into account any process lag (e.g. cooling of a vessel).

3.2.53 **programmable electronics** **PE**

item based on computer technology which may be comprised of hardware, software, and of input and/or output units

Note 1 to entry: This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories. Examples of process sector programmable electronics include:

- smart sensors and final elements;
- programmable electronic logic solvers including:
- programmable controllers;
- programmable logic controllers;
- loop controllers.

3.2.54 **programmable electronic system** **PES**

system for control, protection or monitoring based on one or more programmable electronic devices, including all devices of the system such as power supplies, sensors and other input

devices, data highways and other communication paths, actuators and other output devices (see Figure 5)

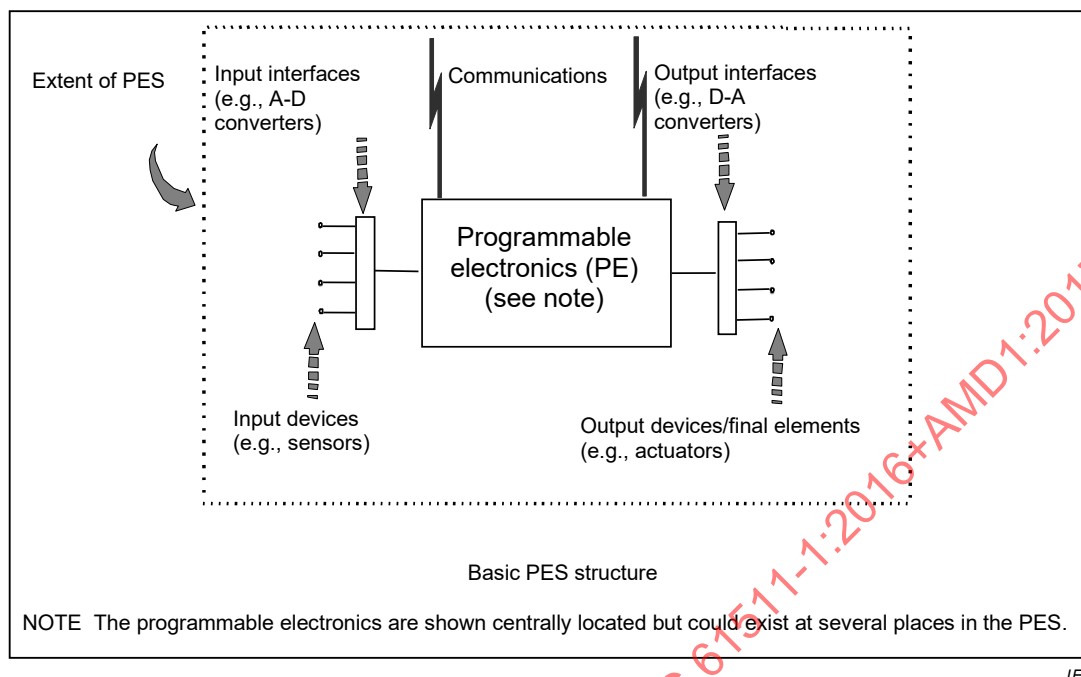


Figure 5 – Programmable electronic system (PES): structure and terminology

3.2.55 programming coding

process of designing, writing and testing a set of instructions for solving a problem or processing data

Note 1 to entry: In the IEC 61511 series, programming is typically associated with PE.

3.2.56 proof test

periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition

3.2.57 protection layer

any independent mechanism that reduces risk by control, prevention or mitigation

Note 1 to entry: It can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical mechanism such as a relief valve, a SIS or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions (see Figure 9).

3.2.58 quality

totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs

Note 1 to entry: See ISO 9000 for more details.

3.2.59 random hardware failure

failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e., random) times.

Note 2 to entry: Two major differences distinguish the random hardware failures and the systematic failures:

- a random hardware failure involves only the system itself while a systematic failure involves both the system itself (a fault) and a particular condition (see 3.2.81). Then a random hardware failure is characterized by a single reliability parameter (i.e., the failure rate) while a systematic failure is characterized by two reliability parameters (i.e., the probability of the pre-existing fault and the hazard rate of the particular condition).
- a systematic failure can be eliminated after being detected while random hardware failures cannot.

This implies that the reliability parameters of random hardware failures can be estimated from field feedback while it is very difficult to do the same for systematic failures. A qualitative approach is preferred for systematic failures.

[SOURCE: IEC 61508-4:2010, 3.6.5, modified – The notes have been changed]

3.2.60

redundancy

the existence of more than one means for performing a required function or for representing information

Note 1 to entry: Examples are the use of duplicate devices and the addition of parity bits.

Note 2 to entry: Redundancy is used primarily to improve reliability or availability.

[SOURCE: IEC 61508-4:2010, 3.4.6]

3.2.61

risk

combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation, the occurrence of a hazardous event, and the possibility to avoid or limit the harm.

[SOURCE: ISO/IEC Guide 51:2014, 3.8]

3.2.62

safe failure

failure which favours a given safety action

Note 1 to entry: A failure is "safe" only with regard to a given safety function.

Note 2 to entry: When fault tolerance is implemented, safe failure can lead to either:

- operation where the safety action is available but with a higher probability of success on demand or a lower likelihood to cause a hazardous event;
- a spurious operation where the safety action is initiated.

Note 3 to entry: When no fault tolerance is implemented, safe failures result in the initiation of the safety action regardless of the process condition. This is also known as a spurious trip.

Note 4 to entry: A spurious trip may be safe with regard to a given safety function but may be dangerous with regard to another safety function.

Note 5 to entry: Spurious trips may also have detrimental effects on the production availability of the process.

3.2.63

safe state

state of the process when safety is achieved

Note 1 to entry: Some states are safer than others and in going from a hazardous condition to the final safe state, or in going from the nominal safe condition to a hazardous condition, the process may have to go through a number of intermediate safe-states.

Note 2 to entry: For some situations, a safe state exists only so long as the process is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

Note 3 to entry: A state which is safe with regard to a given safety function may increase the probability of hazardous event with regard to another given safety function. In this case, the maximum allowable average spurious trip frequency (see 10.3.2) for the first function can consider the potential increased risk associated with the other function.

Note 4 to entry: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.64

safety

freedom from risk which is not tolerable

Note 1 to entry: According to ISO/IEC Guide 51 the terms "acceptable risk" and "tolerable risk" are considered to be synonymous.

[SOURCE: ISO/IEC Guide 51:2014, 3.14, modified – The note has been added]

3.2.65

safety function

function to be implemented by one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

3.2.66

safety instrumented function

SIF

safety function to be implemented by a safety instrumented system (SIS)

Note 1 to entry: A SIF is designed to achieve a required SIL which is determined in relationship with the other protection layers participating to the reduction of the same risk.

3.2.67

safety instrumented system

SIS

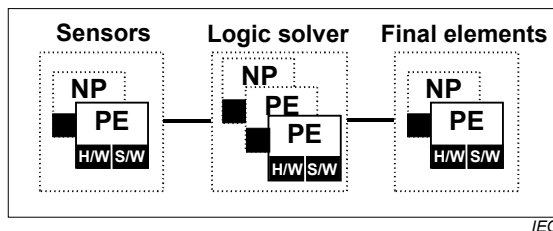
instrumented system used to implement one or more SIFs

Note 1 to entry: A SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s) (e.g., see Figure 6). It also includes communication and ancillary equipment (e.g., cables, tubing, power supply, impulse lines, heat tracing).

Note 2 to entry: A SIS may include software.

Note 3 to entry: A SIS may include human action as part of a SIF (see ISA TR84.00.04:2015, part 1).

SIS architecture and safety instrumented function example with different devices shown



IEC

Figure 6 – Example of SIS architectures comprising three SIS subsystems

3.2.68

safety integrity

ability of the SIS to perform the required SIF as and when required

Note 1 to entry: This definition is equivalent to the dependability of the SIS with regard to the required SIF. Dependability, being often understood as an economical rather than a safety concept, has not been used to avoid confusion.

Note 2 to entry: Ability includes both the functional response (e.g., closing a specified valve within a specified time) and the likelihood that the SIS will act as required.

Note 3 to entry: In determining safety integrity, all causes of random hardware and systematic failures which lead to an unsafe state can be included (e.g., hardware failures, software induced failures and failures due to electrical interferences). Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the average dangerous failure frequency or the probability of failure on demand. However, safety integrity also depends on many systematic factors, which cannot be accurately quantified and are often considered qualitatively throughout the life-cycle. The likelihood that systematic failures result in dangerous failure of the SIS is reduced through hardware fault tolerance (see 11.4) or other methods and techniques.

Note 4 to entry: Safety integrity comprises hardware safety integrity (see 3.2.26) and systematic safety integrity (see 3.2.82), but complex failures caused by the conjunction of both hardware and systematic interaction can also be considered.

3.2.69

safety integrity level

SIL

discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS

Note 1 to entry: The higher the SIL, the lower the expected PFD_{avg} the lower the average frequency of a dangerous failure causing a hazardous event.

Note 2 to entry: The relationship between the target failure measure and the SIL is specified in Tables 4 and 5.

Note 3 to entry: SIL 4 is related to the highest level of safety integrity; SIL 1 is related to the lowest

Note 4 to entry: This definition differs from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.69.1

safety integrity requirements, pl

set of the IEC 61511 requirements which shall be satisfied by a SIS to claim a given SIL for a SIF implemented by this SIS

Note 1 to entry: The safety integrity requirements are strengthened when the related SIL increases.

3.2.70

SIS safety life-cycle

necessary activities involved in the implementation of SIF occurring during a period of time that starts at the concept phase of a project and finishes when all of the SIF are no longer available for use

Note 1 to entry: The term “functional safety life-cycle” is strictly more accurate, but the adjective “functional” is not considered necessary in this case within the context of the IEC 61511 series.

Note 2 to entry: The SIS safety life-cycle model used in IEC 61511 is shown in Figure 7.

3.2.71

safety manual

functional safety manual

information that defines how a SIS device, subsystem or system can be safely applied

Note 1 to entry: The safety manual may include inputs from the manufacturer as well as from the user.

Note 2 to entry: For IEC 61508 compliant devices, the manufacturer's input is the safety manual,

Note 3 to entry: This could be a generic stand-alone document, or a collection of documents.

Note 4 to entry: This definition deviates from the definition in IEC 61508-4:2010 to reflect differences in process sector terminology.

3.2.72 **safety requirements specification** **SRS**

specification containing the functional requirements for the SIFs and their associated safety integrity levels

[SOURCE: IEC 61508-4:2010, 3.5.11, modified – Aligned with IEC 61511 terminology]

3.2.73 **sensor**

part of the BPCS or SIS that measures or detects the process condition

Note 1 to entry: Examples are transmitters, transducers, process switches, and position switches.

3.2.74 **software**

programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

Note 1 to entry: Software is independent of the medium on which it is recorded.

Note 2 to entry: For examples of different types of software, see 3.2.75 and 3.2.76.

3.2.75 **application programming languages**

3.2.75.1 **fixed program language** **FPL**

language in which the user is limited to adjustment of a few pre-defined and fixed set of parameters

Note 1 to entry: Typical examples of device applications with FPL are: smart sensor (e.g., pressure transmitter without control algorithms), smart final element (e.g. valve without control algorithms), sequence of events recorder, set points for dedicated smart alarm box). The use of FPL is often referred to as "configuration of the device".

3.2.75.2 **limited variability language** **LVL**

programming language for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application as defined by the associated safety manual. The notation of this language may be textual or graphical or have characteristics of both.

Note 1 to entry: This type of language is designed to be easily understood by process sector users, and provides the capability to combine predefined, application specific, library functions to implement the SRS. LVL provides a close functional correspondence with the functions required to achieve the application.

Note 2 to entry: IEC 61511 assumes that the constraints necessary to achieve the safety properties are achieved by the combination of the safety manual, the closeness of the language notations to the functions the application programmer needs to define the process control algorithms, and the compile time and run time checks which the logic solver provider embeds into the logic solver system program and the logic solver development environment. The constraints identified in the certification report and safety manual can ensure the relevant requirements of IEC 61508-3:2010 are satisfied.

Note 3 to entry: LVL is the most commonly used language when the IEC 61511 series refers to "application program".

3.2.75.3 **full variability language** **FVL**

language designed to be comprehensible to computer programmers and that provides the capability to implement a wide variety of functions and applications

Note 1 to entry: Typical example of systems using FVL are general purpose computers.

Note 2 to entry: In the process sector, FVL is found in embedded software and rarely in application programming.

Note 3 to entry: FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

3.2.76 software & program types

3.2.76.1 application program

program specific to the user application containing, in general, logic sequences, permissives, limits and expressions that control the input, output, calculations, and decisions necessary to meet the SIS functional requirements

3.2.76.2 embedded software

software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user

Note 1 to entry: Embedded software is also referred to as firmware or system software. See 3.2.75.3 full variability language.

3.2.76.3 utility software

software tools for the creation, modification, and documentation of application programs

Note 1 to entry: These software tools are not required for the operation of the SIS.

3.2.77 application program life-cycle

activities occurring during a period of time that starts when the application program is conceived and ends when the application program is permanently disused

Note 1 to entry: An application program life-cycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and modification phase.

Note 2 to entry: Software, including application program, cannot be maintained; rather, it is modified.

3.2.78 SIS subsystem

independent part of a SIS whose disabling dangerous failure results in a disabling dangerous failure of the SIS

Note 1 to entry: Figure 6 illustrates a SIS made of three SIS subsystems.

Note 2 to entry: From the cut set approach point of view (see IEC 61025) a minimal cut set of a SIS subsystem is also a minimal cut set of the whole SIS. Therefore the SIFs implemented within a SIS are entirely dependent on the SIS subsystems of this SIS (i.e., when a SIS subsystem fails, the related SIFs also fail).

3.2.79 system

set of devices, which interact according to a specification

Note 1 to entry: A person can be part of a system.

Note 2 to entry: This definition deviates from the definition in IEC 61508 to reflect differences in process sector terminology.

3.2.80 systematic capability

measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual

Note 1 to entry: Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults in IEC 61508-2:2010 and IEC 61508-3:2010.

Note 2 to entry: The systematic failure mechanism depends on the nature of the device. For a device comprised solely of hardware, only hardware failure mechanisms are considered. For a device comprised of hardware and software, it is necessary to consider the interactions between hardware and software failure mechanisms.

Note 3 to entry: A systematic capability of SC N for a device means that the systematic safety integrity of SC N has been met when the device is applied in accordance with the instructions specified in the device safety manual for SC N.

3.2.81

systematic failure

failure related to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors.

Note 1 to entry: The cause of systematic failures of the software may be known as "bugs".

Note 2 to entry: Corrective maintenance without modification would usually not eliminate the failure cause which involves the failure under particular conditions.

Note 3 to entry: A systematic failure can be reproduced by deliberately applying the same conditions, although not all reproducible failures are systematic.

Note 4 to entry: Examples of faults leading to systematic failure include human error that originates in:

- the SRS;
- the design, manufacture, installation, operation or maintenance of the hardware;
- the design or implementation of software (including application program).

Note 5 to entry: Similar devices designed, installed, operated, implemented or maintained in the same way are likely to contain the same faults. Therefore they are subject to common cause failures when the particular conditions occur.

3.2.82

systematic safety integrity

part of the safety integrity of the SIS relating to systematic failures in a dangerous mode of failure

Note 1 to entry: Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity).

Note 2 to entry: See 3.2.26 also.

3.2.83

target failure measure

performance required from the SIF and specified in terms of either the average probability of failure to perform the SIF on demand for demand mode of operation or the average frequency of a dangerous failure for continuous mode of operation

Note 1 to entry: The relationship between the target failure measures and the SIL are given in Tables 4 and 5.

3.2.84

tolerable risk

level of risk which is accepted in a given context based on the current values of society

Note 1 to entry: See IEC 61511-3:2016, Annex A.

[SOURCE: ISO/IEC Guide 51:2014, 3.15]

3.2.85

undetected unrevealed covert

not detected or not revealed or not overt

Note 1 to entry: In IEC 61511 and except when the context suggests another meaning, the term “dangerous undetected failures/faults” is related to dangerous failures/faults not detected by diagnostic tests.

3.2.86

validation

confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: In the IEC 61511 series this means demonstrating that the SIF(s) and SIS after installation meet the SRS in all respects.

3.2.87

verification

confirmation by examination and provision of objective evidence that the requirements have been fulfilled

Note 1 to entry: In the IEC 61511 series this is the activity of demonstrating for each phase of the relevant SIS safety life-cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

Note 2 to entry: Example verification activities include:

- reviews on outputs (documents from all phases of the safety life-cycle) to ensure compliance with the objectives and requirements of the phase taking into account the specific inputs to that phase;
- design reviews;
- tests performed on the designed products to ensure that they perform according to their specification;
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

3.2.88

watchdog

combination of diagnostics and an output device (typically a switch) for monitoring the correct operation of the programmable electronic (PE) device and taking action upon detection of an incorrect operation

Note 1 to entry: The watchdog confirms that the software system is operating correctly by the regular resetting of an external device (e.g., hardware electronic watchdog timer) by an output device controlled by the software.

Note 2 to entry: The watchdog can be used to de-energize a group of safety outputs when dangerous failures are detected in order to achieve or maintain a safe state of the process with respect to the hazardous event. The watchdog is used to increase the on-line diagnostic coverage of the PE logic solver (see 3.2.13 and 3.2.15).

3.3 Abbreviations

Abbreviations used throughout IEC 61511 are given in Table 1. Also included are some common abbreviations related to process sector functional safety.

Table 1 – Abbreviations used in IEC 61511

Abbreviation	Full expression
AC/DC	Alternating current/direct current
AIChE	American Institute of Chemical Engineers
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
AP	Application program
BPCS	Basic process control system
CCPS	Centre for Chemical Process Safety (AIChE)
DC	Diagnostic coverage
E/E/PE	Electrical/electronic/programmable electronic
EMC	Electro-magnetic compatibility

Abbreviation	Full expression
FAT	Factory acceptance test
FPL	Fixed program language
FSA	Functional safety assessment
FSMS	Functional safety management system
FTA	Fault tree analysis
FVL	Full variability language
HFT	Hardware fault tolerance
H&RA	Hazard & risk assessment
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
LVL	Limited variability language
MooN	“M” out of “N” channel architecture
MPRT	Maximum permitted repair time
MRT	Mean repair time
MTTR	Mean time to restoration
NFPA	National Fire Protection Association(US)
NP	Non-programmable
OEM	Original Equipment Manufacturer
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of dangerous failure on demand
PFD _{avg}	Average probability of dangerous failure on demand
PFH	Probability (average frequency of dangerous failures) of failure per hour
pl	Plural
PLC	Programmable logic controller
SAT	Site acceptance test
SC	Systematic capability
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification

4 Conformance to the IEC 61511-1:2016

To conform to the IEC 61511-1:2016, it shall be shown that each of the requirements outlined in Clause 5 through Clause 19 has been satisfied to the defined criteria and therefore the clauses' objectives have been met.

5 Management of functional safety

5.1 Objective

The objective of the requirements of Clause 5 is to identify the management activities that are necessary to ensure the functional safety objectives are met.

NOTE 1: Clause 5 is solely aimed at the achievement and maintenance of the functional safety of SIS and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

5.2 Requirements

5.2.1 General

The policy and strategy for achieving functional safety shall be identified together with the methods for evaluating their achievement and shall be communicated within the organization.

5.2.2 Organization and resources

5.2.2.1 Persons, departments, organizations or other units which are responsible for carrying out and reviewing each of the SIS safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them.

5.2.2.2 Persons, departments or organizations involved in SIS safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

The following items shall be addressed and documented when considering the competence of persons, departments, organizations or other units involved in SIS safety life-cycle activities:

- a) engineering knowledge, training and experience appropriate to the process application;
- b) engineering knowledge, training and experience appropriate to the applicable technology used (e.g., electrical, electronic or programmable electronic);
- c) engineering knowledge, training and experience appropriate to the sensors and final elements;
- d) safety engineering knowledge (e.g., process safety analysis);
- e) knowledge of the legal and regulatory functional safety requirements;
- f) adequate management and leadership skills appropriate to their role in the SIS safety life-cycle activities;
- g) understanding of the potential consequence of an event;
- h) the SIL of the SIF;
- i) the novelty and complexity of the application and the technology.

5.2.2.3 A procedure shall be in place to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.

5.2.3 Risk evaluation and risk management

Hazards shall be identified, risks evaluated and the necessary risk reduction determined as defined in Clause 8.

NOTE It may be beneficial to consider also potential capital losses, for economic reasons.

5.2.4 Safety planning

Safety planning shall take place to define the activities that are required to be carried out along with the persons, departments, organizations or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire SIS safety life-cycle (see Clause 6) and carried out to a detailed activity level commensurate with the role the individual or organization is performing in the SIS safety life-cycle.

NOTE The safety planning can be incorporated in

- a section in the quality plan entitled “SIS Safety Life-cycle Plan”; or
- a separate document entitled “SIS Safety Life-cycle Plan”; or
- several documents which may include company procedures or working practices.

5.2.5 Implementing and monitoring

5.2.5.1 Procedures shall be implemented to ensure prompt follow-up and satisfactory resolution of recommendations pertaining to the SIS arising from

- a) hazard analysis and risk assessment;
- b) assurance activities;
- c) verification activities;
- d) validation activities;
- e) FSAs;
- f) functional safety audits;
- g) post-incident and post-accident activities.

5.2.5.2 Any supplier, providing products or services to an organization that has overall responsibility for one or more phases of the SIS safety life-cycle, shall deliver products or services as specified by that organization and shall have a quality management system. Procedures shall be in place to demonstrate the adequacy of the quality management system.

If a supplier makes any functional safety claims for a product or service, which are used by the organization to demonstrate compliance with the requirements of this part of IEC 61511, the supplier shall have a functional safety management system. Procedures shall be in place to demonstrate the adequacy of the functional safety management system.

The functional safety management system shall meet the requirements of the basic safety standard IEC 61508-1:2010, Clause 6, or the functional safety management requirements of the standard derived from IEC 61508 to which functional safety claims are made.

