IEC 61511-1

Edition 2.1 2017-08
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONAL

colour inside

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

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

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.

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

IEC 61511-1

Edition 2.1 2017-08
CONSOLIDATED VERSION

REDLINE VERSION

VERSION REDLINE

colour inside

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

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



IEC 61511-12016-02+AMD1:2017-08 CSV(en-fr)

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

© IEC 2017

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.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 61511-1 edition 2.1 contains 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].

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.

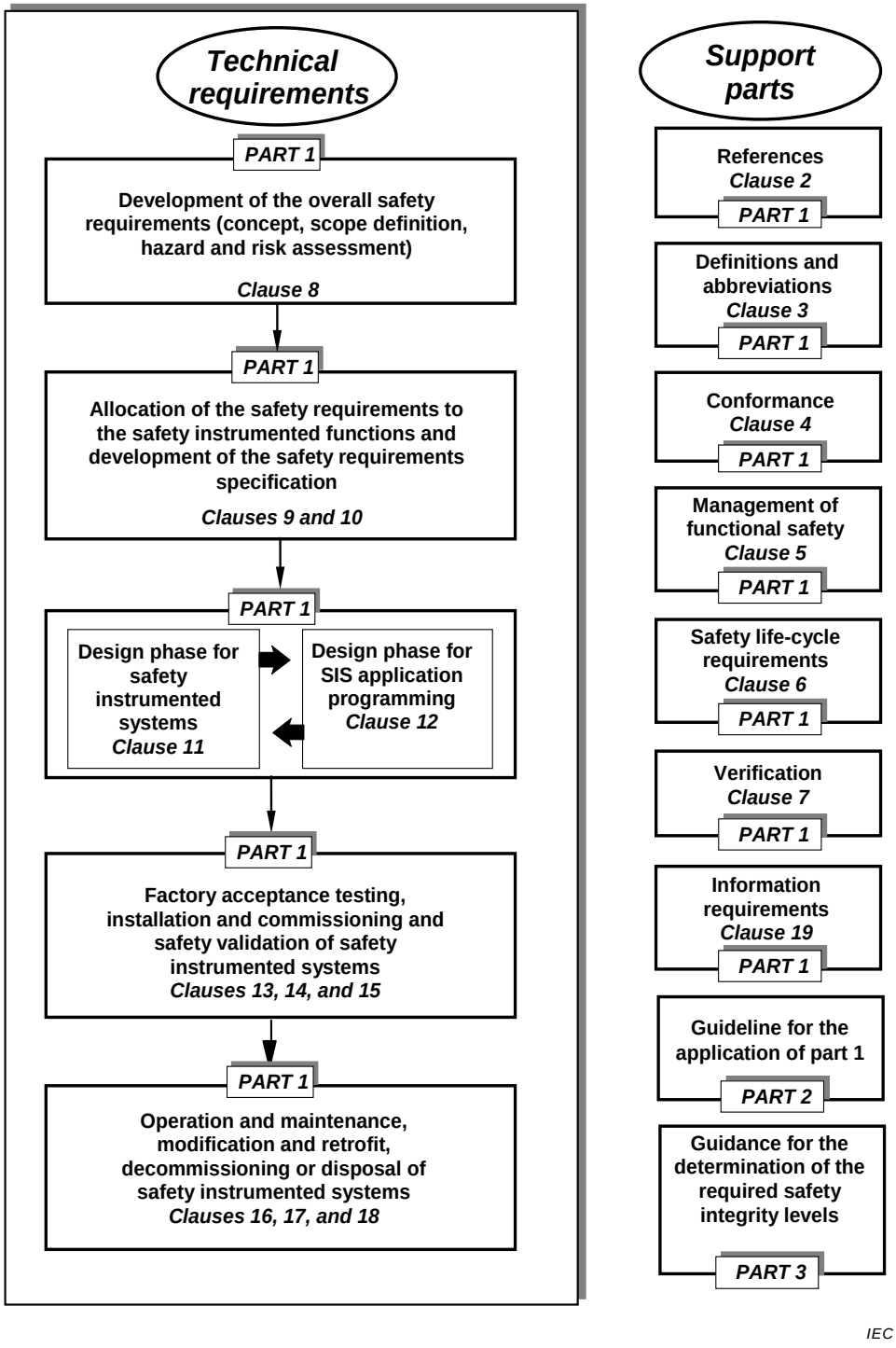


Figure 1 – Overall framework of the IEC 61511 series

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:

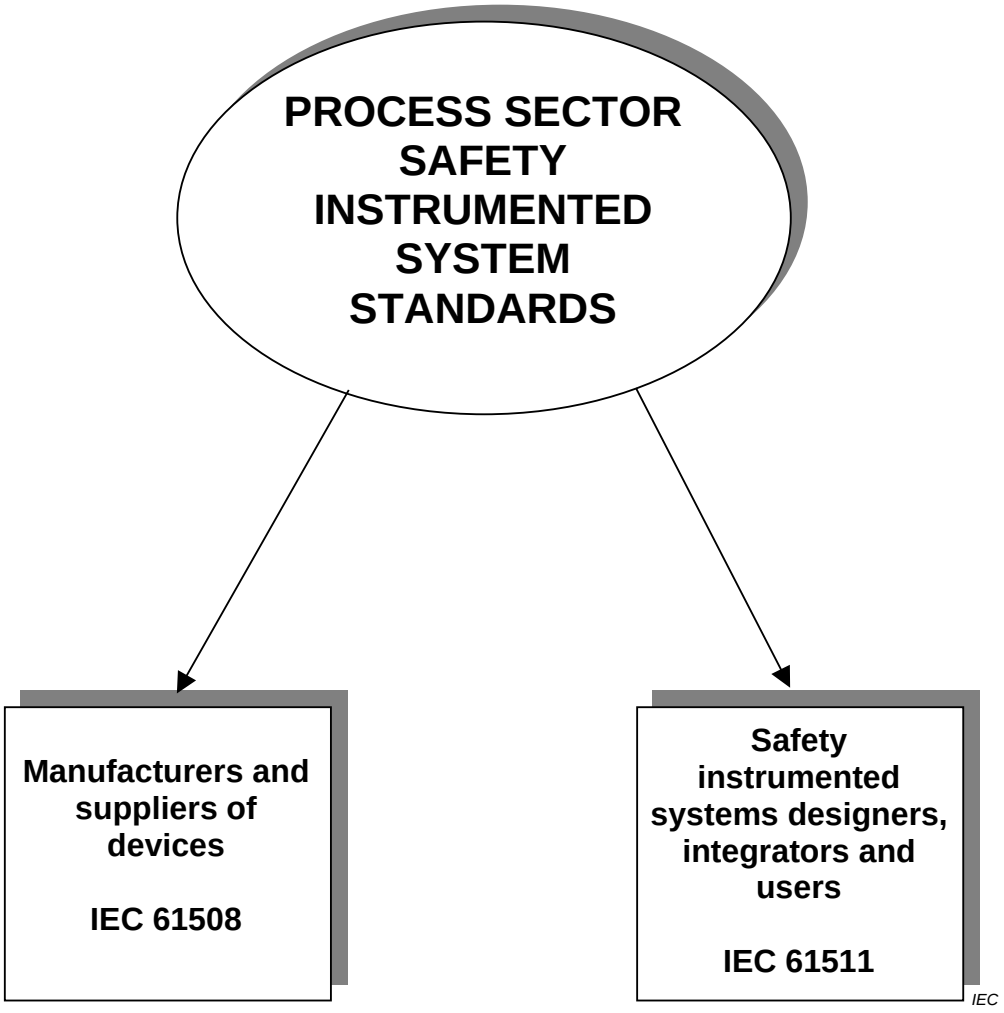


Figure 2 – Relationship between IEC 61511 and IEC 61508

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