5.2.5.3 Procedures shall be implemented to evaluate the performance of the SIS against its safety requirements to:

- identify and prevent systematic failures which could jeopardize safety;
- monitor and assess whether reliability parameters of the SIS are in accordance with those assumed during the design;
- define the necessary corrective action to be taken if the failure rates are greater than what was assumed during design;
- compare the demand rate on the SIF during actual operation with the assumptions made during risk assessment when the SIL requirements were determined.

5.2.5.4 For existing SIS designed and constructed in accordance with code, standards, or practices prior to the issue of this standard the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

5.2.6 Assessment, auditing and revisions

5.2.6.1 Functional safety assessment (FSA)

5.2.6.1.1 A procedure shall be defined and executed for a FSA in such a way that a judgement can be made as to the functional safety and safety integrity achieved by every SIF of the SIS. The procedure shall require that a FSA team be appointed which includes the technical, application and operations expertise needed for the particular application.

5.2.6.1.2 The membership of the FSA team shall include at least one senior competent person not involved in the project design team (for stages 1, 2 and 3) or not involved in the operation and maintenance of the SIS (for stages 4 and 5).

5.2.6.1.3 The following shall be considered when planning a FSA:

- the scope of the FSA;
- who is to participate in the FSA;
- the skills, responsibilities and authorities of the FSA team;
- the information that will be generated as a result of any FSA activity;
- the identity of any other safety bodies involved in the FSA;
- the resources required to complete the FSA activity;
- the level of independence of the FSA team;
- the methods by which the FSA will be revalidated after modifications.

NOTE When the FSA team is large; consideration can be given to having more than one senior competent individual on the team who is independent from the project team.

5.2.6.1.4 A FSA team shall review the work carried out on all phases of the safety life cycle prior to the stage covered by the assessment that have not been already covered by previous FSAs. If previous FSAs have been carried out then the FSA team shall consider the conclusions and recommendations of the previous assessments. The stages in the SIS safety life-cycle at which the FSA activities are to be carried out shall be identified during the safety planning.

NOTE 1 Additional FSA activities can be introduced as new hazards are identified, after modification and at periodic intervals during operation.

NOTE 2 Consideration can be given to carrying out FSA activities at the following stages (see Figure 7).

- Stage 1 – After the H&RA has been carried out, the required protection layers have been identified and the SRS has been developed.
- Stage 2 – After the SIS has been designed.
- Stage 3 – After the installation, pre-commissioning and final validation of the SIS has been completed and operation and maintenance procedures have been developed.
- Stage 4 – After gaining experience in operating and maintenance.
- Stage 5 – After modification and prior to decommissioning of a SIS.

NOTE 3 The number, size and scope of FSA activities can depend upon the specific circumstances. The factors in this decision are likely to include:

- size of project;
- degree of complexity;
- SIL;
- duration of project;
- consequence in the event of failure;
- degree of standardization of design features;
- safety regulatory requirements;
- previous experience with a similar design;
- giving consideration to relevant factors such as:
 - time in operation;
 - number and scope of changes in operation;
 - proof test frequency.

5.2.6.1.5 Prior to the hazards being present the FSA team shall undertake functional safety assessment(s) and shall confirm:

- the H&RA has been carried out (see 8.1);
- the recommendations arising from the H&RA that apply to the SIS have been implemented or resolved;
- project design change procedures are in place and have been properly implemented;
- the recommendations arising from any FSA have been resolved;
- the SIS is designed, constructed and installed in accordance with the SRS, any differences having been identified and resolved;
- the safety, operating, maintenance and emergency procedures pertaining to the SIS are in place;
- the SIS validation planning is appropriate and the validation activities have been completed;
- the employee training has been completed and appropriate information about the SIS has been provided to the maintenance and operating personnel;
- plans or strategies for implementing further FSAs are in place.

5.2.6.1.6 Where design, development and production tools are used for any SIS safety life-cycle activity, they shall themselves be subject to an assessment demonstrating that they do not have any negative impact on the SIS or the output of the tools shall be confirmed by verification procedures.

NOTE 1 The degree to which such tools can be addressed will depend upon their impact on the risk level to be achieved.

NOTE 2 Examples of development and production tools include simulation and modelling tools, measuring equipment, test equipment, equipment used during maintenance activities and configuration management tools.

NOTE 3 Quality assurance of tools includes, but is not limited to, traceability to calibration standards, operating history and defect list.

5.2.6.1.7 The results of the FSA shall be available together with any recommendation coming from this assessment.

5.2.6.1.8 All relevant information shall be made available to the FSA team upon their request.

5.2.6.1.9 In cases where a FSA is carried out on a modification the assessment shall consider the impact analysis carried out on the proposed modification and confirm that the modification work performed is in compliance with the requirements of IEC 61511.

NOTE Safety life cycle (including FSA) requirements related to SIS modifications can be found in 17.2.3.

5.2.6.1.10 A FSA shall also be carried out periodically during the operations and maintenance phase to ensure that maintenance and operation are being carried out according to the assumptions made during design and that the requirements within IEC 61511 for safety management and verification are being met.

5.2.6.2 Functional safety audit and revision

5.2.6.2.1 The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.

5.2.6.2.2 All procedures identified as necessary resulting from all safety life-cycle activities shall be subject to safety audit.

5.2.6.2.3 Functional safety audit shall be performed by an independent person not undertaking work on the SIS to be audited. Procedures shall be defined and executed for auditing compliance with requirements including:

- the frequency of the functional safety audit activities;
- the degree of independence between the persons, departments, organizations or other units carrying out the work and those carrying out the functional safety auditing activities;
- the recording and follow-up activities.

5.2.6.2.4 Management of change procedures shall be in place to initiate, document, review, implement and approve changes to the SIS other than replacement in kind (i.e., like for like, an exact duplicate of an element or an approved substitution that does not require modification to the SIS as installed).

5.2.6.2.5 Management of change procedures shall be in place that identifies changes that will affect the requirements on the SIS (e.g., re-design of a BPCS, changes to manning in a certain area).

5.2.7 SIS configuration management

5.2.7.1 Procedures for configuration management of the SIS during any SIS safety life-cycle phase shall be available.

NOTE In particular, the following can be specified:

- the stage at which formal configuration management is to be implemented;
- the procedures to be used for uniquely identifying all components of a SIS or SIS-subsystem (e.g., devices, application programming);
- the procedures for preventing unauthorized devices from entering service.

5.2.7.2 The SIS software, hardware and procedures used to develop and execute the application program shall be subject to configuration management and shall be maintained under revision control.

NOTE SIS software includes application program (e.g., in logic solvers); embedded software (e.g., sensors, logic solvers, final elements); utility software (tools).

6 Safety life-cycle requirements

6.1 Objectives.

The objectives of Clause 6 are:

- to define the phases and establish the requirements of the SIS safety life-cycle activities;
- to define and organize the technical activities into a SIS safety life-cycle;
- to ensure that adequate planning exists (or is developed) that makes certain that the SIS meets the safety requirements.

NOTE 1 The overall approach of the IEC 61511 series is shown in Figure 7. It can be stressed that this approach is for illustration and is only meant to indicate the typical SIS safety life-cycle activities from initial conception through decommissioning.

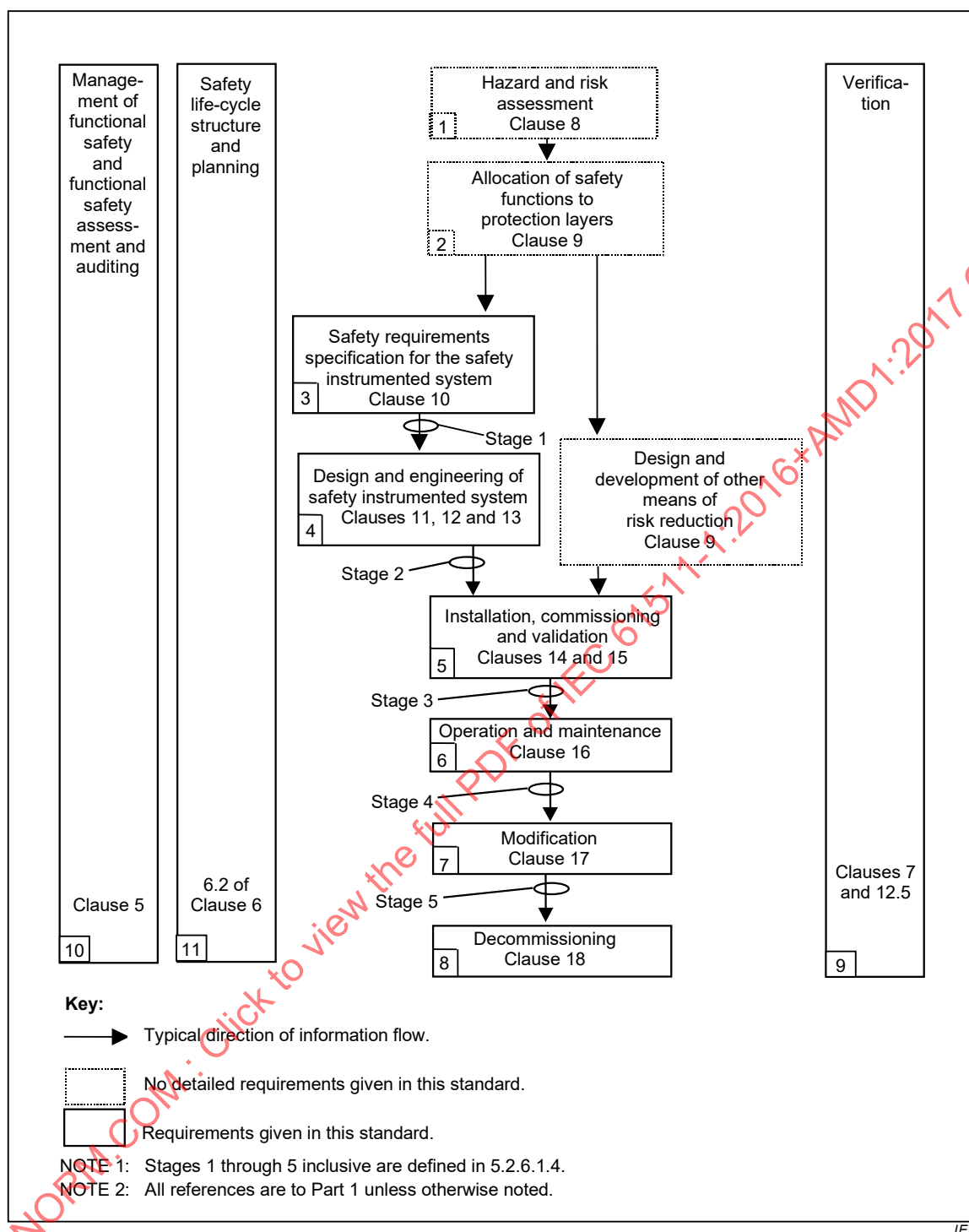


Figure 7 – SIS safety life-cycle phases and FSA stages

NOTE 2 Information in Figure 7 may flow from operation and maintenance back to the earlier life-cycle stages to reflect tracking of incidents and failures and to verify engineering assumptions.

6.2 Requirements

6.2.1 A SIS safety life-cycle incorporating the requirements of the IEC 61511 series shall be defined during safety planning. The safety life-cycle shall also address the application programming (see 6.3.1).

6.2.2 Each phase of the SIS safety life-cycle shall be defined in terms of its inputs, outputs and verification activities (see Table 2).

Table 2 – SIS safety life-cycle overview (1 of 2)

Safety life-cycle phase or activity		Objectives	Requirements Clause	Inputs	Outputs
Figure 7 box number	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	Clause 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
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL	Clause 9	A description of the required SIF and associated safety integrity requirements	Description of allocation of safety requirements
3	SIS safety requirements specification	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	Clause 10	Description of allocation of safety requirements	SIS safety requirements; application program safety requirements
4	SIS design and engineering	To design the SIS to meet the requirements for SIF and their associated safety integrity	Clauses 11, 12	SIS safety requirements Application program safety requirements	Design of the SIS hardware and application program in conformance with the SIS safety requirements; planning for the SIS integration test
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 their associated safety integrity	Clauses 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 safety requirements. Results of SIS integration tests Results of the installation, commissioning and validation activities

Table 2 (2 of 2)

Safety life-cycle phase or activity		Objectives	Requirements Clause	Inputs	Outputs
Figure 7 box number	Title				
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	Clause 16	SIS safety requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	Clause 17	Revised SIS safety requirements	Results of SIS modification
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remains appropriate	Clause 18	As built safety requirements and process information	SIF placed out of service
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	Clause 7, 12.5	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase
10	SIS FSA	To investigate and arrive at a judgement on the functional safety achieved by the SIS	Clause 5	Planning for SIS FSA SIS safety requirement	Results of SIS FSA
11	Safety lifecycle structure and planning	To establish how the lifecycle steps are accomplished	6.2	Not applicable	Safety plan

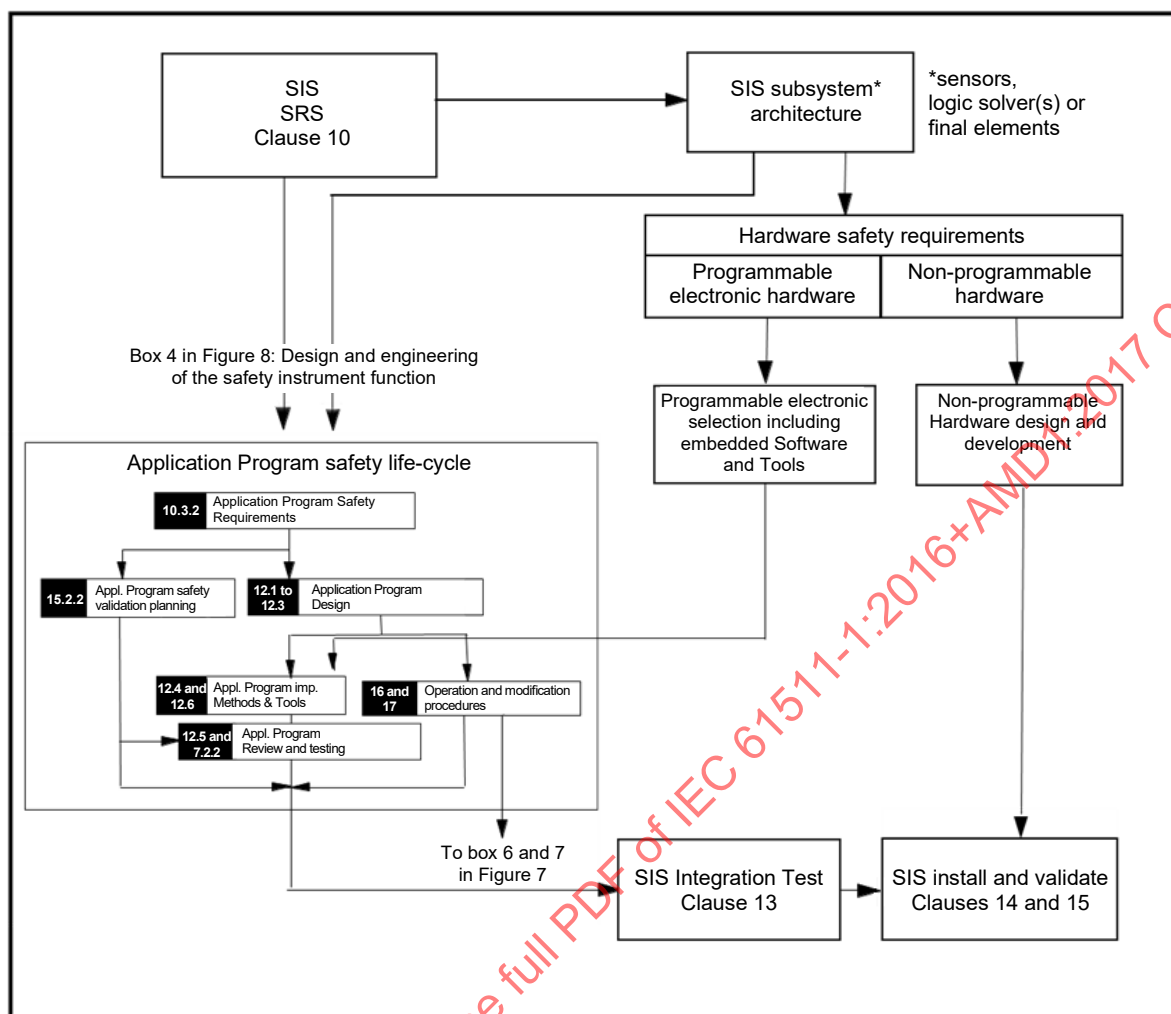
6.2.3 For all SIS safety life-cycle phases, safety planning shall take place to define the activities, criteria, techniques, measures, procedures and responsible organisation/people to:

- ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both functional and safety integrity requirements;
- ensure proper installation and commissioning of the SIS;
- ensure the safety integrity of the SIF after installation;
- maintain the safety integrity during operation (e.g., proof testing, failure analysis);
- manage the process hazards during maintenance activities on the SIS.

6.2.4 If at any stage of the safety life-cycle, a change is required pertaining to an earlier life-cycle phase, then that earlier SIS safety life-cycle phase and the subsequent phases shall be re-examined, altered as required and re-verified.

6.3 Application program SIS safety life-cycle requirements

6.3.1 Each phase of the application program safety life-cycle (see Figure 8) shall be defined in terms of its elementary activities, objectives, required input information and output results and verification requirements (see Table 3).



IEC

Figure 8 – Application program safety life-cycle and its relationship to the SIS safety life-cycle

Table 3 – Application program safety life-cycle: overview (1 of 2)

Safety life-cycle phase		Objectives	Requirements Clause	Inputs	Outputs
Figure 8 box number	Title				
10.3.2	Application program safety requirements	To specify application program safety requirements for each SIS necessary to implement the required SIF. To specify the requirements for application program for each SIF allocated to that SIS.	10.3 11.5	SIS safety requirements. Safety manuals of the selected SIS. SIS architecture.	SIS application program safety requirements specification. Verification information.
15.2.2	Application program safety validation planning	To develop a plan for validating the application program.	15.2.2, 15.2.5	SIS application program safety requirements.	SIS safety validation planning. Verification information.
12.1 to 12.3	Application program development	Architecture. To create an application program architecture that fulfils the specified requirements for application program safety. To review and evaluate the requirements placed on the application program by the hardware architecture of the SIS. To specify the procedures for the development of the application program.	12.1 (also 10.3, 12.2)	SIS application program safety requirements. SIS hardware architecture design constraints.	Description of the architecture design, e.g., segregation of application program into related process sub-system and SIL, e.g., recognition of common application program modules such as pump or valve sequences. Application program architecture and sub-system integration test requirements. Verification information.
	Application program design	To develop the application program design. To identify a suitable set of configuration, library, management, and simulation and test tools, over the safety life-cycle of the application program.	12.3	SIS application program safety requirements. Description of the architecture design. Manuals of the SIS. Safety Manual of the selected SIS logic solver.	Application program design. Procedures for use during programming. Description of the standard (manufacturers) library functions to be used. Verification information.

Table 3 (2 of 2)

Safety life-cycle phase		Objectives	Requirements Clause	Inputs	Outputs
Figure 8 box number	Title				
12.4 12.6	Application program implementation	Application development and application module development. To implement the application program that fulfils the specified requirements for application safety. To use appropriate support tools and programming languages.	12.4 12.3.4 12.6	Description of the design. List of manuals and procedures of the selected logic solver for use with the application program.	Application program (e.g., function block diagrams, ladder logic). Application program simulation and integration test. Special purpose application program safety requirements. Verification information.
12.5 7.2.2	Application program verification	To verify that the requirements for application program safety have been achieved. To show that all SIS application programs interact correctly to perform their intended functions and do not perform unintended functions.	12.5 7.2.2	Application program simulation and integration test requirements (structure based testing). Application program architecture integration test requirements.	Application program test results. Verified and tested application program system. Verification information.
13	SIS integration test	To integrate the application program onto the target logic solver, including interaction with a sample set of field devices and or simulator.	Clause 13	Application program and logic solver integration test requirements.	Application program and logic solver integration test results.

6.3.2 Methods, techniques and tools shall be applied for each life-cycle phase in accordance with 12.6.2.

6.3.3 Each phase of the SIS safety life-cycle for which safety planning has been carried out shall be verified (see Clause 7) and the results shall be available as described in Clause 19.

7 Verification

7.1 Objective

The objective of Clause 7 is to demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases (Figure 7) as identified by the verification planning.

7.2 Requirements

7.2.1 Verification planning shall be carried out throughout the SIS safety life-cycle and shall define all activities required for the appropriate phase (Figure 7) of the safety life-cycle, including the application program. Verification planning shall conform to the IEC 61511 series by addressing the following:

- the verification activities;
- the procedures, measures and techniques to be used for verification including implementation and resolution of resulting recommendations;
- when these activities will take place;
- the persons, departments and organizations responsible for these activities, including levels of independence;
- identification of items to be verified;
- identification of the information against which the verification is carried out;
- the adequacy of the outputs against the requirements for that phase;
- correctness of the data;
- how to handle non-conformances;
- tools and supporting analysis;
- the completeness of the SIS implementation and the traceability of the requirements;
- the readability and audit-ability of the documentation;
- the testability of the design.

7.2.2 Where the verification includes testing, the verification planning shall also address the following:

- the strategy for integration of application program and hardware and field devices, including the integration of sub-systems that shall comply with other standards (such as machinery or burner);
- test scope (describes the test set-up and what type of test to be performed including the hardware, application programming, and programming devices to be included);
- test cases and test data (these will be specific scenarios with the associated data);
- types of tests to be performed;
- test environment including tools, hardware, all software and required configuration;
- test criteria (e.g., pass/fail criteria) on which the results of the test will be evaluated;
- procedures for corrective action on failure during test;
- physical location(s) (e.g., factory or site);
- dependence on external functionality;
- appropriate personnel;
- management of change;
- non-conformances.

7.2.3 Non-safety functions integrated with safety functions shall be verified for non-interference with the safety functions.

7.2.4 Verification shall be performed according to the verification planning.

7.2.5 During testing, any modification shall be subjected to an impact analysis which shall determine all SIS components impacted and the necessary re-verification activities.

7.2.6 The results of the verification process shall be available (see Clause 19), including whether the objective and criteria of the tests have been met.

NOTE 1 Selection of techniques and measures for the verification process and the degree of independence depends upon a number of factors including degree of complexity, novelty of design, novelty of technology and required SIL.

NOTE 2 Examples of some verification activities include design reviews, use of tools and techniques including software verification tools and computer based design analysis tools.

8 Process H&RA

8.1 Objectives

The objectives of the requirements of Clause 8 are 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;
- any requirements for risk reduction;
- the safety functions required to achieve the necessary risk reduction;
- if any of the safety functions are SIFs.

NOTE 1 Clause 8 addresses process engineers, hazard and risk specialists, safety managers as well as instrument engineers. Its purpose is to recognize the multi-disciplinary approach typically required for the determination of SIF.

NOTE 2 Where reasonably practicable, processes can be designed to be inherently safe. When this is not practicable, other layers of protection (see Figure 9) can be required. In some applications, industry standards can specify the use of particular protection layers.

NOTE 3 The risk reduction can be accomplished using several layers of protection (see Clause 9).

8.2 Requirements

8.2.1 A H&RA shall be carried out on the materials, process and equipment. It shall result in:

- a description of each identified hazardous event and the factors that contribute to it;
- a description of the likelihood and consequence of each hazardous event;
- consideration of process operating modes such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown;
- the determination of additional risk reduction necessary to achieve the required functional safety;
- a description of, or references to information on, the measures taken to reduce or remove hazards and risk;
- a detailed description of the assumptions made during the analysis of the risks including demand rates on the protection layers and the average frequency of dangerous failures of the initiating sources, and of any credit taken for operational constraints or human intervention;
- identification of those safety function(s) applied as SIF(s).

NOTE 1 In determining the safety integrity requirements, account can be taken of the effects of common cause between systems that create demands and the protection layers that are designed to respond to those demands. An example of this would be where demands can arise through BPCS failure and the equipment used within the protective layers is similar or identical to the equipment used within the BPCS. In such cases, a demand caused by a failure of BPCS equipment may not be responded to effectively if a common cause has rendered similar equipment in the protection layer to be ineffective. It may not be possible to recognize common cause problems during the initial hazard identification and risk analysis because at such an early stage the design of the protection layers will not necessarily have been completed. In such cases, it can be necessary to reconsider the safety integrity requirements and SIF once the design of the SIS and other protection layers has been completed. In determining whether the overall design of process and protection layers meets requirements, common cause failures will be considered.

NOTE 2 Examples of techniques that can be used to establish the required SILs of SIFs are illustrated in IEC 61511-3:2016.

8.2.2 The average frequency of dangerous failures of a BPCS as an initiating source shall not be assumed to be $<10^{-5}$ per hour.

8.2.3 The H&RA shall be recorded in such a way that the relationship between the above items is clear and traceable.

NOTE 1 The above requirements do not mandate that the safety integrity requirements have to be assigned as numerical values. Qualitative or semi-quantitative approaches (see IEC 61511-3:2016, Annexes C, D & E) can also be used.

NOTE 2 The safety integrity requirements vary depending on the application and national legal requirements. An accepted principle in many countries is that additional risk reduction measures can be applied until the cost incurred becomes disproportionate to the improvement in safety integrity achieved.

8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction;
- a description of, or references to information on, the measures taken to reduce or remove the threats.

NOTE 1 Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

NOTE 2 The information and control of boundary conditions needed for the security risk assessment are typically with owner/operating company of a facility, not with the supplier. Where this is the case, the obligation to comply with 8.2.4 can be with the owner/operating company of the facility.

NOTE 3 The SIS security risk assessment can be included in an overall process automation security risk assessment.

NOTE 4 The SIS security risk assessment can range in focus from an individual SIF to all SISs within a company.

9 Allocation of safety functions to protection layers

9.1 Objectives

The objectives of the requirements of Clause 9 are to

- allocate safety functions to protection layers;
- determine the required SIFs;
- determine for each SIF the associated safety integrity requirements.

NOTE 1 Account can be taken, during the process of allocation, of other industry standards or codes.

NOTE 2 The integrity requirements for each SIF might include the associated risk reduction, PFD, PFH or SIL.

9.2 Requirements of the allocation process

9.2.1 The allocation process shall result in

- the allocation of safety functions required to achieve the necessary risk reduction to specific protection layers;
- the allocation of risk reduction or average frequency of dangerous failure to each SIF.

NOTE Legislative requirements or other industry codes may influence the allocation process.

9.2.2 The required SIL shall be derived taking into account the required PFD or PFH that is to be provided by the SIF.

NOTE Further guidance can be found in IEC 61511-3:2016.

9.2.3 For each SIF operating in demand mode, the required SIL shall be specified in accordance with either Table 4 or Table 5.

9.2.4 For each SIF operating in continuous mode, the required SIL shall be specified in accordance with Table 5.

Table 4 – Safety integrity requirements: PFD_{avg}

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	PFD_{avg}	Required risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10\ 000$ to $\leq 100\ 000$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 1\ 000$ to $\leq 10\ 000$
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to $\leq 1\ 000$
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	Average frequency of dangerous failures (failures per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE 1 Further explanation of modes of operation can be found in 3.2.39.

NOTE 2 The SIL is defined numerically so as to provide an objective measure for comparison of alternate designs and solutions. However, it is recognized that, given the current state of knowledge, many systematic causes of failure can only be assessed qualitatively.

NOTE 3 The required average frequency of dangerous failures for a continuous or demand mode SIF is determined by considering the risk caused by failure of the continuous or demand mode SIF together with the failures of other devices that lead to the same risk, taking into consideration the risk reduction provided by other protection layers.

9.2.5 In cases where the allocation process results in a risk reduction requirement of $>10\ 000$ or average frequency of dangerous failures $<10^{-8}$ per hour for a single SIS or multiple SISs or SIS in conjunction with a BPCS protection layer, there shall be a reconsideration of the application (e.g., process, other protection layers) to determine if any of the risk parameters can be modified so that the risk reduction requirement of $>10\ 000$ or average frequency of dangerous failures $<10^{-8}$ per hour is avoided. The review shall consider whether:

- the process or vessels/pipe work can be modified to remove or reduce hazards at the source;
- additional safety-related systems or other risk reduction means, not based on instrumentation, can be introduced;
- the severity of the consequence can be reduced, e.g., reducing the amount of hazardous material;

- the likelihood of the specified consequence can be reduced e.g., reducing the likelihood of the initiating source of the hazardous event.

NOTE Applications which require the use of a single SIF with a risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour need to be avoided because of the difficulty of achieving and maintaining such high levels of performance throughout the SIS safety life-cycle. Risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour can require high levels of competence and high levels of coverage for all factory acceptance testing, proof testing, verification, and validation activities.

9.2.6 If after further consideration of the application and confirmation that a risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour is still required, then consideration should be given to achieving the safety integrity requirement using a number of protection layers (e.g., SIS or BPCS) with lower risk reduction requirements. If the risk reduction is allocated to multiple protection layers then such protection layers shall be independent from each other or the lack of independence shall be assessed and shown to be sufficiently low compared to the risk reduction requirements. The following factors shall be considered during this assessment:

- common cause of failure of SIS and the cause of demand;

NOTE 1 The extent of the common cause can be assessed by considering the diversity of all devices where failure could cause a demand and all devices of the BPCS protection layer and/or the SIS used for risk reduction.

NOTE 2 An example of common cause between the SIS and the cause of demand is if loss of process control through sensor fault or failure can cause a demand and the sensor used for control is of the same type as the sensor used for the SIS.

- common cause of failure with other protection layers providing risk reduction;

NOTE 3 The extent of the common cause can be assessed by considering the diversity of all devices of the BPCS protection layer and/or the SIS used to achieve the risk reduction requirements.

NOTE 4 An example of common cause between SISs providing risk reduction is when two separate and independent SISs with diverse measurements and diverse logic solvers are used but the final actuation devices are two shut off valves of similar types or a single shut off valve actuated by both SISs.

- any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times;

NOTE 5 Even if the protective layers are diverse then synchronous proof testing will reduce the overall risk reduction achieved and this can be a significant factor impeding achievement of the necessary risk reduction for the hazardous event.

NOTE 6 When high levels of risk reduction are required and proof tests are desynchronised according to Note 5 then the dominant factor is normally common cause failure even if multiple independent protection layers are used to reduce risk. Dependency within and between protection layers providing risk reduction for the same hazardous event can be assessed and shown to be sufficiently low.

9.2.7 If a risk reduction requirement $>10\,000$ or average frequency of dangerous failures $<10^{-8}$ per hour is to be implemented, whether allocated to a single SIS or multiple SIS or SIS in conjunction with a BPCS protection layer, then a further risk assessment shall be carried out using a quantitative methodology to confirm that the safety integrity requirements are achieved. The methodology shall take into consideration dependency and common cause failures between the SIS and:

- any other protection layer whose failure would place a demand on it;
- any other SIS reducing the likelihood of the hazardous event;
- any other risk reduction means that reduce the likelihood of the hazardous event (e.g., safety alarms).

9.2.8 If the risk reduction required for a hazardous event is allocated to multiple SIFs in a single SIS, then the SIS shall meet the overall risk reduction requirement.

9.2.9 The results of the allocation process shall be recorded so that the SIFs are described in terms of the functional needs of the process, e.g., the actions to be taken, set points, reaction times, activation delays, fault treatment, valve closure requirements, and in terms of the risk reduction requirements.

NOTE This description can be in an unambiguous logical form and can be referred to as the process requirements specification or the safety description. The description can make the intent and the approach used in the allocation process clear. The process requirements specification is used as input information for the SRS covered in Clause 10 and can be sufficiently detailed to ensure adequate specification of the SIS and its devices. For example, the description can include the set-points for sensors, the process safety time available for response, and the valve closure requirements.

9.3 Requirements on the basic process control system as a protection layer

9.3.1 The basic process control system may be claimed as a protection layer as shown in Figure 9.

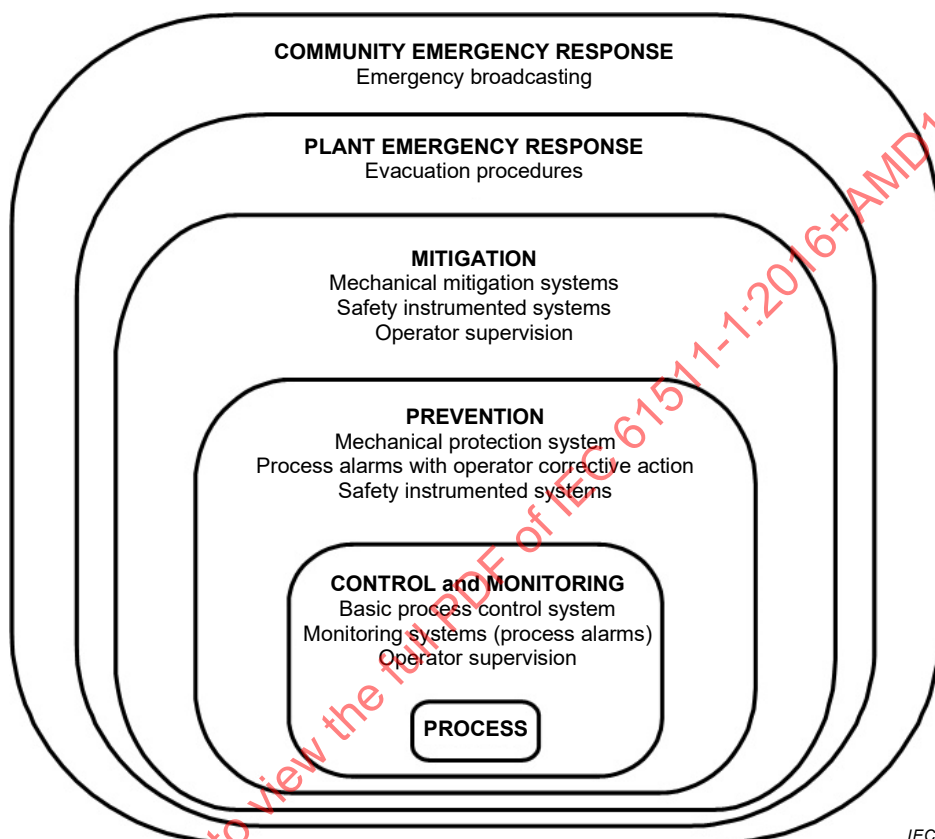


Figure 9 – Typical protection layers and risk reduction means

9.3.2 The risk reduction claimed for a BPCS protection layer shall be ≤ 10 .

NOTE Consideration can be given to the fact that a BPCS may also be an initiating source for the demand on the protection layer.

9.3.3 If the risk reduction claimed for a BPCS protection layer is > 10 , then the BPCS shall be designed and managed to the requirements within the IEC 61511 series.

9.3.4 If it is not intended that the BPCS conform to the IEC 61511 series, then:

- no more than one BPCS protection layer shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is the initiating source for the demand on the protection layer; or
- no more than two BPCS protection layers shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is not the initiating source of the demand.

NOTE The identified BPCS protection layer can consist of one BPCS as the initiating source for the demand (see 8.2.2) and a second independent BPCS protection layer (see 9.3.2 and 9.3.3) or up to two independent BPCS protection layers when the initiating source is not related to BPCS failure.

9.3.5 When 9.3.4 applies, each BPCS protection layer shall be independent and separate from the initiating source and from each other to the extent that the claimed risk reduction of each BPCS protection layer is not compromised.

NOTE 1 The assessment of separation and independence can consider what is necessary to achieve the risk reduction, e.g., the central processing units (CPU), input/output modules, relays, field devices, application programming, networks, program database, engineering tools, human machine interface, by-pass tools and other devices.

NOTE 2 A hot backup controller is not considered to be independent of the primary controller because it is subject to common cause failure (for example, hot backup controllers have components that are common to both the primary and the backup controller, such as the backplane, firmware, diagnostics, transfer mechanisms and undetected dangerous failures).

9.4 Requirements for preventing common cause, common mode and dependent failures

9.4.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between:

- protection layers;
- protection layers and the BPCS.

are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.

NOTE A definition of dependent failure is provided in 3.2.12.

9.4.2 The assessment shall consider the following:

- independence between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS.

NOTE 1 Common causes from the process can be addressed. Plugging of relief valves may cause the same problems as plugging of sensors in a SIS.

NOTE 2 Independence and physical separation can be addressed. A Human Machine Interface, SIS/BPCS networks or bypass means can cause common cause failure.

10 SIS safety requirements specification (SRS)

10.1 Objective

The objective of Clause 10 is to specify the requirements for the SIS, including any application programs and the architecture of the SIS.

10.2 General requirements

The safety requirements shall be derived from the allocation of SIF and from those requirements identified during H&RA. The SIS requirements shall be expressed and structured in such a way that they are

- clear, precise, verifiable, maintainable and feasible;
- written to aid comprehension and interpretation by those who will utilise the information at any phase of the safety life-cycle.

10.3 SIS safety requirements

10.3.1 The objective of 10.3 is to address issues that shall be considered when developing the SIS safety requirements.

10.3.2 These requirements shall be sufficient to design the SIS and shall include a description of the intent and approach applied during the development of the SIS safety requirements as applicable:

- a description of all the SIF necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative);
- a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);
- requirements to identify and take account of common cause failures;
- a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated;
- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system);
- the assumed sources of demand and demand rate on each SIF;
- requirements relating to proof test intervals;
- requirements relating to proof test implementation;
- response time requirements for each SIF to bring the process to a safe state within the process safety time;
NOTE See IEC 61511-2:2016 for further discussion of process safety time.
- the required SIL and mode of operation (demand/continuous) for each SIF;
- a description of SIS process measurements, range, accuracy and their trip points;
- a description of SIF process output actions and the criteria for successful operation, e.g., leakage rate for valves;
- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives for each SIF;
- requirements for manual shutdown for each SIF;
- requirements relating to energize or de-energize to trip for each SIF;
- requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element resets after trips);
- maximum allowable spurious trip rate for each SIF;
- failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shutdown);
- any specific requirements related to the procedures for starting up and restarting the SIS;
- all interfaces between the SIS and any other system (including the BPCS and operators);
- a description of the modes of operation of the plant and requirements relating to SIF operation within each mode;
- the application program safety requirements as listed in 10.3.3;
- requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared;
- the specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors;

- the mean repair time which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints;
- identification of the dangerous combinations of output states of the SIS that need to be avoided;
- identification of the extremes of all environment conditions that are likely to be encountered by the SIS during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;
- identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIFs may be required to support these process operating modes;
- definition of the requirements for any SIF necessary to survive a major accident event, e.g., time required for a valve to remain operational in the event of a fire.

10.3.3 The application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS. The application program safety requirements may be located in the SRS or in a separate document (e.g., application program requirements specification). The input to the application program safety requirements for each SIS subsystem shall include:

- a) the specified safety requirements of each SIF, including sensor voting, etc.;
- b) the requirements resulting from the SIS architecture and the safety manual such as limitations and constraints of the hardware and embedded software;
- c) any requirements of safety planning arising from 5.2.4.

10.3.4 The application program safety requirements shall be specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS.

10.3.5 The application program safety requirements specification shall be sufficiently detailed to allow the design and implementation to achieve the required functional safety and to allow a functional safety assessment to be carried out. The following shall be considered:

- the SIFs supported by the application program and their SIL;
- real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a specified time period;
- program sequencing and time delays if applicable;
- equipment and operator interfaces and their operability;
- all relevant modes of operation of the process as specified in the SRS;
- action to be taken on bad process variable such as sensor value out of range, excessive range of change, frozen value, detected open circuit, detected short circuit;
- functions enabling proof testing and automated diagnostic tests of external devices (e.g., sensors and final elements) performed in the application program;
- application program self-monitoring (e.g., application driven watch-dogs and data range validation);
- monitoring of other devices within the SIS (e.g., sensors and final elements);
- any requirements related to periodic testing of SIF when the process is operational;
- references to the input documents (e.g., specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS);

- the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;
- process dangerous states (for example closure of two isolation gas valves at the same time that could lead to pressure fluctuations thus leading to a dangerous state) generated by the application program shall be identified and avoided;
- definitions of process variable validation criteria for each SIF.

10.3.6 The application program safety requirements specification shall be expressed and structured in such a way that they:

- describe the intent and approach underpinning the application program safety requirements;
- are clear and understandable to those who will utilize the document at any phase of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by all users (e.g., plant operators, maintenance personnel, application programmers);
- are verifiable, testable, modifiable;
- are traceable back through all deliverables including the detailed design documents, the SRS and the H&RA that identifies the required SIF and SIL.

11 SIS design and engineering

11.1 Objective

The objective of the requirements of Clause 11 is to design one or multiple SIS to provide the SIF and meet the specified integrity requirements (e.g., SIL, associated risk reduction, PFD and /or PFH).

11.2 General requirements

11.2.1 The design of the SIS shall be in accordance with the SIS safety requirements specifications, taking into account all the requirements of Clause 11.

11.2.2 Where the SIS is to implement both SIFs and non-SIFs then all the hardware, embedded software and application program that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL of any of the SIFs it can impact.

11.2.3 Where the SIS is to implement SIF of different SIL, then the shared or common hardware and embedded software and application program shall conform to the highest SIL.

NOTE Embedded software or application programs of different SIL could coexist in the same device provided it can be demonstrated that the SIF of lower SIL cannot negatively affect the SIF of the higher SIL.

11.2.4 If it is intended not to qualify the BPCS to the IEC 61511 series, then the SIS shall be designed to be separate and independent from the BPCS to the extent that the safety integrity of the SIS is not compromised.

NOTE 1 Operating information can be exchanged but not compromise the functional safety of the SIS.

NOTE 2 Devices of the SIS can also be used for functions of the BPCS if it can be demonstrated that a failure of the BPCS does not compromise the SIF of the SIS.

11.2.5 Requirements for operability, maintainability, diagnostics, inspection and testability shall be addressed during the design of the SIS in order to reduce the likelihood of dangerous failures.

11.2.6 The design of the SIS shall take into account human capabilities and limitations and be suitable for the tasks assigned to operators and maintenance staff. The design of operator interfaces shall follow good human factors practice and shall accommodate the likely level of training that operators should receive.

NOTE 1 For example, human factor studies may be necessary if operation requires data entry of limits or other operator input on a regular basis.

11.2.7 The SIS shall be designed in such a way that once it has placed the process in a safe state, the process shall remain in the safe state until a reset has been initiated unless otherwise directed by the SRS.

11.2.8 Manual means (e.g., emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the SRS.

11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependency between the SIS and BPCS, and the SIS and other protection layers.

11.2.10 A device used by the BPCS shall not be used by the SIS where a failure of that device may result in both a demand on the SIF and a dangerous failure of the SIF, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand on the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared device because if the shared device fails, a demand will be created immediately to which the SIS may not be capable of responding. For that reason, additional analysis can be necessary in these cases to ensure that the dangerous failure rates of the shared devices are sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.

11.2.11 For any SIS device that on loss of utility (e.g., electrical power, air, hydraulics or pneumatic supply) does not fail to the safe state, loss of utility and SIS circuit integrity shall be detected and alarmed (e.g., end-of-line monitoring, supply pressure measurement, hydraulic or pneumatic pressure monitoring) and action taken according to 11.3.

NOTE 1 Utility integrity can be improved through using a supplementary supply (e.g., battery back-up, uninterruptible power supplies, air reservoir, hydraulic accumulator, second gas supply).

NOTE 2 The loss of a utility is likely to affect multiple SIFs and, possibly, multiple SISs.

11.2.12 The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

NOTE Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

11.2.13 A safety manual covering operation, maintenance, fault detection and constraints associated with the SIS shall be available covering the intended configurations of the devices and the intended operating environment.

11.2.14 All communications used to implement a SIF shall be established using techniques appropriate for safety applications to meet the required SIL.