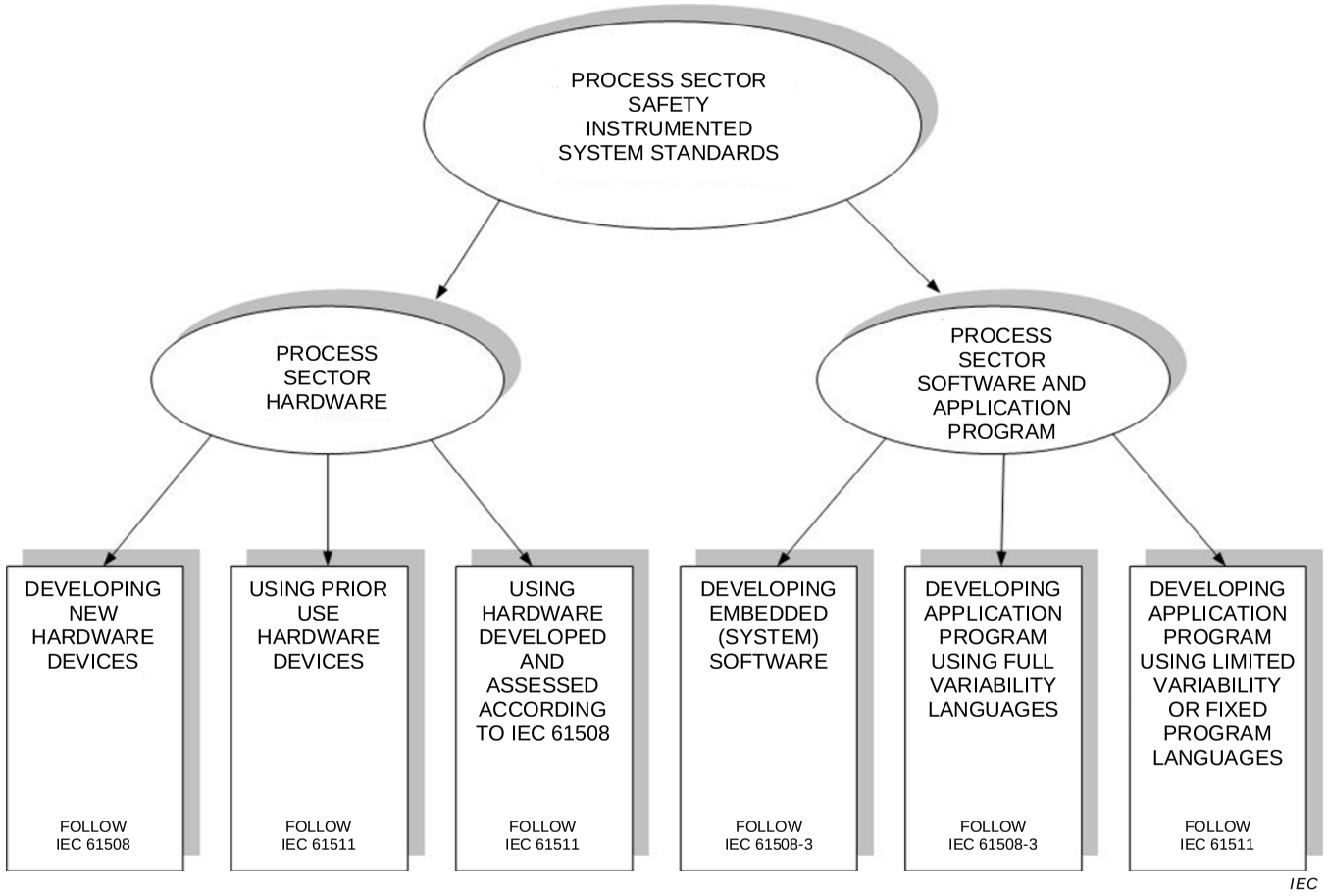


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

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.).

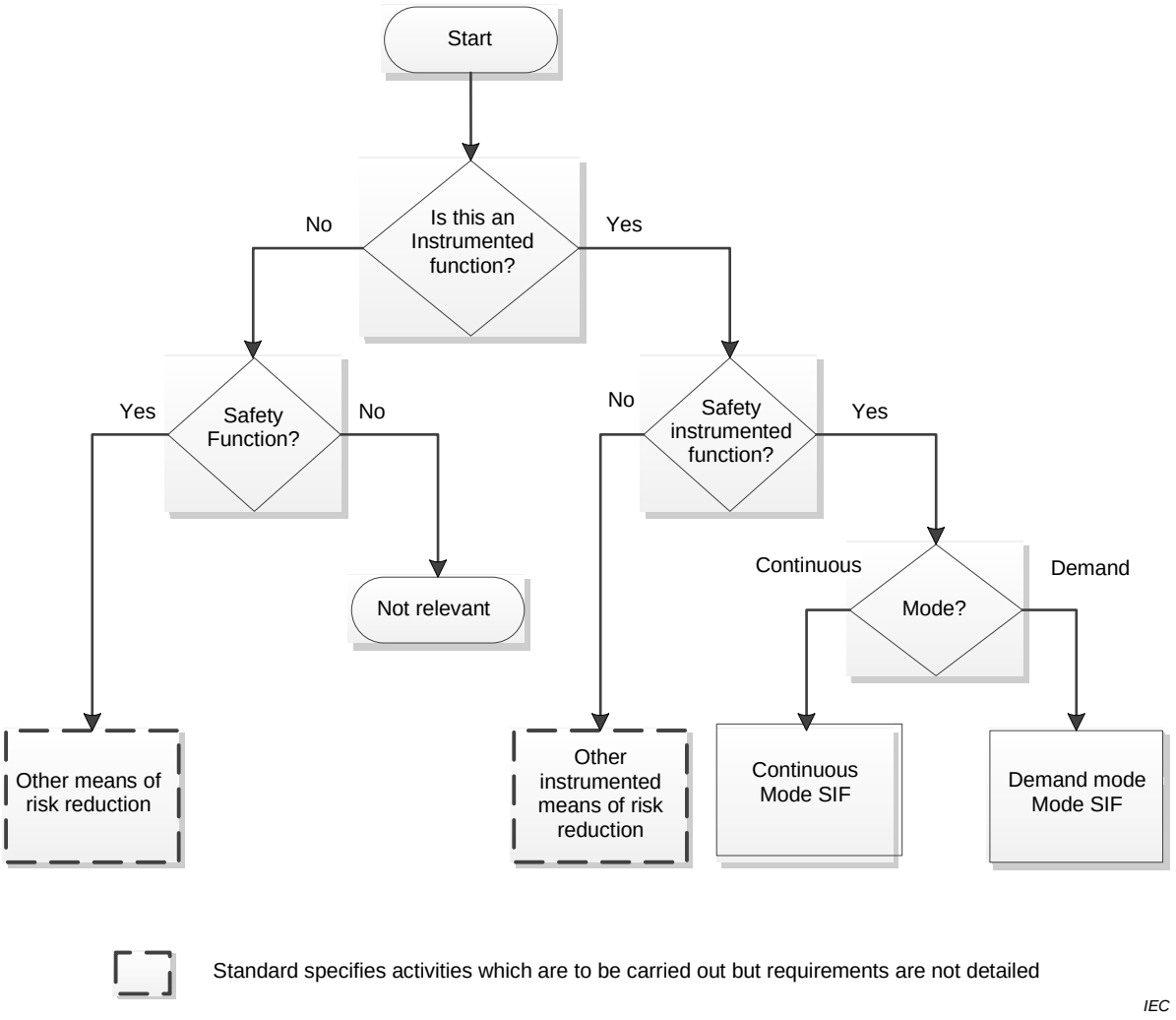


Figure 4 – Relationship between safety instrumented functions and other functions

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*

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

_____

SÉCURITE 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.

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

L'IEC 61511-1 édition 2.1 contient 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].

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:

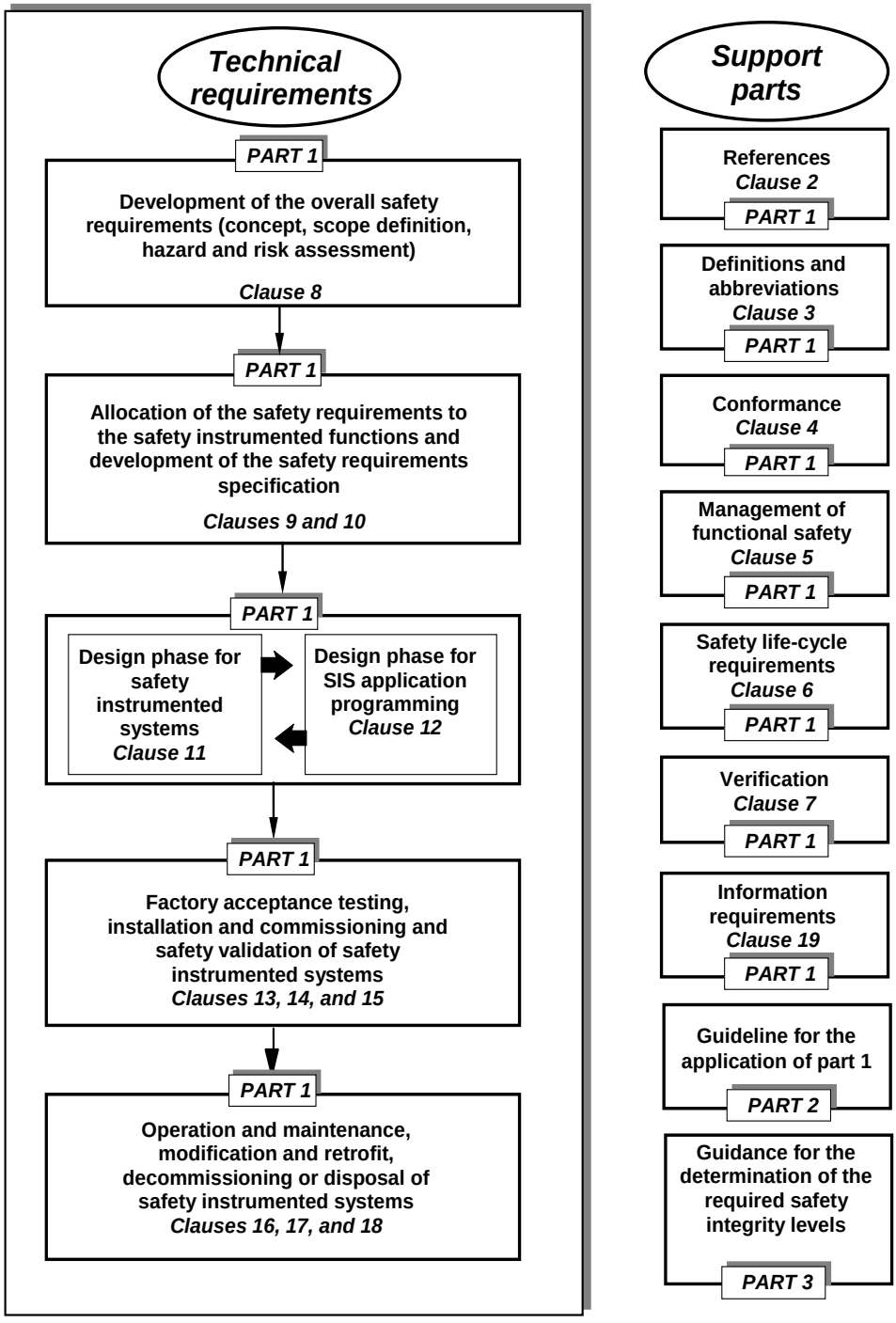
- aborde la réalisation d'une analyse de danger et de risque pour identifier les exigences de sécurité globales;
- prend en compte l'affectation des exigences de sécurité aux SIS;
- s'inscrit dans un cadre applicable à tous les moyens instrumentés qui permettent d'obtenir la sécurité fonctionnelle;
- 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.


Technical requirements
PART 1
Development of the overall safety requirements (concept, scope definition, hazard and risk assessment)
Clause 8
PART 1
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification
Clauses 9 and 10
PART 1
Design phase for safety instrumented systems
Clause 11
Design phase for SIS application programming
Clause 12
PART 1
Factory acceptance testing, installation and commissioning and safety validation of safety instrumented systems
Clauses 13, 14, and 15
PART 1
Operation and maintenance, modification and retrofit, decommissioning or disposal of safety instrumented systems
Clauses 16, 17, and 18
Support parts
References
Clause 2
PART 1
Definitions and abbreviations
Clause 3
PART 1
Conformance
Clause 4
PART 1
Management of functional safety
Clause 5
PART 1
Safety life-cycle requirements
Clause 6
PART 1
Verification
Clause 7
PART 1
Information requirements
Clause 19
PART 1
Guideline for the application of part 1
PART 2
Guidance for the determination of the required safety integrity levels
PART 3
IEC