11.3 Requirements for system behaviour on detection of a fault

11.3.1 When a dangerous fault in a SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation. If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken. Where the compensating measures depend on an operator taking specific action in response to an alarm (e.g., opening or closing a valve) then the alarm shall be considered part of the SIS.

NOTE 1 The specified action (fault reaction) required to achieve or maintain a safe state of the process can be specified in the SRS (see 10.3.1). It can consist of the safe shutdown of the process or of that part of the process which relies on the faulty SIS for risk reduction.

NOTE 2 The compensating measures required for continued safe operations can depend on safety integrity requirements, the tolerable risk associated with the hazardous event, the hardware fault tolerance of the SIS, the anticipated MRT and the availability of any other layers of protection. In some cases it can be adequate to ensure action is taken to ensure repair of the dangerous failure within the assumed MPRT in the calculation of the PFDavg but in other cases it can be judged necessary to provide other measures to compensate for the reduced risk reduction until the SIS is fully restored. See also 16.2.3.

11.3.2 Where any dangerous fault in an SIS is brought to the attention of an operator by an alarm then the alarm shall be subject to appropriate proof testing and management of change.

11.4 Hardware fault tolerance

11.4.1 The SIS shall have a minimum HFT with respect to each SIF it implements.

NOTE This does not exclude the possibility that the HFT may be reduced below the minimum requirement at certain times during operation of the system following the occurrence of faults.

11.4.2 When the SIS can be split into independent SIS subsystems (e.g. sensors, logic solvers and final elements), then the HFT can be assigned at the SIS subsystem level.

11.4.3 The HFT of the SIS or its SIS subsystems shall be in accordance with;

- 11.4.5 to 11.4.9 of clause 11 or,
- the requirements of 7.4.4.2 (route 1H) of IEC 61508-2:2010 or,
- the requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.

NOTE The route developed in IEC 61511 is derived from route 2_H of IEC 61508-2:2010.

11.4.4 When determining the achieved HFT, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements. Any such fault exclusions shall be justified and documented.

NOTE Further information about fault exclusion can be found in ISO13849-1:2006 and ISO13849-2:2012.

11.4.5 The minimum HFT for a SIS (or its SIS subsystems) implementing a SIF of a specified SIL shall be in accordance with Table 6 and if appropriate 11.4.6 and 11.4.7.

NOTE The HFT requirements in Table 6 represent the minimum system or, where relevant, the SIS subsystem redundancy. Depending on the application, device failure rate and proof-testing interval, additional redundancy can be required to satisfy the failure measure for the SIL of the SIF according to 11.9.

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

11.4.6 For a SIS or SIS subsystem that does not use FVL or LVL programmable devices and if the minimum HFT as specified in Table 6, would result in additional failures and lead to decreased overall process safety, then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.

NOTE Fault tolerance is the preferred solution to achieve the required confidence that a robust architecture has been achieved. When 11.4.6 applies, the purpose of the justification is to demonstrate that the proposed alternative architecture provides an equivalent or better solution. This may vary depending on the application and/or the technology in use; examples 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 diversified 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.

11.4.7 If a fault tolerance equal to zero results from applying 11.4.6, the justification required by 11.4.6 shall provide evidence that the related dangerous failure modes can be excluded, in accordance with 11.4.4 including consideration of the potential for systematic failures.

11.4.8 FVL and LVL programmable devices shall have diagnostic coverages not less than 60 %.

11.4.9 Reliability data used in the calculation of the failure measure shall be determined by an upper bound statistical confidence limit of no less than 70 %.

11.5 Requirements for selection of devices

11.5.1 Objectives

The objectives of the requirements of 11.5 are to:

- specify the requirements for the selection of devices which are to be used as part of the SIS;
- specify the requirements to enable a device to be integrated in the architecture of a SIS;
- specify acceptance criteria for devices in terms of associated SIF and safety integrity requirements.

11.5.2 General requirements

11.5.2.1 Devices selected for use as part of a SIS with a specified SIL shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010 and/or 11.5.3 through 11.5.6, as appropriate.

NOTE Devices assessed against IEC 61508-2:2010 and IEC 61508-3:2010 can be applied in accordance with the requirements for systematic capability in IEC 61508-2:2010.

11.5.2.2 All devices shall be suitable for the operating environment as determined through consideration of the manufacturer's documentation, the constraints within the SRS and the reliability parameters assumed in respect of 11.9. Suitability of the selected devices shall always be considered in the context of the operating environment.

NOTE Devices may exhibit different failure rates dependent on the operating environment and mode of operation. Failure rate data available from manufacturers may not be valid in all applications. For example, the failure rate and failure mode distribution can be different for a valve that is frequently exercised versus one that stands still for long periods of time.

11.5.3 Requirements for the selection of devices based on prior use

11.5.3.1 Appropriate evidence shall be available that the devices are suitable for use in the SIS.

NOTE 1 The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 2 Level of detail of the evidence can be in accordance with the complexity of the considered device.

NOTE 3 A prior use evaluation involves gathering documented information concerning the device performance in a similar operating environment. Prior use demonstrates the functionality and integrity of the installed device, including the process interfaces, full device boundary, communications, and utilities. The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity.

NOTE 4 Prior use data can contribute to a database for the calculation of hardware failure rates as described in 11.9.3.

11.5.3.2 The evidence of suitability shall include the following:

- consideration of the manufacturer's quality, management and configuration management systems;
- adequate identification and specification of the devices;
- demonstration of the performance of the devices in similar operating environments;

NOTE 1 In the case of field devices (e.g., sensors and final elements) fulfilling a given specification, the behaviour of the device in the operating environment is usually identical in safety and non-safety applications. Therefore, evidence of the performance of similar devices in non-safety applications can also be used to satisfy this requirement.

- the volume of the operating experience.

NOTE 2 For field devices, information relating to operating experience is mainly recorded in the user's list of equipment approved for use in their facilities, based on an extensive history of successful performance in safety and non-safety applications, and on the elimination of equipment not performing in a satisfactory manner. The list of field devices can be used to support claims of experience in operation, provided that:

- the list is updated and monitored regularly;
- field devices are only added when sufficient operating experience has been obtained;
- field devices are removed when they show a history of not performing in a satisfactory manner;
- the operating environment is included in the list where relevant.

NOTE 3 Device performance is highly affected by the operating environment. It is generally recommended that selection of devices can be based on adequate performance of an installed sufficient number of devices in multiple installations for a sufficient operating time. The gained experience can allow time to reveal early failures, such as those related to specification, handling, installation, and commissioning.

NOTE 4 The amount of operational experience to gain credible statistical reliability data is typically much higher compared to the operational experience necessary to get evidence of prior use.

11.5.3.3 All devices selected on the basis of prior use shall be identified by a specified revision number and shall be under the control of a management of change procedure. In the case of a change being made to the device, the continued validity of the evidence of prior use shall be justified by evaluating the significance of the change made.

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

11.5.4.1 For SIL 1, SIL 2, and SIL 3, the requirements of 11.5.2 and 11.5.3 apply, together with the following subclauses.

11.5.4.2 All configuration options of the device possibly influencing safety shall be identified and considered. It is important to check that wherever specific settings are not defined that the default settings of the device are confirmed to be appropriate. Unused features of the devices shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required SIF.

11.5.4.3 For the specific configuration and operating environment of the device, the evidence of suitability shall consider:

- characteristics of input and output signals;
- modes of use;
- functions and configurations used;
- prior use in similar operating environments.

11.5.4.4 In addition, for SIL 3 applications, an assessment of the FPL device shall be carried out to show that:

- the FPL device is both able to perform the required functions and that prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous

event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;

- appropriate standards for hardware and software have been applied;
- the FPL device has been used or tested in configurations representative of the intended operational profiles.

11.5.5 Requirements for selection of LVL programmable devices based on prior use

11.5.5.1 The following requirements apply to PE devices used in SISs which implement SIL 1 or SIL 2 SIFs.

11.5.5.2 The requirements of 11.5.4 apply.

11.5.5.3 Where there is any difference between the operating environment of a device as experienced previously, and the operating environment of the device when used within the SIS, then any such differences shall be identified and there shall be an assessment based on analysis and testing, as appropriate, to show that the likelihood of systematic faults when used in the SIS is sufficiently low.

11.5.5.4 The operating experience considered necessary to justify the suitability shall be determined taking into account:

- the SIL of the SIF;
- the complexity and functionality of the devices.

11.5.5.5 For SIL 1 or 2 applications, a safety configured PE logic solver may be used provided that all the following additional provisions are met:

- understanding of unsafe failure modes;
- use of techniques for safety configuration that address the identified failure modes;
- the embedded software has a good history of use for safety applications;
- protection against unauthorized or unintended modifications.

NOTE A safety configured PE logic solver is a general purpose industrial grade PE logic solver which is specifically configured by the OEM, a systems engineer or the end-user for use in safety applications.

11.5.5.6 A formal assessment of any PE logic solver used in a SIL 2 application shall be carried out to show that:

- it is both able to perform the required functions and that prior use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the SIS, due to either random hardware failures or systematic faults in hardware or software;
- measures are implemented to detect faults during program execution and initiate appropriate responses; these measures shall comprise all of the following:
 - program sequence monitoring;
 - protection of code against modifications or failure detection by on-line monitoring;
 - failure assertion or diverse programming;
 - range check of variables or plausibility check of values;
 - modular approach;
 - appropriate coding standards have been used for the embedded and utility software;
 - testing in typical configurations, with test cases representative of the intended operational profiles;
 - trusted verified software modules and components have been used;
 - the system has undergone dynamic analysis and testing;

- the system does not use artificial intelligence or dynamic reconfiguration;
- documented fault-insertion testing (negative testing) has been performed.

11.5.6 Requirements for selection of FVL programmable devices

When the applications are programmed using a FVL, the PE device shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010.

11.6 Field devices

11.6.1 Field devices shall be selected and installed to minimize failures that could result in inaccurate information due to conditions arising from the operating environment. Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, coking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse lines.

11.6.2 Energize to trip circuits shall apply means to ensure circuit and power supply integrity.

NOTE 1 An example of such means is an end-of-line monitor, where a pilot current is continuously monitored to detect circuit continuity and where the pilot current is not of sufficient magnitude to affect proper I/O operation.

NOTE 2 Additional requirements for loss of power can be found in 11.2.11.

11.6.3 Smart sensors shall be write-protected to prevent inadvertent modification, unless appropriate safety review (e.g., H&RA) allows the use of read/write.

NOTE The review can take into account human factors such as failure to follow procedures.

11.7 Interfaces

11.7.1 General

Interfaces to the SIS can include, but are not limited to:

- operator interface(s);
- maintenance/engineering interface(s);
- communication interface(s).

11.7.2 Operator interface requirements

11.7.2.1 Where the SIS operator interface is via the BPCS operator interface, account shall be taken of credible failures that may occur in the BPCS operator interface.

NOTE This can include preparing plans to enable an orderly safe shutdown in the event of total failure of the operational displays.

11.7.2.2 The design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while hazards are present. If the design does require the use of operator actions, the design should include facilities for protection against operator error.

NOTE If the operator has to select a particular option, there can be a confirmation step.

11.7.2.3 Bypass switches or means shall be protected to prevent unauthorized use (e.g., by key locks or passwords in conjunction with effective management controls).

NOTE Consideration can be given to enforcing time limits on bypass operation and to limiting the number of bypasses that can be active at any one time.

11.7.2.4 The SIS status information that is critical to maintaining the SIF shall be available as part of the operator interface. This information may include:

- where the process is in its sequence;
- indication that SIS protective action has occurred;
- indication that a protective function is bypassed;
- indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- status of sensors and final elements;
- the loss of energy where that energy loss impacts safety;
- the results of diagnostics;
- failure of environmental conditioning equipment which is necessary to support the SIS.

11.7.2.5 The SIS operator interface design (see 11.7.2.7) shall be such as to prevent changes to the SIS application program.

11.7.2.6 Where information is transferred from the BPCS to the SIS, systems, equipment or procedures shall be applied to confirm that the correct information has been transferred and that the safety integrity of the SIS is not compromised.

NOTE The systems, equipment or procedures used can include control over selective writing from the BPCS to specific SIS variables.

11.7.2.7 The design of the SIS operator interface via the BPCS operator interface shall be such that provision of incorrect information or data from the BPCS to the SIS shall not compromise safety.

11.7.3 Maintenance/engineering interface requirements

11.7.3.1 The design of the SIS maintenance/engineering interface shall ensure that any failure of this interface shall not adversely affect the ability of the SIS to carry out the required SIFs. This may require disconnecting of maintenance/engineering interfaces, such as programming panels, during normal SIS operation.

11.7.3.2 The maintenance/engineering interface shall provide the following functions with access security protection to each:

- SIS mode of operation, program, data, means of disabling alarm communication, test, bypass, maintenance;
- SIS diagnostics, voting and fault handling services;
- add, delete, or modify application program;
- data necessary to troubleshoot the SIS;
- where bypasses are required they should be installed such that alarms and manual shutdown facilities are not disabled.

11.7.3.3 The maintenance/engineering interface shall not be used as the operator interface.

11.7.3.4 Enabling and disabling the read-write access shall be carried out only by a configuration management process using the maintenance/engineering interface with appropriate documentation and security measures such as authentication and user secure channels.

11.7.4 Communication interface requirements

11.7.4.1 The design of any SIS communication interface shall ensure that any failure of the communication interface shall not adversely affect the ability of the SIS to achieve or maintain a safe state of the process.

11.7.4.2 When the SIS is able to communicate with the BPCS and peripherals, the communication interface, BPCS, or peripherals shall not adversely impact any of the SIFs within the SIS.

11.7.4.3 The communication interface shall be sufficiently robust to withstand electro-magnetic interference including power surges without causing a dangerous failure of the SIS.

11.7.4.4 The communication interface shall be suitable for communication between devices referenced to different electrical ground potentials.

NOTE An alternate medium (e.g., fibre optics) can be required.

11.8 Maintenance or testing design requirements

11.8.1 The design shall allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.

NOTE The term “end-to-end” means from process fluid at sensor end to process fluid at actuation end.

11.8.2 When on-line proof testing is required, test facilities shall be an integral part of the SIS design.

11.8.3 When test or bypass facilities are included in the SIS, they shall conform with the following:

- The SIS shall be designed in accordance with the maintenance and testing requirements defined in the SRS;
- The operator shall be alerted to the bypass of any portion of the SIS via an alarm or operating procedure.

11.8.4 The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.

11.8.5 Compensating measures that ensure continued safe operation shall be provided in accordance with 11.3 when the SIS is in bypass (repair or testing).

11.8.6 Forcing of inputs and outputs in PE SIS shall not be used as a part of application program(s), operating procedure(s) and maintenance (except as noted below).

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

11.9 Quantification of random failure

11.9.1 The calculated failure measure of each SIF shall be equal to, or better than, the target failure measure related to the SIL as specified in the SRS. This shall be determined by calculation.

NOTE In complex applications, the hazardous event frequency can be used as an alternative to the target failure measures (e.g., where different demand causes have different safety integrity requirements or where non-independent SISs act in sequence).

11.9.2 The calculated failure measure of each SIF due to random failures shall take into account all contributing factors including the following:

- a) the architecture of the SIS and of its SIS subsystems where relevant as they relate to each SIF under consideration;

- b) the estimated failure rate related to each failure mode, due to random hardware failures, which would contribute to a dangerous failure of the SIS but which are detected by diagnostic tests;
- c) the estimated failure rate related to each failure mode, due to random hardware failures, which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests but which are detected by proof tests;
- d) the estimated failure rate related to each failure mode, due to random hardware failure, which would contribute to a dangerous failure of the SIS which are undetected by the diagnostic tests and undetected by proof tests;
- e) the susceptibility of the SIS to failures caused by the proof tests themselves;
- f) the susceptibility of the SIS to common cause failures;
- g) the diagnostic coverage of any periodic diagnostic tests, the associated diagnostic test interval and the probability of failure of the diagnostic facilities;
- h) the coverage of any periodic proof tests, the associated proof test procedure and the reliability for the proof test facilities and procedure;
- i) the repair times for detected failures and the state of the SIS during repairs (on line or off line);
- j) the estimated dangerous failure rate of any communication process in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);
- k) the estimated likelihood that operator response would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);
- l) the reliability of any utility necessary for the SIS.

NOTE Several modelling approaches are available and the most appropriate approach is a matter for the analyst and can depend on the circumstances. Available means include (see IEC 61508-6:2010, annex B):

- cause consequence analysis;
- reliability block diagrams;
- fault-tree analysis;
- Markov models;
- Petri nets models.

The probabilistic calculations can be performed analytically or by numerical simulation (e.g., Monte Carlo simulation).

11.9.3 The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified and shall be based on field feedback from similar devices used in a similar operating environment.

NOTE 1 This includes user collected data, vendor/provider/user data derived from data collected on devices, data from general field feedback reliability databases, etc. In some cases, engineering judgement can be used to assess missing reliability data or evaluate the impact on reliability data collected in a different operating environment.

NOTE 2 The lack of reliability data reflective of the operating environment is a recurrent shortcoming of probabilistic calculations. End-users can organize relevant device reliability data collections in accordance with IEC 60300-3-2:2004 or ISO 14224:2006 to improve the implementation of the IEC 61511 series.

NOTE 3 Vendor data based on returns can be restricted to a population where there is full knowledge of the operational environment and fully recorded in accordance with IEC 60300-3-2:2004 or ISO 14224:2006. The user can also record the operational environment for the SIF and be able to demonstrate that the vendor's operational environment data matches the environment of the SIF.

11.9.4 The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.

NOTE 1 The reliability data uncertainties can be evaluated according to the amount of field feedback (less field feedback results in more uncertainty) or/and exercise of expert judgement. Published standards (IEC 60605-4), Bayesian approaches, engineering judgement techniques, etc. can be used to estimate the reliability data uncertainties.

NOTE 2 The following techniques can be used for calculating the failure measures (more information can be found in IEC 61511-2:2016):

- use of an upper bound confidence of 70 % for each input reliability parameter instead of its mean in order to obtain conservative point estimations of the failure measures, or;
- use the probabilistic distributions functions of input reliability parameters, perform Monte Carlo simulations to obtain an histogram representing the distribution of the failure measure and assess a conservative value from this distribution (e.g., that there is a 90 % confidence that the true failure measure is better than the value calculated).

11.9.5 If, for a particular design, the target failure measure for the relevant SIF is not achieved then:

- a) identify the devices or parameters contributing most to the failure measure;

NOTE Fault tree cut-set analysis can be useful here.

- b) evaluate the effect of possible improvement measures on the identified devices or parameters (e.g., more reliable devices, additional defences against common mode failures, increased diagnostic or proof test coverage, increased redundancy, reduced proof test interval, staggering tests, etc.);
- c) select and implement improvement measures to establish the new result;
- d) compare the new result to the target failure measure and repeat the steps a) to d) until the target failure measure is achieved in a conservative manner.

12 SIS application program development

12.1 Objective

The objective of Clause 12 is to define the requirements for the development of the application program.

12.2 General requirements

12.2.1 The application program of the SIS shall be in accordance with the application program safety requirements (see 10.3.3) and all the requirements of this clause for all SIL up to and including SIL 3.

12.2.2 The application programmer shall review the information in the SRS and the application program safety requirements to ensure that the requirements are comprehensive, unambiguous, understandable and consistent. Any deficiencies in the application program safety requirements shall be identified and resolved, and if changes are made to the application program safety requirements, an impact analysis shall be carried out.

12.2.3 The IEC 61511 series addresses programming in Limited Variability Languages (LVL) and the use of devices using Fixed Program Languages (FPL). The IEC 61511 series does not address Full Variability Language (FVL) and the IEC 61511 series does not address SIL 4 application programming. Where function blocks are written in FVL then these shall be developed and modified under IEC 61508-3:2010.

12.2.4 Where the application program of the SIS is to implement both safety and non-safety functions, then all of the application program shall be treated as part of the SIS and shall comply with this standard and in addition, it shall be shown through assessment and test that the non-safety functions cannot interfere with the safety functions.

12.2.5 The application program shall be designed in such a way as to ensure that once the SIS has placed the process in a safe state, the process remains in the safe state, including under loss of power conditions and on power restoration, until a reset has been initiated unless otherwise directed by the SRS.

NOTE 1 If the SIF does not have a reset then there can be a documented engineering argument as to why it is acceptable to reinitiate the process without requiring the safe delay a reset would impose.

NOTE 2 More information can be found in 11.2.7.

12.2.6 During SIS start-up (or power up) the application program shall ensure that safety outputs remain in the safe state (typically de-energized state) until a reset has been initiated unless otherwise directed by the SRS.

12.2.7 The application program shall be designed in such a way that all parts of the application program are executed on every application program scan unless there is a specific alternate requirement that is supported in the safety manual. Process safety time requirements shall be considered when establishing application program scanning requirements.

12.2.8 The SIS application program and data shall be subject to modification, revision control, version management, back-up and restoration procedures.

12.2.9 The SIS application program safety life cycle planning shall address the following aspects:

- SIS safety life-cycle phases and activities that are to be applied during the design and development of the application program. These requirements include the application of measures and techniques, which are intended to avoid errors in the application program and to control failures which may occur;
- information relating to the application program validation to be passed to the organization carrying out the SIS integration;
- preparation of information and procedures needed by the user for operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications of the application program.

12.3 Application program design

12.3.1 An application program design shall address all SIS logic including all process operating modes for each SIF.

12.3.2 The input to the application program design shall be the SRS including the application program requirements (see Clause 10), the SIS architecture (see Clause 11) and the means and tools for developing the application program design (see 12.6). The application program design shall be consistent with and traceable back to the SRS.