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

SÉCURITE 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 [11.5] 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;

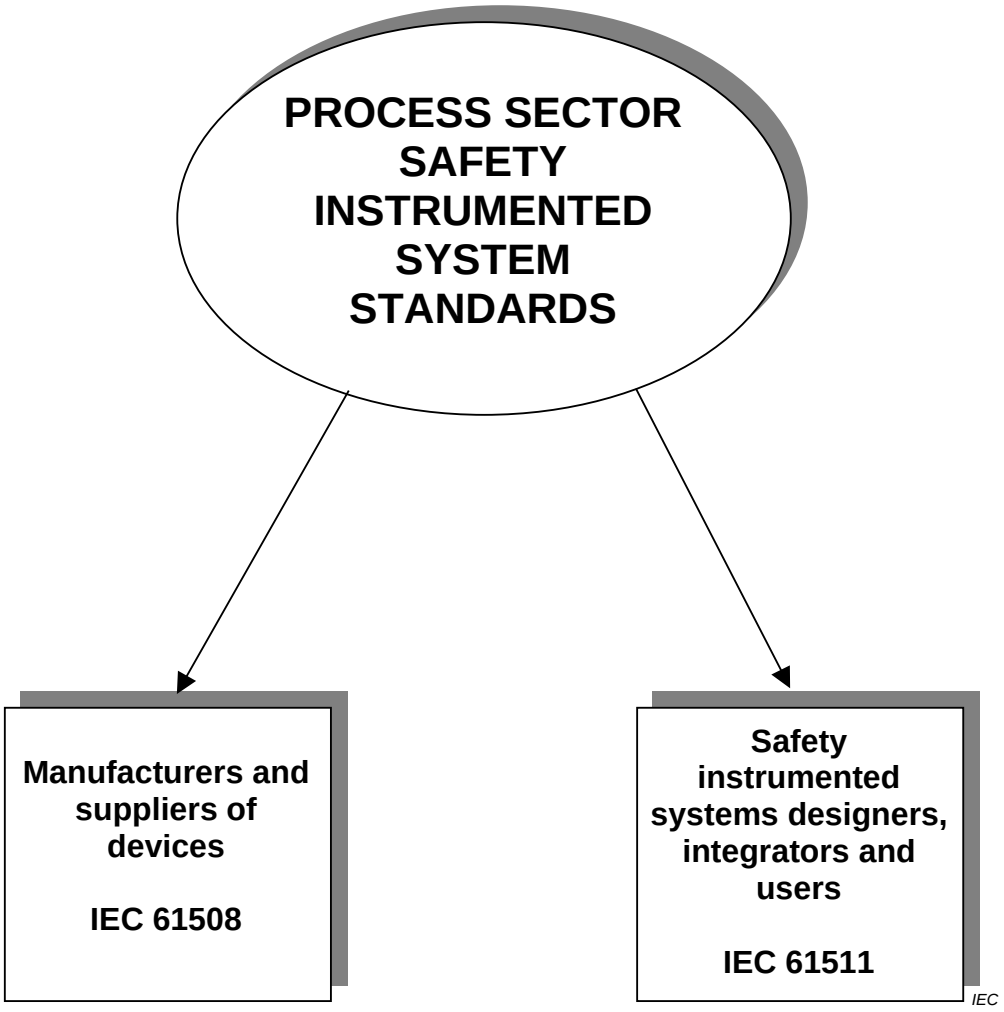
t) fournit un cadre pour l'établissement du SIL, mais ne spécifie pas le SIL exigé pour les applications spécifiques (qu'il convient d'établir sur la base de la connaissance de l'application particulière et par rapport à la réduction de risque globale souhaitée);

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;