12.3.3 The application program design shall allow an assessment of functional safety to be carried out.

12.3.4 The application program design and its decomposition into modules if applicable, shall address how the requirements are to be implemented, including the following as appropriate:

- the functions that enable the process to achieve or maintain a safe state;
- the specification of all identified application program components, and the description of connections and interactions between identified components;
- the timing constraints associated with the application program functions and their implementation in program scan time(s);
- a detailed description of the standard library modules (function blocks) being used;
- a detailed description of the application specific modules (function blocks) being used;
- a description of the way memory allocation has been achieved;
- the list of global variables used and the way in which their integrity is protected;

- identification of all non-SIF and the interfaces to non-safety related parts of the application program, to ensure that they cannot affect the proper operation of any SIF;
- definition of input and output interfaces, including tag listings and the associated data types;
- details of the data exchanged between the SIS application program and the operator interfaces;
- details of the data exchanged between the SIS application program and the BPCS and peripherals such as printers, data storage, etc.;
- how external and internal diagnostic information will be processed and logged;
- detailed description of how the operation and maintenance interfaces are implemented, including the way in which alarms are prioritised, indicated and accepted;
- a detailed description of any application level diagnostics that may be implemented such as external watch dogs, application data integrity checking, sensor validation to meet the required SIL;
- system configuration checks including the existence and accessibility of expected hardware devices and software modules;
- how the complexity in the application program design is minimised e.g., through use of modular design and simple functionality;
- functions related to the detection, annunciation and management of faults in SIS subsystems;
- functions related to the periodic testing of SIF on-line;
- functions related to the periodic testing of SIF off-line;
- functions that allow maintenance of the SIS to be carried out safely;
- references to documents on which the application program design specification is based.

12.3.5 The application program design shall ensure:

- completeness with respect to the SRS and its intended purpose;
- correctness with respect to the SRS and its intended purpose;
- freedom from ambiguity, i.e., clear to those who will utilize the document at any stage of the SIS safety life-cycle: this includes the use of terminology and descriptions which are unambiguous and understood by plant operators and system maintainers, as well as the application programmers;
- freedom from design faults.

12.4 Application program implementation

12.4.1 The application program development methodology shall comply with the development tools and restrictions given by the manufacturer of the SIS PE subsystem on which the application program shall be used.

12.4.2 The following information shall be contained in the application program or related documentation:

- a) the application program originator;
- b) a description of the purpose of the application program;
- c) the versions of the safety manuals that were used;
- d) identification of the dependency of each SIF on the parts (modules) of the application program;
- e) traceability to the application program safety requirements specification;
- f) identification of each SIF and its SIL;

- g) identification and description of the symbols used, including logic conventions, standard library functions, application library functions;
- h) identification of the SIS logic solver input and output signals;
- i) where the overall SIS utilises communications, a description of the communications information flow;

NOTE An example would be where a SIF uses several logic solvers.

- 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 sub-systems and any limitations imposed by scan times;
- k) If required by the SRS, the means by which:
 - the correctness of field data is ensured, (e.g., comparison between analog sensors to improve the diagnostic coverage);
 - the correctness of data sent over a communication link is ensured (e.g., when communicating from an HMI, before implementation of a command an 'ack' or 'acknowledge' is transmitted);
 - communications are made secure (e.g., cyber security measures);
- l) version identification and a history of changes.

12.4.3 If previously developed application program library functions are to be used as part of the design, their suitability shall be justified and based upon:

- compliance to IEC 61508; if proven-in-use evaluation for FVL in compliance to IEC 61508-3:2010 is undertaken, the programmable devices on which the application program library functions execute shall also be evaluated as proven-in-use according to IEC 61508-2:2010; or
- compliance to IEC 61511 prior use requirements (see 11.5.4 or 11.5.5) when using FPL or LVL;
- in all cases, demonstrating that any unused functions do not adversely impact the application program.

12.4.4 The application program shall be produced in a structured way so as to achieve:

- modular decomposition of the functionality;
- keep the complexity of SIF application program to a minimum consistent with that of the complexity of the required SIF;
- testability of functionality (including fault tolerant features) and of the internal structure of the application program;
- traceability to, and explanation of, application functions and associated constraints;
- one to one mapping between the hardware architecture and application program architecture.

12.5 Requirements for application program verification (review and testing)

12.5.1 Verification planning shall be carried out in accordance with Clause 7.

12.5.2 The application program including its documentation shall be reviewed by a competent person not involved in the original development. The approach used for the review and the review results shall be documented.

12.5.3 The application program, including its decomposition into modules if appropriate, shall be verified through review, analysis, simulation and testing techniques using written procedures and test specifications, that shall be carried out to confirm that the application program functions meet the SRS and that unintended functions are not executed and that there are no unintended side effects with respect to the SIF. The following shall be addressed:

- conformance to the application program design specification, the defined means and procedures, and the requirements of safety validation and test planning;
- exercising of all parts of the application program;
- exercising a representative range of data conditions;
- testing for failure conditions (i.e., negative testing);
- timing and the sequence of execution;
- testing of communications to and from the SIS;
- integration of the off-line application program with the logic solver hardware and the underlying PE;
- internal data flow checks to confirm that the logic solver is not just apparently working, but is working as expected;
- when possible, integration of the application program and 3rd party devices

12.5.4 The mapping of the I/O data to the application program, including data type and range, shall be verified.

12.5.5 During testing, modifications to the application program shall be subject to an impact analysis in order to determine:

- all application program parts impacted;
- the necessary re-design and re-verification activities.

12.5.6 The results of application program testing shall be documented and include:

- the versions of the application program and its supporting documentation being tested;
- the versions of supporting software and test tools;
- names of the person(s) who performed the tests and reviews and dates;
- descriptions of the tests, reviews and dates performed;
- the test results;
- whether the objective and criteria of the tests have been met;
- if there was a failure during the test, the reasons why the failure occurred, the analysis of the failure and the records of its correction and re-test requirements.

12.6 Requirements for application program methodology and tools

12.6.1 The application program development shall comply with the constraints in the applicable safety manual(s).

NOTE When reviewing the safety manual(s), if required for a specific application, additional procedures for and/or constraints on the use of methodologies and tools can be implemented.

12.6.2 Methods, techniques and tools shall be selected and applied for each life-cycle phase so as to:

- minimize the risk of introducing faults into the application program;
- reveal and remove faults that already exist in the application program;
- ensure as far as is practicable that any faults remaining in the application program will not lead to unacceptable results;
- enhance the means of managing modifications of the application program throughout the lifetime of the SIS;
- provide evidence that the application program has the required quality.

13 Factory acceptance test (FAT)

13.1 Objective

The objective of Clause 13 is to test the devices of the SIS to ensure that the requirements defined in the SRS are met.

NOTE 1 By testing the logic solver, associated software and hardware prior to installation, errors can be readily identified and corrected.

NOTE 2 The FAT is sometimes referred to as an integration test and can be part of the validation.

NOTE 3 Testing of field elements together with the logic solver can be recommended when there needs to be a high confidence in operation prior to final installation, e.g., subsea applications.

13.2 Recommendations

13.2.1 The need for a FAT shall be specified during the safety planning for a project.

NOTE 1 Close co-operation between the logic solver supplier and design contractor can be required in order to develop the integration tests.

NOTE 2 The activities follow the design and development phases and precede the installation and commissioning.

NOTE 3 The activities are applicable to the SIS subsystems with or without programmable electronics.

NOTE 4 It is usual for the FAT to take place in a factory environment prior to installation and commissioning in the plant.

13.2.2 The planning for a FAT shall specify the following:

- Types of tests to be performed including black-box system functionality tests; performance tests; internal checks; performance tests; environmental tests; interface testing; testing in degraded or faulted condition; exception testing; testing for safe reaction in case of power failure (including restart after power restored); and application of the SIS maintenance and operating manuals;

NOTE 1 Black-box functionality testing is a test design method that treats the system as a "black box", so it does not explicitly use knowledge of its internal structure. Black-box test design is usually described as focusing on testing function requirements. Synonyms for black box include behavioural, functional, opaque-box, and closed-box testing.

NOTE 2 Performance tests determine whether the system meets timing, reliability and availability, integrity, safety targets and constraints.

NOTE 3 Environmental tests include EMC, life-and stress-testing.

NOTE 4 Internal data flow checks can be carried out to confirm that the SIS is processing input data and generating output response as specified.

- Test cases, test description and test data;

NOTE 5 Clarity in defining who is responsible for developing the test case and who is going to be responsible for carrying out the test and witnessing the test can be very important.

- Dependence on other systems/interfaces;

- Test environment and tools;

- Logic solver, sensor and final element configuration;

- Test criteria on which the completion of the test shall be judged;

- Procedures for corrective action on failure of test;

- Test personnel competences;

- Physical location;

- Hazards posed by the testing especially dealing with stored energy;

- A clear diagram of the test-set up.

- Recording of tests conducted, data, results and observations whilst the tests are being conducted.

NOTE 6 Tests that cannot be physically demonstrated are normally resolved by a formal line of reasoning as to why the SIS achieves the requirement, target or constraint.

13.2.3 The FAT shall take place on a defined version of the logic solver.

13.2.4 The FAT shall be conducted in accordance with the FAT planning. These tests shall show that all the logic performs correctly.

13.2.5 For each test carried out the following shall be addressed:

- the version of the test planning being used;
- the SIF and performance characteristic being tested;
- the detailed test procedures and test descriptions;
- a chronological record of the test activities;
- the tools, equipment and interfaces used.

13.2.6 The results of FAT shall be documented, stating

- the test cases;
- the test results;
- whether the objectives and test criteria have been met.

If there is a failure during test, the reasons for the failure shall be documented and analysed and the appropriate corrective action should be implemented.

13.2.7 During FAT, any modification or change shall be subject to a safety analysis to determine:

- the extent of impact on each SIF;
- the extent of testing and verification which shall be defined and implemented.

NOTE Commissioning can commence whilst corrective action is undertaken, depending on the results of the FAT.

14 SIS installation and commissioning

14.1 Objectives

The objectives of the requirements of Clause 14 are to:

- install the SIS according to the specifications and drawings;
- commission the SIS so that it is ready for final system validation.

NOTE The purpose of commissioning activities is to ensure that each of the SIS devices is individually ready to operate, as specified in the design phase.

14.2 Requirements

14.2.1 Installation and commissioning planning shall define all activities required for installation and commissioning. The planning shall provide the following:

- the installation and commissioning activities;
- the procedures, measures and techniques to be used for installation and commissioning;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities.

Installation and commissioning planning may be integrated in the overall project planning where appropriate.

14.2.2 All SIS devices shall be properly installed according to the design and installation plan(s).

14.2.3 The SIS shall be commissioned in accordance with planning in preparation for the final system validation. Commissioning activities shall include, but not be limited to, confirmation of the following:

- earthing (grounding) has been properly connected;
- energy sources have been properly connected and are operational;
- transportation stops and packing materials have been removed;
- no physical damage is present;
- all instruments have been properly calibrated and configured;
- all field devices are operational;
- logic solver and input/outputs are operational;
- the interfaces to other systems and peripherals are operational;
- all communications between remote SIS systems are operational.

14.2.4 Appropriate records of the commissioning of the SIS shall be produced, stating the results of the activities and whether the objectives and criteria identified during the design phase have been met. If there is a failure, the reasons for the failure shall be recorded.

14.2.5 Where it has been established that the actual installation does not conform to the design information then the difference shall be evaluated by a competent person and impact of the difference on safety shall be determined. If it is established that the difference has no impact on safety, then the design information shall be updated to “as-built” status. If the difference has a negative impact on safety, then the installation shall be modified to meet the design requirements.

15 SIS safety validation

15.1 Objective

The objective of the requirements of Clause 15 is to validate, through inspection and testing, that the installed and commissioned SIS and its associated SIF(s) achieve the requirements as stated in the SRS.

NOTE This is sometimes referred to as a site acceptance test (SAT).

15.2 Requirements

15.2.1 Validation planning of the SIS shall be carried out throughout the SIS safety life-cycle and shall define all activities and equipment required for validation. The following items shall be included:

- the validation activities including validation of the SIS with respect to the SRS including implementation and resolution of resulting recommendations;
- validation of all relevant process operating modes of the process and its associated equipment including;
 - preparation for use including setting and adjustment;
 - start-up, automatic, manual, semi-automatic, steady state of operation;
 - re-setting, shutdown, maintenance;
 - other modes identified in previous phases of the SIS safety life-cycle;

- the procedures, measures and techniques to be used for validation, including how validation activities can be performed, without putting the plant and process at risk of the hazardous events the SIS is to protect against;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities and the levels of independence for validation activities;
- reference to information against which validation shall be carried out (e.g., cause and effect chart);
- the equipment and facilities that needs to be installed or made available (e.g. isolation valves and leak detection equipment that will be needed for the testing of valves).

NOTE Examples of validation activities include loop testing, logic testing, calibration procedures, simulation of application program.

15.2.2 Validation planning for the application program shall include the following:

- identification of the application program functions which needs to be validated for each process operating mode before commissioning begins;
- the technical strategy for the validation including (where relevant):
 - manual and automated techniques;
 - static and dynamic techniques;
 - analytical and statistical techniques.
- in accordance with the preceding bullet, the measures (techniques) and procedures that will be used for confirming that each SIF conforms with the specified safety requirements and the specified SIL;
- the required environment in which the validation activities are to take place (e.g., for tests this would include calibrated tools and equipment);
- the application program;
- the pass/fail criteria for accomplishing validation including:
 - the required process and operator input signals with their sequences and their values;
 - the anticipated output signals with their sequences and their values;
 - other acceptance criteria, for example memory usage, timing and value tolerances.
- the policies and procedures for evaluating the results of the validation, particularly failures;
- all documents (see Clause 19) are validated for accuracy, consistency and traceability of the SIF from inception during the H&RA through the final installed SIF.

15.2.3 Where measurement accuracy is required as part of the validation then instruments used for this function should be calibrated against a specification traceable to a standard within an uncertainty appropriate to the application. If such a calibration is not feasible, an alternative method shall be used and documented.

15.2.4 The validation of the SIS and its associated SIF(s) shall be carried out in accordance with the SIS validation planning. Validation activities shall include, but not be limited to, the following:

- confirmation that the SIS performs under normal and abnormal process operating modes (e.g., start-up, shutdown) as identified in the SRS;
- confirmation that adverse interaction of the BPCS and other connected systems do not affect the proper operation of the SIS;
- the SIS properly communicates (where required) with the BPCS or any other system or network, including during abnormal conditions such as a data overload;

- sensors, logic solver, and final elements perform in accordance with the SRS, including all redundant channels, including abnormal condition such as data overload;

NOTE If a factory acceptance test (FAT) was performed on the logic solver as described in Clause 13, credit can be taken for validation of the logic solver by the FAT. After all equipment is installed in the plant, full loop validation will test the logic solver functionality and its connections to other SIS subsystems.

- SIS design documentation is consistent with the installed system;
- confirmation that the SIF performs as specified on invalid process variable values (e.g., out of range);
- the proper shutdown sequence is activated;
- the SIS provides the proper annunciation and proper operation display;
- computations that are included in the SIS are correct for expected range of values but also at limits and over the limits;
- the SIS reset functions perform as defined in the SRS;
- bypass functions operate correctly;
- start-up overrides operate correctly;
- manual shutdown systems operate correctly;
- the proof-test policy documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- confirmation that the SIS performs as required on loss of utilities (e.g., electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the SIS returns to the desired state;
- confirmation that the EMC immunity, as specified in the SRS (see 10.3), has been achieved.

15.2.5 The validation of the application program shall determine whether:

- all of the specified application program safety requirements (see 10.3.2) are correctly performed;
- the application program does not jeopardize the safety requirements under SIS fault conditions and in degraded modes of operation and for BPCS fault conditions for any interfaces between the SIS and BPCS;
- the application program does not jeopardize the safety requirements by executing “unused” software functionality, i.e., functionality not defined in the specification.

The information of the validation activities shall be available.

15.2.6 The results from the validation plan activities shall represent and cover the entire SIS validation process. SIS validation documentation shall be produced which provides:

- the version of the SIS validation planning being used;
- the SIF(s) under test (or analysis), along with the specific reference to the requirement identified during the SIS validation planning;
- tools and equipment used, along with their calibration data;
- the results of each test;
- the version of the test specification used;
- the criteria for acceptance of the completed tests;
- the version of the SIS hardware, application program(s), and other software being tested;
- any discrepancy between expected and actual results and the resolution of that discrepancy;

- the analysis made and the decisions taken on whether to continue the test or to issue a change request, in the case where discrepancies occur.

15.2.7 The results shall be verified against the expected results. All discrepancies shall be analysed and the findings shall be available as part of the validation documentation. This shall include the analysis made and the decisions taken on whether to continue the validation or to issue a change request and to return to an earlier part of the development life-cycle.

15.2.8 After the SIS validation and prior to the identified hazards being present, the following activities shall be carried out:

- all bypass functions (e.g., PE logic solver and PE sensor forces, disabled alarms) shall be returned to their normal position;
- all process isolation valves shall be set according to the process start-up requirements and procedures;
- all test materials (e.g., fluids) shall be removed;
- all commissioning overrides and force permissives shall be removed.

16 SIS operation and maintenance

16.1 Objectives

The objectives of the requirements of Clause 16 are to ensure that:

- the required SIL of each SIF is maintained during operation and maintenance;
- the SIS is operated and maintained in a way that sustains the required safety integrity.

16.2 Requirements

16.2.1 Operation and maintenance planning for the SIS shall be carried out. It shall provide the following:

- routine and abnormal operation activities;
- inspection, proof testing, preventive and breakdown maintenance activities;
- the procedures, measures and techniques to be used for operation and maintenance;
- the operational response to faults and failures identified by diagnostics, inspections or proof-tests;
- verification of conformity to operations and maintenance procedures;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities;
- a SIS maintenance plan.

NOTE The SIS maintenance plan can state different maintenance features depending on the SIL level.

16.2.2 Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:

- a) the routine methods and procedures which need to be carried out to maintain the "as designed" functional safety of the SIS;
- b) the procedures used to ensure the quality and consistency of proof testing, and to ensure adequate validation is being performed after replacement of any device;
- c) the measures and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (e.g., when a system needs to be bypassed for testing or maintenance, what additional risk reduction needs to be implemented);
- d) the methods and procedures which are used to test the diagnostics;

- e) the information which needs to be maintained on SIS failure and the demand rates on the SIS;
- f) procedures for collecting data related to the demand rate and SIS reliability parameters;

NOTE 1 Collection and analysis of failure data has many benefits including the potential to reduce maintenance costs if failures rates in operation are significantly lower than what were predicted during design. Implementation costs of new installations can also be reduced because new designs can be based on less conservative failure rates.

- g) the information which needs to be maintained showing results of audits and tests on the SIS;
- h) the maintenance procedures to be followed when faults or failures occur in the SIS, including:

- procedures for fault diagnostics and repair;
- procedures for revalidation;
- maintenance reporting requirements;
- procedures for tracking maintenance performance.

NOTE 2 Considerations include:

- procedures for reporting failures;
- procedures for analysing systematic failures;
- the actions to allow safe shutdown in the event of BPCS failure;
- ensuring that test equipment is properly calibrated and maintained.

16.2.3 Operation procedures shall be made available. Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.). The operator shall be provided with information on the procedures to be applied before and during bypass and what should be done before the removal of the bypass and the maximum time allowed to be in the bypass state. This information shall be reviewed on a regular basis.

NOTE The operating and maintenance procedures can include verification that bypasses are removed after proof testing.

16.2.4 Continued process operation with a SIS device in bypass shall only be permitted if a hazards analysis has determined that compensating measures are in place and that they provide adequate risk reduction. Operating procedures shall be developed accordingly.

16.2.5 Operation and maintenance shall proceed in accordance with the relevant procedures.

16.2.6 Operators shall be trained on the function and operation of the SIS in their area. This training shall ensure that they understand:

- how the SIS functions (trip points and the resulting action that is taken by the SIS);
- the hazard the SIS is protecting against;
- the correct operation and management of all bypass/override switches and under what circumstances these bypasses are to be used;

- the operation of any manual shutdown switches and manual start-up activity and when these manual switches are to be activated;

NOTE 2 This can include “system reset” and “system restart”.

- expectation on activation of any diagnostic alarms (e.g., what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS);
- the proper verification of the diagnostics.

16.2.7 The status of all bypasses shall be recorded in a bypass log. All bypasses need authorization and indication.

16.2.8 Maintenance personnel shall be trained as required to sustain full functional performance of the SIS (hardware and software) to meet the target SIL of each SIF.

16.2.9 Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:

- the demand rate on each SIF (see 5.2.5.3);
- the actions taken following a demand on the system;
- the failures and failure modes of equipment forming part of the SIS, including those identified during normal operation, inspection, testing or demand on a SIF;
- the cause of the demands;
- the cause and frequency of spurious trips;
- the failure of equipment forming part of any compensating measures

16.2.10 The operation and maintenance procedures may require revision, if necessary, following:

- functional safety audits;
- tests on the SIS;
- experience from normal or abnormal operation and maintenance events.

16.2.11 Written proof-test procedures shall be developed for every SIF to reveal dangerous failures undetected by diagnostics. These written test procedures shall describe every step that is to be performed and shall include:

- the correct operation of each sensor and final element;
- correct logic action;
- correct alarms and indications.

NOTE The following methods can be used to determine the undetected failures that need to be tested:

- examination of fault trees;
- failure mode and effect analysis;
- reliability centred maintenance.

16.2.12 SIS spare parts shall be identified and shall be made available to minimize the bypass duration due to unavailability of any replacement part for the SIS.

NOTE Replacements that are not in kind (like for like) can be managed as a modification to the SIS.

16.2.13 Persons responsible for operations and maintenance shall review the hazard and risk analysis, allocation and design to ensure the assumptions made are valid e.g. assumptions on occupancy and corrosion protection.

16.3 Proof testing and inspection

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.

NOTE 1 Particular attention can be made to identify failure causes that may lead to common cause failures.

NOTE 2 Functional test procedures can also emphasize the need to avoid introducing common cause failures.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).

NOTE Testing of the SIS can be performed either end-to-end or in segments (see 11.8.1).

16.3.1.3 The schedule for the proof tests shall be according to the SRS. The frequency of proof tests for a SIF shall be determined through PFD_{avg} or PFH calculation in accordance with 11.9 for the SIS as installed in the operating environment.

NOTE Different parts of the SIS can require different test intervals, for example, the logic solver can require a different test interval than the sensors or final elements.

16.3.1.4 Any deficiencies found during the proof testing shall be repaired in a safe and timely manner. A proof test shall be repeated after the repair is completed.

16.3.1.5 At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.

NOTE The user can adjust the test frequency based on this data and an analysis of the original basis for test frequency.

16.3.1.6 Any change to the application program requires full validation and a proof test of any SIF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were designed per the updated safety requirements and correctly implemented.

16.3.1.7 Suitable management procedures shall be applied to review deferrals and prevent significant delay to proof testing.

16.3.2 Inspection

Each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (e.g., missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation).

NOTE These problems could indicate an increase in the frequency of faults.

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

- a) description of the tests and inspections performed including identification of the test procedure used;
- 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 including the "as-found" condition, all faults found (including the failure mode) and the "as-left" condition.

17 SIS modification

17.1 Objectives

The objectives of the requirements of Clause 17 are:

- that modifications to any SIS are properly planned, reviewed, approved and documented prior to making the change;
- to ensure that the required safety integrity of the SIS is maintained despite of any changes made to the SIS.

NOTE Modifications to the BPCS, other equipment, process or operating conditions can be reviewed to determine whether they are such that the nature or frequency of demands on the SIS will be affected. Those having an adverse effect can be considered further to determine whether the level of risk reduction will still be sufficient.

17.2 Requirements

17.2.1 Prior to carrying out any modification to a SIS, procedures for authorizing and controlling changes shall be in place.

17.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and the hazards that may be affected.

17.2.3 Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification could impact safety then there shall be a return to the first phase of the SIS safety life-cycle affected by the modification.

17.2.4 Safety planning for the modification and re-verification shall be available. Modifications and re-verifications shall be carried out in accordance with the planning.

17.2.5 All documentation affected by the modification shall be updated.

17.2.6 Modification activity shall not begin until a FSA is completed in accordance with 5.2.6.1.9 and after proper authorisation.

17.2.7 Appropriate information shall be maintained for all changes to the SIS. The information shall include:

- a description of the modification or change;
- the reason for the change;
- identified hazards and SIFs which may be affected;
- an analysis of the impact of the modification activity on the SIS;
- all approvals required for the changes;
- tests used to verify that the change was properly implemented and the SIS performs as required;
- details of all SIS modification activities (e.g., a modification log);
- appropriate configuration history;
- tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.

17.2.8 Modification shall be performed with qualified personnel who have been properly trained. All affected and appropriate personnel should be notified of the change and trained with regard to the change.

18 SIS decommissioning

18.1 Objectives

The objectives of the requirements of Clause 18 are to ensure that:

- prior to decommissioning any SIS from active service, a proper review is conducted and required authorization is obtained;
- the required SIF(s) remain operational during decommissioning activities.

18.2 Requirements

18.2.1 Prior to carrying out any decommissioning of part or all of a SIS or SIF, procedures for authorizing and controlling changes shall be in place.

18.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and identifying the hazards that may be affected.

18.2.3 An analysis shall be carried out on the impact on functional safety as a result of the proposed decommissioning activity. The assessment shall include an update of the H&RA sufficient to determine the scope of impact to the SIS safety life cycle. The subsequent SIS safety life-cycle phases shall need to be re-evaluated. The assessment shall also consider:

- functional safety during the execution of the decommissioning activities;
- the impact of decommissioning the SIS on adjacent operating units and facility services.

18.2.4 The results of the impact analysis shall be used during safety planning to re-implement the relevant requirements of the IEC 61511 series including re-verification and re-validation.

18.2.5 Decommissioning activities shall not begin without proper documentation and authorization.

19 Information and documentation requirements

19.1 Objectives

The objectives of the requirements of Clause 19 are to ensure that the necessary information is available and documented in order that:

- all phases of the SIS safety life-cycle can be effectively performed;
- verification, validation and FSA activities can be effectively performed.

19.2 Requirements

19.2.1 The documentation required by the IEC 61511 series shall be available to personnel implementing the requirements of the IEC 61511 series.

19.2.2 The documentation shall:

- describe the installation, system or equipment and the use of it;
- be accurate and up to date;
- be easy to understand;
- suit the purpose for which it is intended;
- be available in an accessible, maintainable and editable form, so that appropriate and relevant documents can be readily and accurately identified, located, retrieved and revised.

NOTE Further details of the requirements for information are included in Clause 14 and Clause 15.

19.2.3 The documentation shall have unique identities so it shall be possible to reference the different parts.

19.2.4 The documentation shall have designations indicating the type of information.

19.2.5 The documentation shall be traceable to the functional and integrity requirements arising from this standard, including the H&RA.

19.2.6 The documentation shall have a revision index (for example, version numbers) to make it possible to identify different versions of the information.

19.2.7 The documentation shall be structured to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document.

NOTE The physical structure of the documentation can vary depending upon a number of factors such as the size of the system, its complexity and the organizational requirements.

19.2.8 All relevant documentation shall be revised, amended, reviewed, approved and shall be under the control of an appropriate information control scheme.

19.2.9 Current documentation pertaining to the following shall be maintained:

- a) the results of the H&RA and the related assumptions;
- b) the equipment used for SIF together with its safety requirements;
- c) the organization responsible for maintaining functional safety;
- d) the procedures necessary to achieve and maintain functional safety of the SIS;
- e) the modification information as defined in 17.2.5;
- f) the safety manual(s);
- g) design, implementation, test and validation.

NOTE Further details of the requirements for information are included in 12.4.2, Clauses 14 and 15 and in 16.3.3.

Bibliography

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at <http://www.electropedia.org/>)

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

IEC 60300-3-2:2004, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60605-4:2001, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60617-12:1997, *Graphical symbols for diagrams – Part 12: Binary logic elements*¹

IEC TS 61000-1-2:2008, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61131-3:2013, *Programmable controllers – Part 3: Programming language*

IEC 61131-6:2012, *Programmable controllers – Part 6: Functional Safety*

IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations*

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*

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

IEC 61511-3:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443-2-1:2010, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC 62682:2014, *Management of alarms for the process industry*

ISO/IEC 2382:2006, *Information technology – Vocabulary*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

¹ Withdrawn.

ISO/IEC 90003:2014, *Software engineering – Part 3: Guidelines for the application of ISO 9001:2000 to computer software*

ISO 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

ISO 9001:2008, *Quality management systems – Requirements*

ISO TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

ISO 13849-1:2006, *Safety of machinery – Safety related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety related parts of control systems – Part 2: Validation*

ISO 14224:2006, *Petroleum, petrochemical and natural gas industries- Collection and exchange of reliability and maintenance of data for equipment*

ISA TR 84.00.04 Part 1:2015, *Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

ISA TR 84.00.09:2013, *Security Countermeasures Related to Safety Instrumented Systems (SIS)*

SOMMAIRE

AVANT-PROPOS	85
INTRODUCTION.....	87
1 Domaine d'application	91
2 Références normatives	97
3 Termes, définitions et abréviations	97
3.1 Termes	97
3.2 Termes et définitions	97
3.3 Abréviations.....	119
4 Conformité à l'IEC 61511-1:2016	120
5 Gestion de la sécurité fonctionnelle	120
5.1 Objectif	120
5.2 Exigences	120
5.2.1 Généralités	120
5.2.2 Organisation et ressources	120
5.2.3 Evaluation et gestion des risques	121
5.2.4 Planification de la sécurité	121
5.2.5 Mise en œuvre et surveillance	121
5.2.6 Evaluation, audits et révisions	122
5.2.7 Gestion de configuration du SIS	125
6 Exigences relatives au cycle de vie de sécurité	125
6.1 Objectifs	125
6.2 Exigences	127
6.3 Exigences relatives au cycle de vie de sécurité du SIS du programme d'application.....	130
7 Vérification	133
7.1 Objectif	133
7.2 Exigences	133
8 Analyse de danger et de risque du processus.....	135
8.1 Objectifs	135
8.2 Exigences	135
9 Affectation des fonctions de sécurité aux couches de protection.....	136
9.1 Objectifs	136
9.2 Exigences relatives au processus d'allocation.....	137
9.3 Exigences relatives au système de commande de processus de base en tant que couche de protection.....	139
9.4 Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes	141
10 Spécification des exigences de sécurité (SRS) du SIS.....	141
10.1 Objectif	141
10.2 Exigences générales.....	142
10.3 Exigences de sécurité du SIS	142
11 Conception et ingénierie du SIS.....	144
11.1 Objectif	144
11.2 Exigences générales.....	144
11.3 Exigences relatives au comportement du système lors de la détection d'une anomalie.....	146

11.4	Tolérance aux défauts du matériel	146
11.5	Exigences relatives au choix des appareils	148
11.5.1	Objectifs	148
11.5.2	Exigences générales	148
11.5.3	Exigences relatives au choix des appareils basés sur l'utilisation préalable	148
11.5.4	Exigences relatives au choix des appareils programmables FPL (p. ex.: appareils de terrain) basés sur l'utilisation préalable	149
11.5.5	Exigences relatives au choix des appareils programmables LVL basés sur l'utilisation préalable	150
11.5.6	Exigences relatives au choix des appareils programmables FVL	151
11.6	Appareils de terrain	151
11.7	Interfaces	151
11.7.1	Généralités	151
11.7.2	Exigences relatives à l'interface opérateur	151
11.7.3	Exigences relatives à l'interface de maintenance/d'ingénierie	152
11.7.4	Exigences relatives à l'interface de communication	153
11.8	Exigences relatives à la maintenance ou à la conception des essais	153
11.9	Quantification de défaillance aléatoire	154
12	Développement du programme d'application du SIS	155
12.1	Objectif	155
12.2	Exigences générales	156
12.3	Conception du programme d'application	156
12.4	Mise en œuvre du programme d'application	158
12.5	Exigences relatives à la vérification du programme d'application (revue et essai)	159
12.6	Exigences relatives à la méthodologie et aux outils du programme d'application	160
13	Essai de réception en usine (ERU)	161
13.1	Objectif	161
13.2	Recommandations	161
14	Installation et mise en service du SIS	162
14.1	Objectifs	162
14.2	Exigences	162
15	Validation de sécurité du SIS	163
15.1	Objectif	163
15.2	Exigences	163
16	Fonctionnement et maintenance du SIS	166
16.1	Objectifs	166
16.2	Exigences	166
16.3	Essais périodiques et inspection	169
16.3.1	Essais périodiques	169
16.3.2	Inspection	170
16.3.3	Documentation des essais périodiques et de l'inspection	170
17	Modification du SIS	170
17.1	Objectifs	170
17.2	Exigences	171
18	Déclassement du SIS	171
18.1	Objectifs	171

18.2 Exigences	172
19 Exigences relatives aux informations et à la documentation.....	172
19.1 Objectifs	172
19.2 Exigences	172
Bibliographie.....	174
Figure 1 – Cadre général de la série IEC 61511.....	90
Figure 2 – Relations entre l'IEC 61511 et l'IEC 61508.....	93
Figure 3 – Relations détaillées entre l'IEC 61511 et l'IEC 61508	95
Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions.....	96
Figure 5 – Système électronique programmable (PES): structure et terminologie.....	110
Figure 6 – Exemple d'architectures SIS comprenant trois sous-systèmes SIS.....	113
Figure 7 – Phases de cycle de vie de sécurité d'un SIS et étapes FSA	127
Figure 8 – Cycle de vie de sécurité du programme d'application et ses relations avec le cycle de vie de sécurité du SIS	131
Figure 9 – Couches de protection types et moyens de réduction de risque.....	140
Tableau 1 – Abréviations utilisées dans l'IEC 61511	119
Tableau 2 – Vue d'ensemble du cycle de vie de sécurité d'un SIS (1 de 2)	128
Tableau 3 – Cycle de vie de sécurité du programme d'application: vue d'ensemble (1 de 2).....	132
Tableau 4 – Exigences concernant l'intégrité de sécurité: PFD_{avg}	137
Tableau 5 – Exigences concernant l'intégrité de sécurité: fréquence moyenne de défaillance dangereuse de la SIF.....	137
Tableau 6 – Exigences de HFT minimale en fonction du SIL	147

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

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.

DÉGAGEMENT DE RESPONSABILITÉ

Cette version consolidée n'est pas une Norme IEC officielle, elle a été préparée par commodité pour l'utilisateur. Seules les versions courantes de cette norme et de son(ses) amendement(s) doivent être considérées comme les documents officiels.

Cette version consolidée de l'IEC 61511-1 porte le numéro d'édition 2.1. Elle comprend la deuxième édition (2016-02) [documents 65A/777/FDIS et 65A/784/RVD], son corrigendum 1 (2016-09) et son amendement 1 (2017-08) [documents 65A/844/FDIS et 65A/848/RVD]. Le contenu technique est identique à celui de l'édition de base et à son amendement.

Cette version Finale ne montre pas les modifications apportées au contenu technique par l'amendement 1. Une version Redline montrant toutes les modifications est disponible dans cette publication.

La Norme internationale IEC 61511-1 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 constitue une révision technique et inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- remplacement des références et exigences logiciel par des références et exigences de programmation d'application;
- exigences d'évaluation de la sécurité fonctionnelle décrites avec plus de détails pour améliorer la gestion de la sécurité fonctionnelle.
- ajout de la gestion des exigences de changement;
- ajout des exigences d'évaluation du risque de sécurité;
- extension des exigences au système de base de contrôle de processus comme couche de protection;
- modification des exigences relatives à la tolérance de panne matérielle et réexamen minutieux pour comprendre les options utilisateurs/intégrateurs.

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

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 la publication de base et de son amendement 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.

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 et certains niveaux de performance minimaux.

La série IEC 61511 concerne l'application des SIS aux industries de transformation. La série IEC 61511 porte également sur la réalisation d'une analyse de danger et de risque relative au processus (H&RA) visant à en déduire la spécification relative aux SIS. D'autres contributions du système de sécurité sont uniquement prises en compte eu égard aux exigences de performance du SIS. Le SIS inclut tous les appareils nécessaires à l'acheminement de la SIF entre le capteur et l'élément terminal.

La série IEC 61511 aborde deux concepts essentiels à son application: le cycle de vie de sécurité des SIS et les niveaux d'intégrité de sécurité (SIL).

La série IEC 61511 concerne les SIS reposant sur l'utilisation d'une technologie électrique/électronique/électronique programmable. Si d'autres technologies sont utilisées pour les unités logiques, il convient d'appliquer les principes de base de la série IEC 61511 pour garantir que les exigences de sécurité fonctionnelle soient 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 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 principes minimaux. Cette approche a été adoptée afin de mettre en œuvre une politique technique cohérente et rationnelle.

Dans la plupart des cas, la sécurité est obtenue de la meilleure façon par une conception de processus à sécurité intrinsèque. Toutefois, dans certains cas, cela s'avère impossible ou peu pratique. Si nécessaire, cette approche peut être combinée à un ou plusieurs systèmes de protection afin de couvrir les risques résiduels identifiés éventuels. Les systèmes de protection peuvent reposer sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). Pour faciliter cette approche, la série IEC 61511:

- aborde la réalisation d'une analyse de danger et de risque pour identifier les exigences de sécurité globales;
- prend en compte l'affectation des exigences de sécurité aux SIS;
- s'inscrit dans un cadre applicable à tous les moyens instrumentés 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.

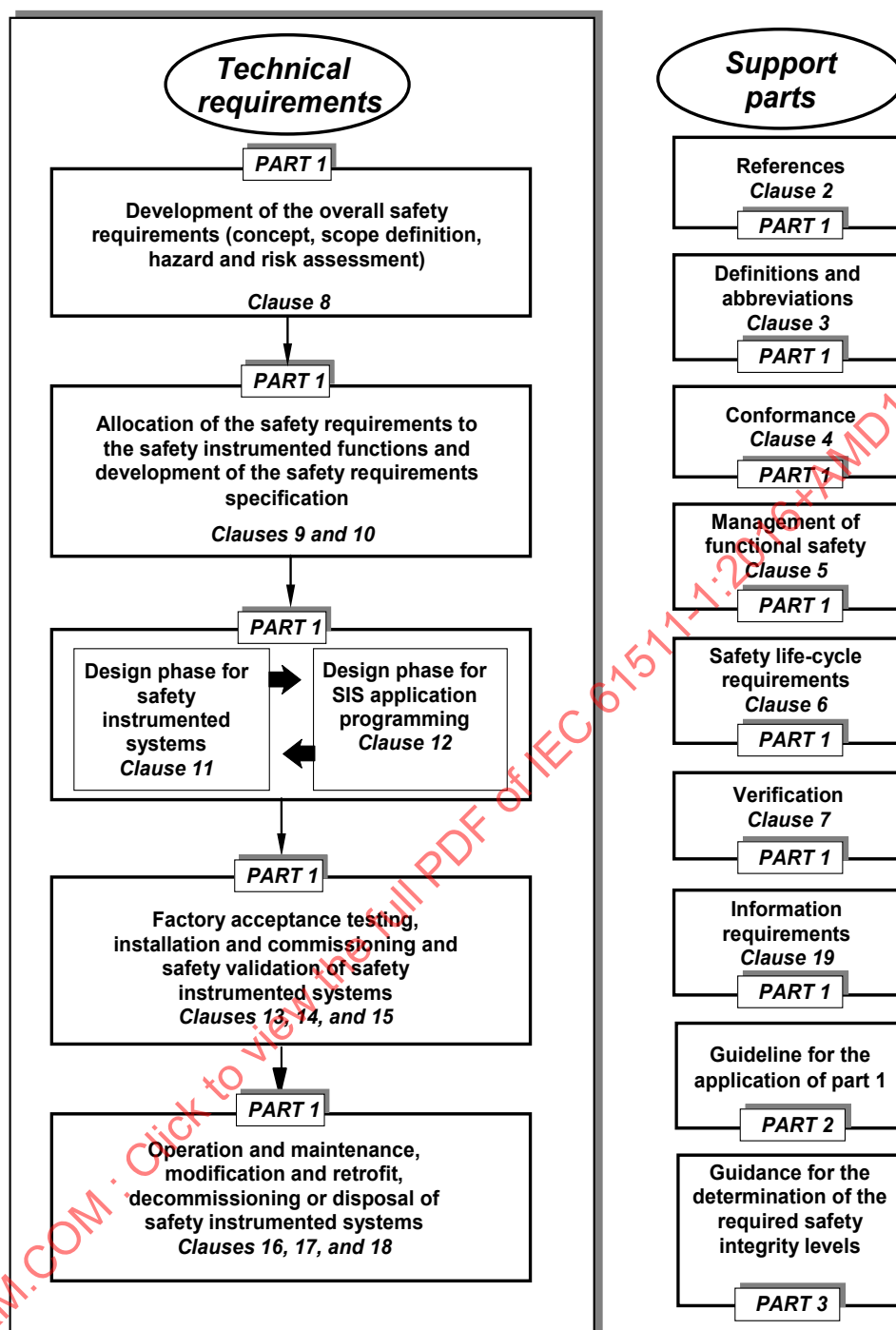
La série IEC 61511 relative aux SIS pour les industries de transformation:

- prend en compte toutes les phases relatives au cycle de vie de sécurité des SIS (concept initial, conception, mise en œuvre, fonctionnement, maintenance et déclassement);
- permet d'harmoniser les normes des industries de transformation nationales existantes ou nouvelles par rapport à la série IEC 61511.

L'IEC 61511 vise à obtenir un haut niveau de cohérence (p. ex.: des principes sous-jacents, de la terminologie et de l'information) dans le secteur des industries de transformation. Il convient de noter que cela présente des avantages tant du point de vue de la sécurité que du point de vue économique. La Figure 1 ci-dessous présente un cadre général de la série IEC 61511.

Dans les juridictions où les autorités compétentes (p. ex.: nationales, fédérales, étatiques, provinciales, cantonales, municipales) ont défini des réglementations relatives à la conception de la sécurité des processus, la gestion de la sécurité des processus ou autres, ces réglementations sont prioritaires par rapport aux exigences définies dans la série IEC 61511.

IECNORM.COM : Click to view the full PDF of IEC 61511-1:2016+AMD1:2017 CSV



Anglais	Français
Technical requirements	Exigences techniques
PART 1	PARTIE 1
PART 2	PARTIE 2
PART 3	PARTIE 3
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
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification Clauses 9 and 10	Allocation 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
Guidance for the determination of the required safety integrity levels	Ligne directrice pour la détermination des niveaux d'intégrité de sécurité exigés

Figure 1 – Cadre général de la série IEC 61511

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

Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

1 Domaine d'application

La présente partie de l'IEC 61511 décrit les exigences relatives à la spécification, la conception, l'installation, au fonctionnement et à la maintenance d'un système instrumenté de sécurité (SIS, Safety Instrumented System) de manière à ce qu'il puisse être mis en œuvre en toute confiance pour établir ou maintenir le processus dans un état de sécurité convenable. L'IEC 61511-1 a été conçue pour être une mise en œuvre de l'IEC 61508:2010 dans le secteur des industries de transformation.

En particulier, l'IEC 61511-1:

- a) spécifie les exigences permettant d'obtenir la sécurité fonctionnelle, mais ne spécifie pas la responsabilité de la mise en œuvre des exigences (p. ex.: les concepteurs, les fournisseurs, la société propriétaire/exploitante, l'entrepreneur). Cette responsabilité sera assignée aux différentes parties selon la planification de la sécurité, la planification et la gestion de projets, ainsi que les règlements nationaux;
- b) s'applique lorsque des appareils satisfaisant aux exigences de la série IEC 61508 parue en 2010 ou de l'IEC 61511-1:2016 [115] sont intégrés dans un système qui doit être utilisé pour une application du secteur des industries de transformation. Elle ne concerne pas les fabricants qui souhaitent revendiquer la possibilité d'utiliser ces appareils dans les SIS du secteur des industries de transformation (voir l'IEC 61508-2:2010 et l'IEC 61508-3:2010);
- c) définit les relations entre les normes IEC 61511 et IEC 61508 (voir Figures 2 et 3);
- d) s'applique lorsque des programmes d'application sont développés pour des systèmes possédant un langage de variabilité limitée ou lors de l'utilisation d'appareil à langage de programmation figé, mais ne s'applique pas aux fabricants, concepteurs, intégrateurs et utilisateurs du SIS qui développent des logiciels intégrés (logiciels système) ou utilisent des langages de variabilité totale (voir l'IEC 61508-3:2010);
- e) s'applique à de nombreuses industries de transformation (p. ex.: produits chimiques, pétrole et gaz, pâte à papier et papier, produits pharmaceutiques, produits alimentaires et boissons, production d'électricité non-nucléaire);
NOTE 1 Dans le secteur des industries de transformation, certaines applications peuvent faire l'objet d'exigences supplémentaires qui doivent être satisfaites.
- f) met en évidence les relations entre les SIF et d'autres fonctions instrumentées (voir Figure 4);
- g) aboutit à l'identification des exigences fonctionnelles et des exigences concernant l'intégrité de sécurité relatives aux SIF en tenant compte de la réduction de risque obtenue par d'autres méthodes;
- h) spécifie les exigences relatives au cycle de vie de l'architecture du système et la configuration du matériel, ainsi que de la programmation d'application et de l'intégration du système;
- i) spécifie les exigences relatives à la programmation d'application pour les intégrateurs et utilisateurs de SIS;

- j) s'applique lorsque la sécurité fonctionnelle est obtenue en utilisant une ou plusieurs SIF pour la protection du personnel, la protection du grand public ou la protection de l'environnement;
 - k) peut s'appliquer dans des applications non liées à la sécurité (la protection de biens, par exemple);
 - l) définit les exigences pour la mise en œuvre des SIF dans le cadre des dispositions globales permettant d'obtenir la sécurité fonctionnelle;
 - m) utilise le cycle de vie de sécurité d'un SIS (voir Figure 7) et définit une liste des activités devant être réalisées pour déterminer les exigences fonctionnelles, ainsi que les exigences concernant l'intégrité de sécurité relatives au SIS;
 - n) spécifie qu'une H&RA doit être réalisée pour définir les exigences de sécurité fonctionnelle et les niveaux d'intégrité de sécurité (SIL) de chaque SIF;
- NOTE 2 Pour avoir une vue d'ensemble des moyens de réduction de risque, voir la Figure 9.
- o) établit des objectifs quantitatifs relatifs à la probabilité moyenne de défaillance en cas de sollicitation (en mode sollicitation) et à la fréquence moyenne de défaillance dangereuse (en mode sollicitation ou en mode continu) pour chaque SIL;
 - p) spécifie des exigences minimales pour la tolérance aux défauts du matériel (HFT);
 - q) spécifie les mesures et techniques exigées pour obtenir le SIL indiqué;
 - r) définit un niveau maximal de performance de sécurité fonctionnelle (SIL 4) qui peut être atteint pour une SIF mise en œuvre conformément à l'IEC 61511-1;
 - s) définit un niveau minimal de performance de sécurité fonctionnelle (SIL 1) au-dessous duquel l'IEC 61511-1 ne s'applique pas;
 - t) fournit un cadre pour l'établissement du SIL, mais ne spécifie pas le SIL exigé pour les applications spécifiques (qu'il convient d'établir sur la base de la connaissance de l'application particulière et par rapport à la réduction de risque globale souhaitée);
 - u) spécifie les exigences pour toutes les parties du SIS, depuis le capteur jusqu'à l'élément terminal ou jusqu'aux éléments terminaux;
 - v) définit les informations qui sont nécessaires pendant le cycle de vie de sécurité du SIS;
 - w) spécifie que la conception du SIS tient compte des facteurs humains;
 - x) n'applique aucune exigence directe relative à l'opérateur individuel ou au technicien de maintenance.

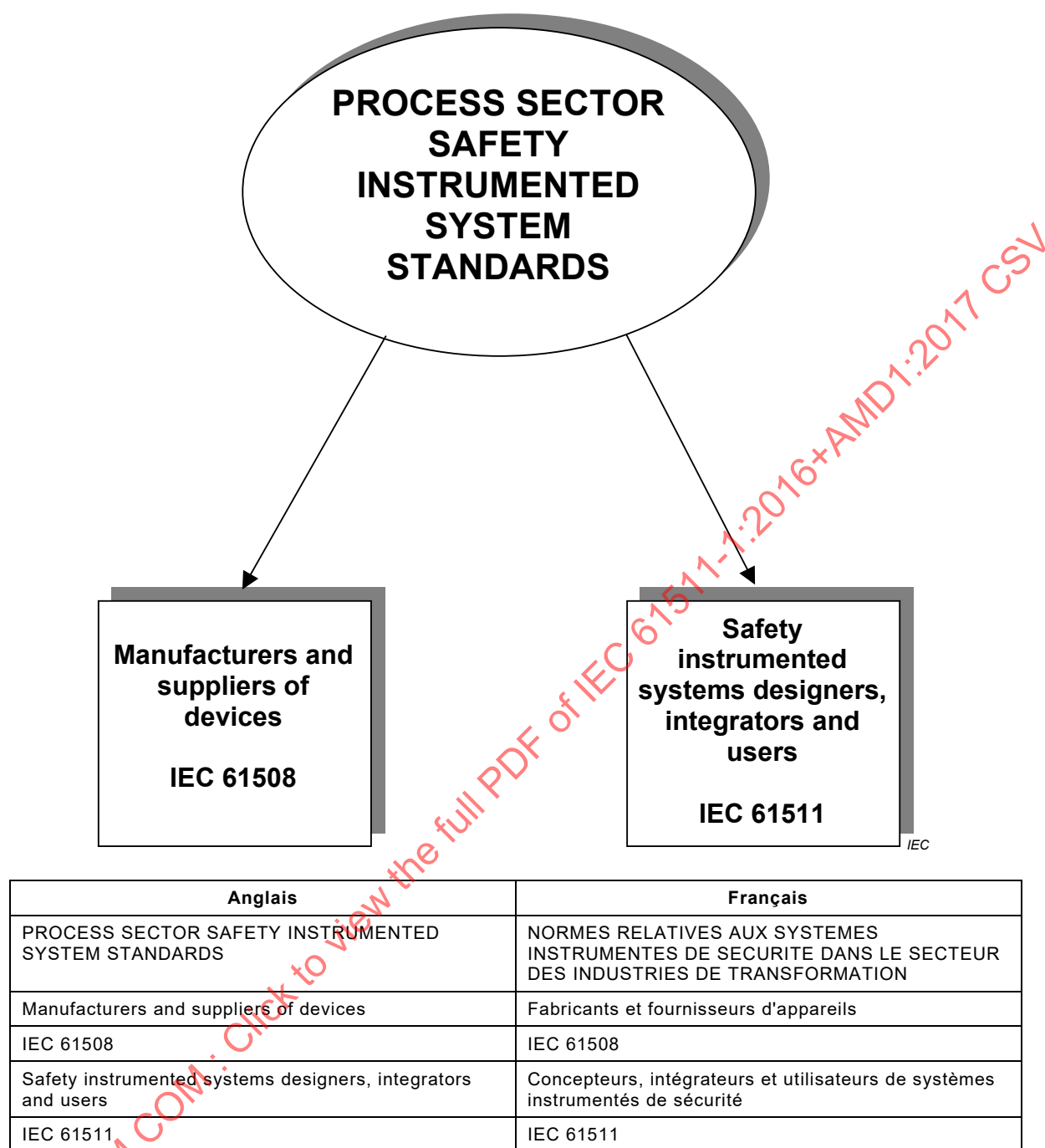
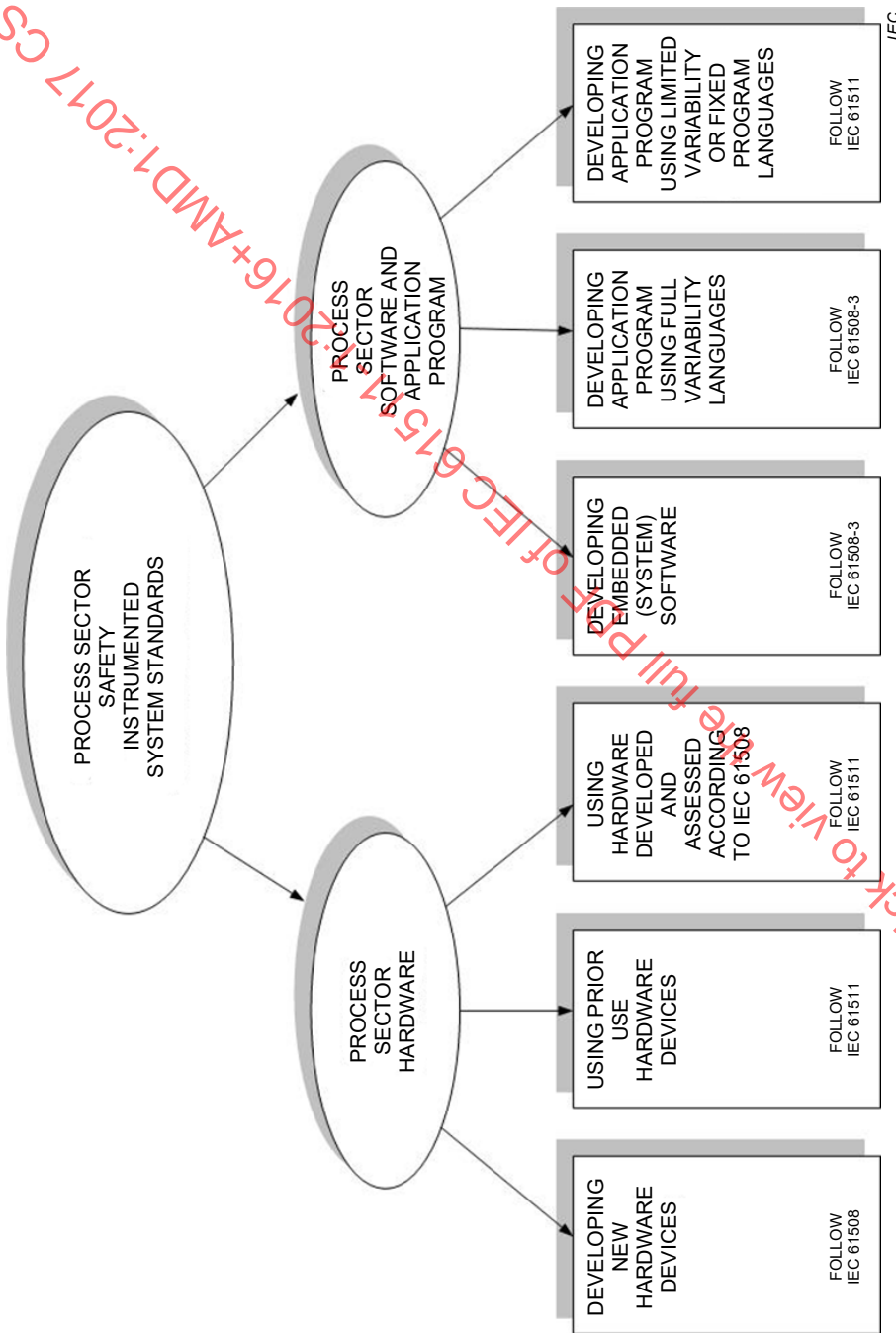


Figure 2 – Relations entre l'IEC 61511 et l'IEC 61508

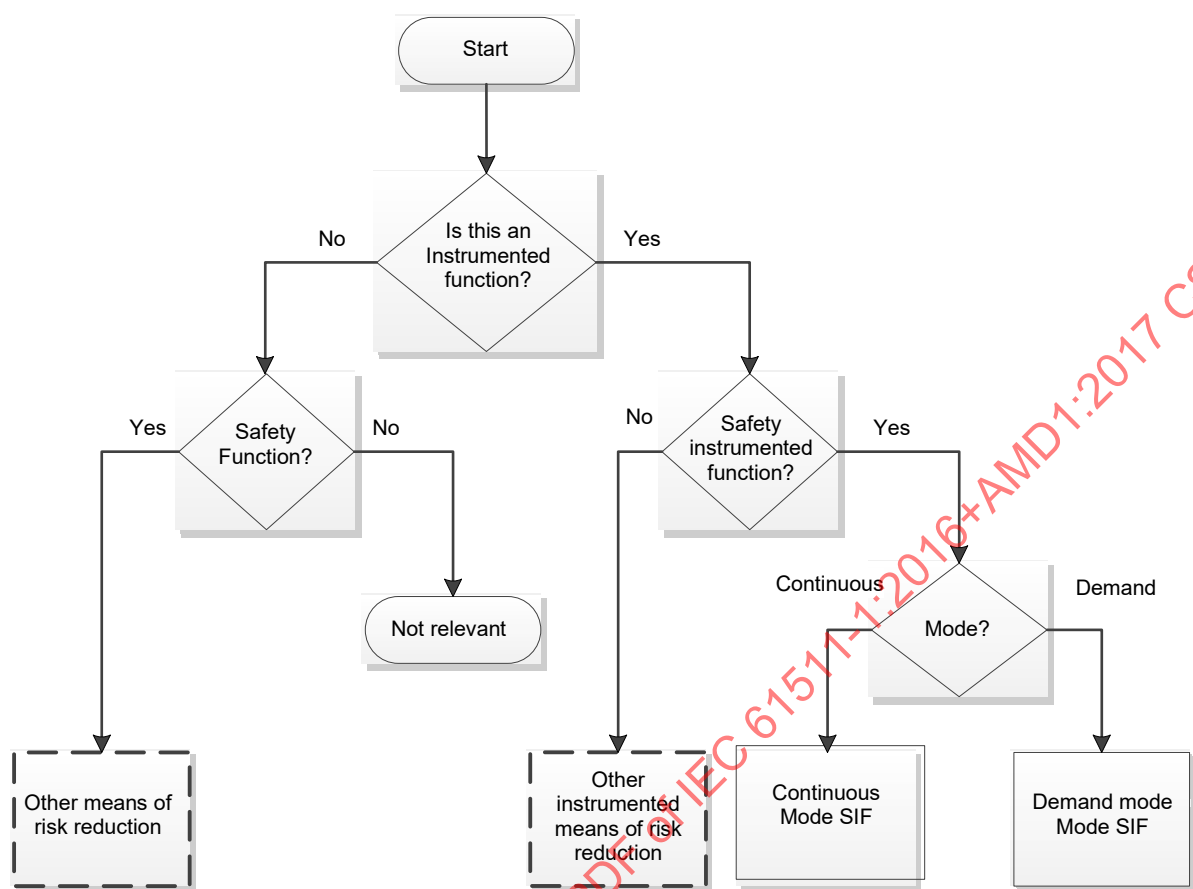
NOTE 3 L'IEC 61508 est également utilisée par les concepteurs, intégrateurs et utilisateurs de SIS lorsque cela est indiqué dans l'IEC 61511.



Anglais	Français
PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS	NORMES RELATIVES AUX SYSTEMES INSTRUMENTES DE SECURITE DANS LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
PROCESS SECTOR HARDWARE	MATERIEL POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
PROCESS SECTOR SOFTWARE & APPLICATION PROGRAM	LOGICIEL ET PROGRAMME D'APPLICATION POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
DEVELOPING NEW HARDWARE DEVICES	DEVELOPPEMENT DE NOUVEAUX APPAREILS MATERIELS
FOLLOW IEC 61508	SUIVRE L'IEC 61508
USING PRIOR USE HARDWARE DEVICES	UTILISATION D'APPAREILS MATERIELS BASES SUR L'UTILISATION ANTERIEURE
FOLLOW IEC 61511	SUIVRE L'IEC 61511
USING HARDWARE DEVELOPED AND ASSESSED ACCORDING TO IEC 61508	UTILISATION DE MATERIEL DEVELOPPE ET EVALUE CONFORMEMENT A L'IEC 61508
DEVELOPING EMBEDDED (SYSTEM) SOFTWARE	DEVELOPPEMENT DE LOGICIELS (SYSTEME) INTEGRES
FOLLOW IEC 61508-3	SUIVRE L'IEC 61508-3
DEVELOPING APPLICATION PROGRAM USING FULL VARIABILITY LANGUAGES	DEVELOPPEMENT DE PROGRAMME D'APPLICATION UTILISANT DES LANGAGES DE VARIABILITE TOTALE
DEVELOPING APPLICATION PROGRAM USING LIMITED VARIABILITY OR FIXED PROGRAM LANGUAGES	DEVELOPPEMENT DE PROGRAMME D'APPLICATION UTILISANT DES LANGAGES DE VARIABILITE LIMITEE OU DES LANGAGES DE PROGRAMME FIGE

Figure 3 – Relations détaillées entre l'IEC 61511 et l'IEC 61508

NOTE 4 Pour connaître les lignes directrices concernant le traitement de l'intégration des sous-systèmes qui satisfont à d'autres normes (machines, brûleur, etc.), voir 7.2.2 de l'IEC 61511-1:2016 et A.7.2.2 de l'IEC 61511-2:2016.



Standard specifies activities which are to be carried out but requirements are not detailed

IEC

Anglais	Français
Start	Démarrage
Is this an Instrumented function?	Est-ce une fonction instrumentée?
No	Non
Yes	Oui
Safety Function?	Fonction de sécurité?
Safety instrumented function?	Fonction instrumentée de sécurité?
Not relevant	Non pertinent
Mode?	Mode?
Continuous	Continu
Demand	Sollicitation
Other means of risk reduction	Autres moyens de réduction de risque
Other instrumented means of risk reduction	Autres moyens instrumentés de réduction de risque
Continuous Mode SIF	SIF en mode continu
Demand mode Mode SIF	SIF en mode sollicitation
Standard specifies activities which are to be carried out but requirements are not detailed	La norme spécifie les activités devant être réalisées, mais les exigences ne sont pas détaillées

Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions

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 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

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*

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

3 Termes, définitions et abréviations

3.1 Termes

Les termes figurent dans l'ordre alphabétique en 3.2.

3.2 Termes et définitions

Pour les besoins du présent document, les définitions suivantes s'appliquent.

Dans certains cas, ces définitions diffèrent de celles correspondant aux mêmes termes dans l'IEC 61508-4:2010. Dans certains cas, cela est dû à la terminologie utilisée dans le secteur des industries de transformation. Dans d'autres cas, ces définitions ont été alignées avec d'autres références définitives pertinentes (p. ex.: l'IEC 60050, le Vocabulaire Electrotechnique International, l'ISO/IEC Guide 51:2013). Toutefois, sauf indication contraire, il n'existe aucune différence de signification technique entre ces définitions et celles des mêmes termes dans l'IEC 61508-4:2010.

3.2.1

architecture

configuration

configuration spécifique des éléments matériels et logiciels dans un système

Note 1 à l'article: Dans la série IEC 61511, cela peut signifier, par exemple, la disposition des sous-systèmes SIS, la structure interne d'un sous-système SIS ou la structure interne des programmes d'application du SIS.

3.2.2

protection de biens

fonction allouée à la conception d'un système dans le but de prévenir la perte ou l'endommagement de biens

3.2.3

système de commande de processus de base

BPCS

système qui répond aux signaux d'entrée provenant du processus, de ses équipements associés, d'autres systèmes programmables et/ou des opérateurs, et qui génère des signaux de sortie faisant fonctionner le processus et ses équipements associés de la manière souhaitée, mais qui n'exécute aucune fonction instrumentée de sécurité (SIF)

Note 1 à l'article: Un BPCS inclut tous les appareils nécessaires pour s'assurer que le processus fonctionne de la manière souhaitée.

Note 2 à l'article: Un BPCS peut habituellement mettre en œuvre différentes fonctions (p. ex.: fonctions de commande de processus, surveillance, et alarmes).

Note 3 à l'article: L'abréviation «BPCS» est dérivée du terme anglais développé correspondant «basic process control system».

3.2.4

dérivation

action ou installation empêchant l'exécution de tout ou partie des fonctionnalités du SIS

Note 1 à l'article: Des exemples de dérivation incluent ce qui suit:

- le signal d'entrée en provenance du circuit de déclenchement est bloqué, mais les paramètres d'entrée et l'alarme sont toujours présentés à l'opérateur;
- le signal de sortie du circuit de déclenchement à un élément terminal est maintenu à l'état normal empêchant le fonctionnement de l'élément terminal;
- une ligne de dérivation physique est fournie autour de l'élément terminal;
- un état d'entrée présélectionné (p. ex.: acheminer/arrêter le signal d'entrée) ou un ensemble de paramètres est forcé par l'intermédiaire d'un outil d'ingénierie (p. ex.: dans le programme d'application).

Note 2 à l'article: La notion de dérivation est également rendue par d'autres termes (p. ex.: neutralisation, mise en échec, désactivation, forçage, inhibition, shuntage ou blocage).

3.2.5

canal

appareil ou groupe d'appareils exécutant une fonction indépendante spécifique

Note 1 à l'article: Les appareils d'un canal peuvent comporter des appareils d'entrée et de sortie (E/S), des unités logiques, des capteurs et des éléments terminaux.

Note 2 à l'article: Une configuration à double canal (à deux canaux) comprend deux canaux réalisant indépendamment la même fonction. Les canaux peuvent être identiques ou différents.

Note 3 à l'article: Ce terme peut être utilisé pour décrire un système complet ou une partie seulement d'un système (p. ex.: les capteurs ou les éléments terminaux).

Note 4 à l'article: Un canal décrit les éléments architecturaux matériels d'un SIS souvent utilisés pour satisfaire aux exigences de tolérance aux défauts du matériel.

3.2.6

cause commune

3.2.6.1

défaillances de cause commune, pl

défaillances concomitantes affectant plusieurs appareils, qui proviennent d'un événement unique et ne résultent pas les unes des autres

Note 1 à l'article: Toutes les défaillances résultant d'une cause commune ne se produisent pas nécessairement exactement à la même heure, et cela peut laisser du temps pour détecter l'occurrence de la cause commune avant qu'un SIS ne subisse réellement une défaillance.

Note 2 à l'article: Les défaillances de cause commune peuvent également donner lieu à des défaillances de mode commun.

Note 3 à l'article: La possibilité de défaillances de cause commune réduit l'efficacité de la redondance ou de la tolérance aux anomalies d'un système (p. ex.: augmente la probabilité de défaillance de deux canaux ou plus dans un système multicanal).

Note 4 à l'article: Les défaillances de cause commune sont des défaillances dépendantes. Elles peuvent résulter d'événements extérieurs (p. ex.: température, humidité, surtension, incendie et corrosion), d'erreurs systématiques (p. ex.: erreurs de conception, d'assemblage ou d'installation, bogues), d'erreurs humaines (p. ex.: mauvaise utilisation), etc.

Note 5 à l'article: Par extension, une défaillance de cause commune (au singulier) est une défaillance appartenant à un ensemble de défaillances concomitantes (au pluriel) selon la définition donnée en 3.2.6.1.

3.2.6.2

défaillances de mode commun, pl

défaillances concomitantes affectant plusieurs appareils, caractérisées par le même mode de défaillance (c'est-à-dire des défaillances identiques)

Note 1 à l'article: Les défaillances de mode commun peuvent avoir différentes causes.

Note 2 à l'article: Les défaillances de mode commun peuvent également être le résultat de défaillances de cause commune (3.2.6.1).

Note 3 à l'article: La possibilité de défaillances de mode commun réduit l'efficacité de la redondance ou de la tolérance aux anomalies d'un système (p. ex.: défaillance de deux canaux ou plus de la même manière, ce qui entraîne le même résultat erroné).

Note 4 à l'article: Par extension, une défaillance de mode commun (au singulier) est une défaillance appartenant à un ensemble de défaillances concomitantes (au pluriel) selon la définition donnée en 3.2.6.2.

3.2.7

mesure compensatoire

mise en œuvre temporaire de méthodes planifiées et documentées de gestion des risques au cours d'une période de maintenance ou de fonctionnement du processus lorsque les performances du SIS sont réputées être dégradées

3.2.8

composant

l'une des parties d'un système, d'un sous-système SIS ou d'un appareil, exécutant une fonction spécifique

Note 1 à l'article: Un composant peut également inclure des logiciels.

3.2.9

gestion de configuration

discipline d'identification des composants d'un système évolutif et des dispositions de ces composants ayant pour objectif de maîtriser les modifications de ces composants et de maintenir la continuité du système et la traçabilité des changements apportés tout au long du cycle de vie

3.2.9.1

approche prudente

manière prévoyante de réaliser des analyses et calculs

Note 1 à l'article: Dans le domaine de la sécurité, chaque fois qu'une analyse ou qu'une hypothèse doit être formulée ou qu'un calcul doit être réalisé (concernant des modèles, des données d'entrée, des calculs, etc.), une approche prudente peut être choisie pour s'assurer de produire des résultats pessimistes.

3.2.10

système de commande

système qui réagit à des signaux d'entrée provenant du processus et/ou d'un opérateur et qui produit des signaux de sortie qui font que le processus fonctionne de la manière souhaitée

Note 1 à l'article: Le système de commande comprend des capteurs et des éléments terminaux et peut être soit un BPCS, soit un SIS ou une combinaison des deux.

3.2.11

défaillance dangereuse

défaillance qui neutralise ou désactive une action de sécurité donnée

Note 1 à l'article: Une défaillance est "dangereuse" uniquement au regard d'une SIF donnée.

Note 2 à l'article: Lorsque la tolérance aux anomalies est mise en œuvre, une défaillance dangereuse peut conduire à:

- une SIF dégradée où l'action de sécurité est disponible, mais où il existe une plus grande probabilité de PFD ou de PFH;

- une SIF désactivée où l'action de sécurité est complètement désactivée ou l'événement dangereux a été induit.

Note 3 à l'article: Lorsqu'aucune tolérance aux anomalies n'est mise en œuvre, toutes les défaillances dangereuses conduisent à une SIF désactivée.

3.2.12

défaillance dépendante

défaillance dont la probabilité ne peut pas être exprimée en tant que simple produit des probabilités non conditionnelles de chacun des événements individuels qui l'ont provoquée

Note 1 à l'article: Deux événements A et B sont dépendants si la probabilité d'occurrence de A et B, $P(A \text{ et } B)$, est supérieure à $P(A) \times P(B)$.

Note 2 à l'article: Pour plus d'informations sur les défaillances dépendantes entre les couches de protection, voir 9.4.2 et l'IEC 61511-3:2016, Annexe J.

Note 3 à l'article: Les défaillances dépendantes incluent la cause commune.

3.2.13

défecté

révélé

déclaré

se rapporte aux défaillances ou erreurs du matériel et du logiciel qui ne sont pas cachées, parce qu'elles s'annoncent elles-mêmes ou qu'elles sont détectées lors du fonctionnement normal ou par des méthodes de détection dédiées

Note 1 à l'article: Il existe quelques différences pour l'utilisation de ces adjectifs:

- L'adjectif "déclaré" désigne les défaillances ou erreurs qui s'annoncent elles-mêmes au moment où elles surviennent (p. ex.: du fait du changement d'état). La réparation de telles défaillances peut débuter dès leur occurrence.
- L'adjectif "détecté" désigne les défaillances ou erreurs qui ne s'annoncent pas elles-mêmes au moment où elles surviennent et qui restent cachées jusqu'à ce qu'elles soient détectées par les essais de diagnostic, les essais périodiques ou l'intervention de l'opérateur (p. ex.: examen physique et essais manuels). La réparation de telles défaillances ne peut débuter qu'une fois qu'elles ont été révélées. Pour connaître l'usage spécifique de ce terme dans l'IEC 61511, se reporter à la Note 2.
- L'adjectif "révélé" désigne les défaillances ou erreurs qui deviennent évidentes parce qu'elles sont déclarées ou ont été détectées.

Note 2 à l'article: Dans l'IEC 61511 et excepté lorsque le contexte suggère une autre signification, le terme "défaillances/erreurs détectées dangereuses" se rapporte aux défaillances/erreurs dangereuses détectées par les essais de diagnostic.

Note 3 à l'article: Lorsque la détection est très rapide (p. ex.: essais de diagnostic), les défaillances ou erreurs détectées peuvent être considérées comme des défaillances ou erreurs déclarées.

Lorsque la détection n'est pas très rapide (p. ex.: essais périodiques), les défaillances ou erreurs détectées ne peuvent pas être considérées comme des défaillances ou erreurs déclarées en ce qui concerne les niveaux d'intégrité de sécurité.

Note 4 à l'article: Une défaillance révélée dangereuse peut uniquement être traitée comme une défaillance en sécurité si des mesures efficaces (automatiques ou manuelles) sont mises en œuvre dans un délai suffisamment court pour maintenir la sécurité du processus.

3.2.14

appareil

matériel, avec ou sans logiciel, capable de réaliser une fonction spécifiée

Note 1 à l'article: Des exemples incluent les capteurs, les unités logiques, les éléments terminaux, les interfaces opérateur et les raccordements à l'installation.

3.2.14.1

appareil de terrain

appareil SIS ou BPCS connecté directement au processus ou situé à proximité du processus

Note 1 à l'article: Des exemples incluent les capteurs, les éléments terminaux et les commutateurs manuels.

3.2.15 **diagnostic**

essai automatique fréquent (lié au temps de sécurité du processus) visant à révéler des défaillances

3.2.15.1 **couverture du diagnostic** DC

taux de défaillances dangereuses détectées par les diagnostics. La couverture du diagnostic ne comprend aucune défaillance détectée par les essais périodiques

Note 1 à l'article: La couverture du diagnostic s'applique habituellement aux appareils SIS ou aux sous-systèmes SIS. Par exemple, la couverture du diagnostic est généralement déterminée pour un capteur, un élément terminal ou une unité logique.

Note 2 à l'article: Pour les applications de sécurité, la couverture du diagnostic s'applique habituellement aux défaillances dangereuses des appareils SIS ou des sous-systèmes SIS. Par exemple, la couverture du diagnostic pour les défaillances dangereuses d'un appareil est $DC = \lambda_{DD} / \lambda_{DT}$, où λ_{DD} est le taux de défaillances dangereuses détectées et λ_{DT} est le taux de défaillances dangereuses totales. Pour un sous-système SIS avec redondance interne, DC dépend du temps: $DC(t) = \lambda_{DD}(t) / \lambda_{DT}(t)$.

Note 3 à l'article: Lorsque la couverture du diagnostic (DC) et le taux de défaillances dangereuses totales (λ_{DT}) sont donnés, les taux de défaillances dangereuses détectées (λ_{DD}) et non détectées (λ_{DU}) peuvent être calculés comme suit:

$$\lambda_{DD} = DC \times \lambda_{DT} \text{ et } \lambda_{DU} = (1-DC) \times \lambda_{DT}.$$

Note 4 à l'article: L'abréviation "DC" est dérivée du terme anglais développé correspondant "diagnostic coverage".

3.2.16 **diversité** moyens différents pour réaliser une fonction exigée

Note 1 à l'article: La diversité peut être réalisée en utilisant des moyens physiques, des techniques de programmation ou des approches de conception différents.

3.2.17 **erreur**

écart entre une valeur ou condition calculée, observée ou mesurée et la valeur ou condition vraie, spécifiée ou théoriquement correcte

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.2.18 **défaillance** perte de l'aptitude à fonctionner tel que requis

Note 1 à l'article: La défaillance d'un appareil est un événement qui provoque un état d'anomalie de cet appareil.

Note 2 à l'article: Lorsque la perte d'aptitude est causée par une panne latente, la défaillance survient lorsqu'un ensemble particulier de circonstances est réuni.

Note 3 à l'article: L'accomplissement des fonctions exigées exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportement à éviter. L'occurrence d'un tel comportement est une défaillance.

Note 4 à l'article: Les défaillances sont soit aléatoires, soit systématiques (voir 3.2.59 et 3.2.81).

[SOURCE: IEC 60050-192:2015, 192-03-01, modifiée – Les notes à l'article ont été modifiées]

3.2.18.1 **mode de défaillance** manière selon laquelle une défaillance se produit

Note 1 à l'article: Un mode de défaillance peut être défini par la fonction perdue ou par la transition d'état qui s'est produite.

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.2.19

anomalie

inaptitude à fonctionner tel que requis, due à un état interne

Note 1 à l'article: La panne d'une entité est due soit à une défaillance de l'entité elle-même, soit à une imperfection lors d'une étape précédente du cycle de vie, telle que la spécification, la conception, la fabrication ou la maintenance.

Note 2 à l'article: Une panne d'un appareil donne lieu à une défaillance lorsqu'un ensemble particulier de circonstances est réuni.

[SOURCE: IEC 60050-192:2015, 192-04-01, modifiée – Certaines notes à l'article ont été modifiées, d'autres supprimées. "Panne" a été changé en "anomalie"]

3.2.20

évitement des anomalies

utilisation de techniques et procédures destinées à éviter l'apparition d'anomalies durant chacune des phases du cycle de vie de sécurité du SIS

3.2.20.1

exclusion des anomalies

élimination dans les examens futurs d'anomalies résultant de modes de défaillance improbables

Note 1 à l'article: Pour plus d'informations sur l'exclusion des anomalies, l'ISO 13849-1 et l'ISO 13849-2 peuvent être consultées. Outre ces normes, l'exclusion des anomalies peut reposer sur:

- l'improbabilité technique de l'occurrence de certaines anomalies;
- l'expérience technique généralement acceptée, indépendamment de l'application concernée;
- les exigences techniques relatives à l'application et au danger spécifique.

Note 2 à l'article: Les modes de défaillance (identifiés dans les appareils réalisant la fonction de sécurité) peuvent être exclus, car leurs taux de défaillances dangereuses sont très faibles par rapport au niveau objectif de défaillances relatif à la fonction de sécurité à l'étude. Autrement dit, la somme des taux de défaillances dangereuses de tous les appareils en série sur lesquels l'exclusion des anomalies est revendiquée ne peut en général pas être supérieure à 1 % du niveau objectif de défaillances.

3.2.21

tolérance aux anomalies

aptitude d'une entité fonctionnelle à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs

3.2.22

élément terminal

partie du BPCS ou du SIS qui met en œuvre l'action physique nécessaire pour obtenir ou maintenir un état de sécurité

Note 1 à l'article: Des exemples sont les vannes, appareils de commutation et moteurs, comprenant leurs éléments auxiliaires (p. ex.: une électrovanne et un actionneur utilisés pour faire fonctionner une vanne).

3.2.23

sécurité fonctionnelle

sous-ensemble de la sécurité globale se rapportant au processus et au BPCS, qui dépend du fonctionnement correct du SIS et d'autres couches de protection

3.2.24

évaluation de la sécurité fonctionnelle

FSA

recherche, à partir de preuves, destinée à juger de l'état de sécurité fonctionnelle atteint par un ou plusieurs SIS et/ou d'autres couches de protection

Note 1 à l'article: L'abréviation «FSA» est dérivée du terme anglais développé correspondant «functional safety assessment».

3.2.25

audit de la sécurité fonctionnelle

examen systématique et indépendant destiné à déterminer si les procédures spécifiques aux exigences sur la sécurité fonctionnelle sont conformes aux procédures prévues, sont effectivement mises en œuvre et permettent d'atteindre les objectifs spécifiés

Note 1 à l'article: Un audit de la sécurité fonctionnelle peut être mené dans le cadre d'une FSA.

3.2.26

intégrité de sécurité du matériel

partie de l'intégrité de sécurité du SIS liée aux défaillances aléatoires du matériel en mode de défaillance dangereux

Note 1 à l'article: Les deux niveaux de défaillances qui sont pertinents dans ce contexte sont la fréquence moyenne de défaillance dangereuse et la probabilité moyenne de défaillance en cas de sollicitation.

Note 2 à l'article: Voir 3.2.82.

Note 3 à l'article: Cette définition diffère de celle donnée par l'IEC 61508-4:2010 pour refléter les différences dans la terminologie relevant du secteur des industries de transformation.

3.2.27

dommage

blessure ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.2.27.1

événement préjudiciable

événement dangereux qui conduit à un dommage

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés à la situation dangereuse et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence. Un événement dangereux qui a conduit à un dommage est appelé "événement préjudiciable".

3.2.28

danger

source potentielle de dommage

Note 1 à l'article: Ce terme comprend le danger sur des personnes survenant dans un court laps de temps (p. ex.: feu ou explosion), et aussi le danger à long terme sur la santé d'une personne (p. ex.: dégagement d'une substance toxique ou radioactivité).

[SOURCE: ISO/IEC Guide 51:2014, 3.2, modifiée – La Note 1 à l'article a été ajoutée]

3.2.28.1

événement dangereux

événement pouvant conduire à un dommage

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés à la situation dangereuse et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence.

[SOURCE: ISO/IEC Guide 51:2014: 3.3, modifiée – voir Note 1]

3.2.28.2

situation dangereuse

situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs dangers

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.2.29

erreur humaine

action humaine ou absence d'intervention prévue ou non prévue, qui produit un résultat non approprié

Note 1 à l'article: Les fautes, chutes et inattentions constituent des exemples d'erreurs humaines.

Note 2 à l'article: Les actions malveillantes sont exclues.

3.2.30

analyse d'impact

activité consistant à déterminer l'effet que la modification à une fonction ou à un composant d'un système aura sur les autres fonctions ou les autres composants de ce système tout comme sur d'autres systèmes

3.2.31

organisation indépendante

organisation distincte et séparée, par sa direction et ses autres ressources, de celles responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité du SIS et qui est chargée de la FSA ou de la validation

3.2.32

personne indépendante

personne distincte et séparée de celles responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité du SIS, qui est chargée de la FSA ou de la validation, et qui n'a pas de responsabilité directe dans ces activités

3.2.33

fonction d'entrée

fonction qui contrôle le processus et ses équipements associés afin de fournir des informations d'entrée à l'unité logique

Note 1 à l'article: Une fonction d'entrée peut être une fonction manuelle.

3.2.34

instrument

appareil utilisé pour effectuer une action (généralement présent dans les systèmes instrumentés)

3.2.34.1

système instrumenté

système composé de capteurs (p. ex.: transmetteurs de pression, de débit et de température), d'unités logiques (p. ex.: contrôleurs programmables, systèmes de commande distribués, contrôleurs discrets) et d'éléments terminaux (p. ex.: vannes de commande, circuits de commande moteur)

Note 1 à l'article: Les systèmes instrumentés réalisent des fonctions instrumentées, notamment des fonctions de commande, de surveillance, d'alarme et de protection. Les systèmes instrumentés peuvent être des SIS (voir 3.2.67) ou des BPCS (voir 3.2.3).

3.2.35

fonction logique

fonction qui réalise les transformations entre les informations d'entrée (fournies par une ou plusieurs fonctions d'entrée) et les informations de sortie (utilisées par une ou plusieurs fonctions de sortie)

Note 1 à l'article: Les fonctions logiques assurent la transformation d'une ou de plusieurs fonctions d'entrée en une ou plusieurs fonctions de sortie.

Note 2 à l'article: Pour d'autres lignes directrices, voir l'IEC 61131-3:2012 et l'IEC 60617-12:1997.

3.2.36

unité logique

partie d'un BPCS ou d'un SIS qui exécute une ou plusieurs fonctions logiques

Note 1 à l'article: Dans l'IEC 61511, les termes suivants sont utilisés pour désigner des unités logiques:

- systèmes logiques électriques pour la technologie électromécanique;
- systèmes logiques électroniques pour la technologie électronique;
- systèmes logiques programmables (PE) pour les systèmes électroniques programmables.

Note 2 à l'article: Des exemples incluent les systèmes électriques, les systèmes électroniques, les systèmes électroniques programmables, les systèmes pneumatiques et les systèmes hydrauliques. Les capteurs et les éléments terminaux ne font pas partie de l'unité logique.

3.2.36.1

unité logique PE configurée pour la sécurité

unité logique de catégorie "électronique programmable pour usage général industriel" spécifiquement configurée pour être utilisée dans des applications de sécurité

Note 1 à l'article: D'autres lignes directrices peuvent être consultées en 11.5.

3.2.37

interface de maintenance/d'ingénierie

matériels et logiciels fournis pour permettre la maintenance ou la modification ad hoc du SIS

Note 1 à l'article: L'interface de maintenance/d'ingénierie peut comprendre des instructions et des diagnostics, pouvant être trouvés dans le logiciel, les terminaux de programmation avec les protocoles de transmission appropriés, des outils de diagnostic, des indicateurs, des appareils de dérivation, des appareils d'essai, et des appareils d'étalonnage.

3.2.37.1

temps moyen de dépannage

MRT

durée totale de dépannage prévue

Note 1 à l'article: Le MRT comprend les temps (b), (c) et (d) pour les durées applicables à la MTTR (voir 3.2.37.2).

Note 2 à l'article: L'abréviation «MRT» est dérivée du terme anglais développé correspondant «mean repair time».

3.2.37.2

durée moyenne de rétablissement

MTTR

durée prévue de rétablissement effectif

Note 1 à l'article: La MTTR comprend:

- le temps de détection de la défaillance (a);
- le temps écoulé avant de commencer la réparation (b);
- le temps de réparation effectif (c);
- le temps écoulé avant la remise en fonctionnement du composant (d).

Le temps de démarrage applicable à (b) est la fin du temps (a); le temps de démarrage applicable à (c) est la fin du temps (b) et le temps de démarrage applicable à (d) est la fin du temps (c).

Note 2 à l'article: L'abréviation «MTTR» est dérivée du terme anglais développé correspondant «mean time to restoration».

3.2.37.3

temps de dépannage maximal admis

MPRT

durée maximale admise pour réparer une défaillance après sa détection

Note 1 à l'article: Le MRT peut être utilisé comme MPRT, mais le MPRT peut être défini sans rapport avec le MRT:

- Un MPRT inférieur au MRT peut être choisi pour diminuer la probabilité d'un événement dangereux.
- Un MPRT supérieur au MRT peut être choisi si la probabilité d'un événement dangereux peut être réduite.

Note 2 à l'article: Lorsqu'un MPRT a été défini, il peut être utilisé à la place du MRT lors du calcul de la probabilité des défaillances aléatoires du matériel.

Note 3 à l'article: L'abréviation «MPRT» est dérivée du terme anglais développé correspondant «maximum permitted repair time».

3.2.38

atténuation

action qui atténue la (les) conséquence(s) d'un événement dangereux

Note 1 à l'article: Il s'agit, par exemple, de la dépressurisation de secours ou de la fermeture des clapets de ventilation en cas de détection ou de confirmation d'incendie ou de fuite de gaz ou le déclenchement de déluge suite à la détection confirmée d'un incendie.

3.2.39

mode de fonctionnement (d'une SIF)

manière dont fonctionne une SIF qui peut être le mode à faible sollicitation, le mode à sollicitation élevée ou le mode continu

- a) **mode à faible sollicitation:** mode de fonctionnement dans lequel la SIF n'est réalisée que sur sollicitation, afin de faire passer le processus dans un état de sécurité spécifié, et où la fréquence des sollicitations n'est pas supérieure à une par an.
- b) **mode à sollicitation élevée:** mode de fonctionnement dans lequel la SIF n'est réalisée que sur sollicitation, afin de faire passer le processus dans un état de sécurité spécifié, et où la fréquence des sollicitations est supérieure à une par an.
- c) **mode continu:** mode de fonctionnement dans lequel la SIF maintient le processus dans un état de sécurité en fonctionnement normal.

3.2.39.1

SIF en mode sollicitation

fonctionnement de la SIF en mode à faible sollicitation (3.2.39 a)) ou en mode à sollicitation élevée (3.2.39 b))

Note 1 à l'article: Dans l'éventualité d'une défaillance dangereuse de la SIF, un événement dangereux ne peut se produire que:

- si la défaillance n'est pas détectée et qu'une sollicitation survient avant l'essai périodique suivant;
- si la défaillance est détectée par les essais de diagnostic, mais que le processus concerné et ses équipements associés n'ont pas basculé dans un état de sécurité avant qu'une sollicitation ne survienne.

Note 2 à l'article: En mode à sollicitation élevée, il sera normalement approprié d'utiliser les critères du mode continu.

Note 3 à l'article: Les niveaux d'intégrité de sécurité des SIF fonctionnant en mode sollicitation sont définis au Tableau 4 et au Tableau 5.

3.2.39.2

SIF en mode continu

SIF fonctionnant en mode continu (3.2.39 c))