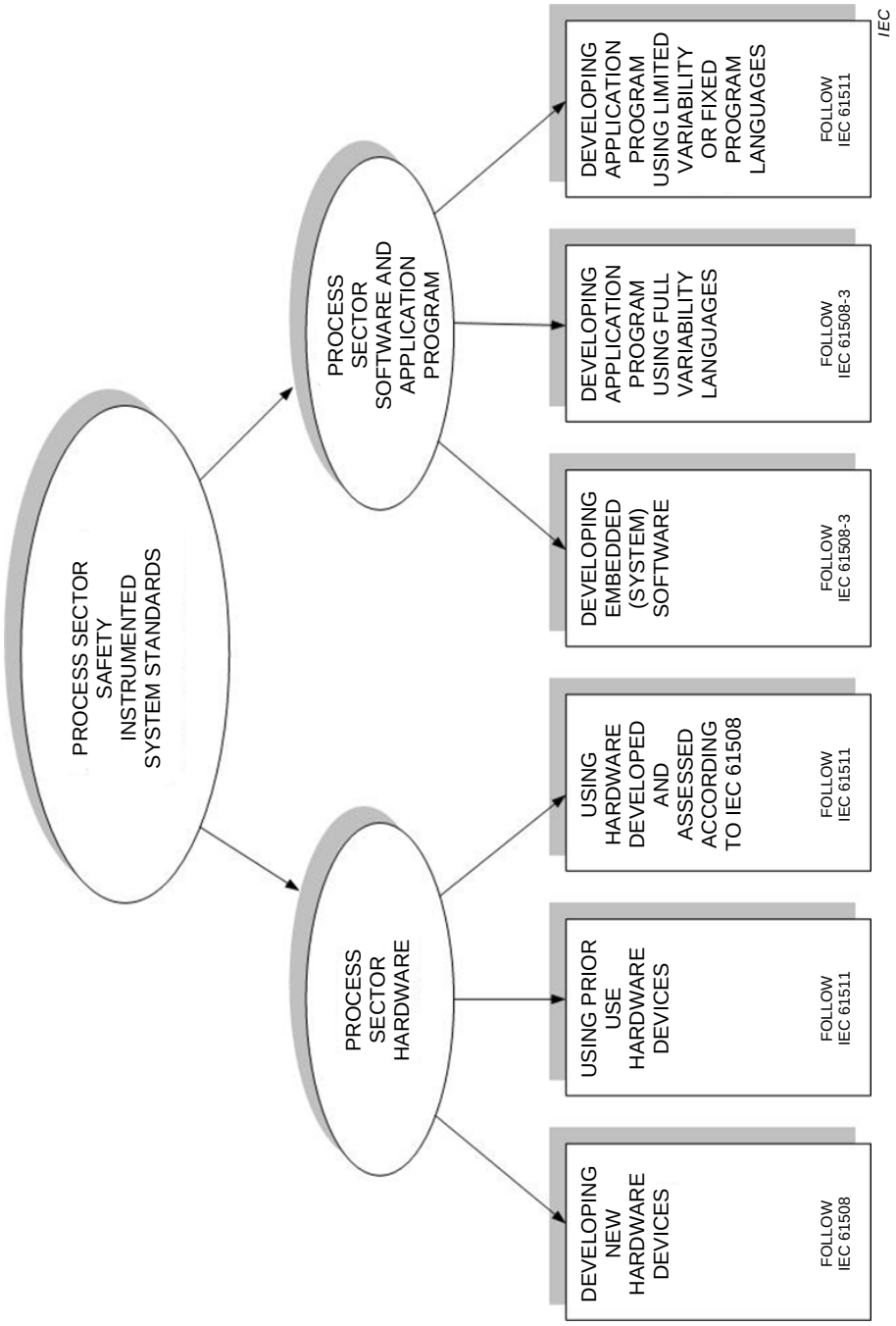
x) n'applique aucune exigence directe relative à l'opérateur individuel ou au technicien de maintenance.



Anglais	Français
PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS	NORMES RELATIVES AUX SYSTEMES INSTRUMENTES DE SECURITE DANS LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
Manufacturers and suppliers of devices	Fabricants et fournisseurs d'appareils
IEC 61508	IEC 61508
Safety instrumented systems designers, integrators and users	Concepteurs, intégrateurs et utilisateurs de systèmes instrumentés de sécurité
IEC 61511	IEC 61511

Figure 2 – Relations entre l'IEC 61511 et l'IEC 61508

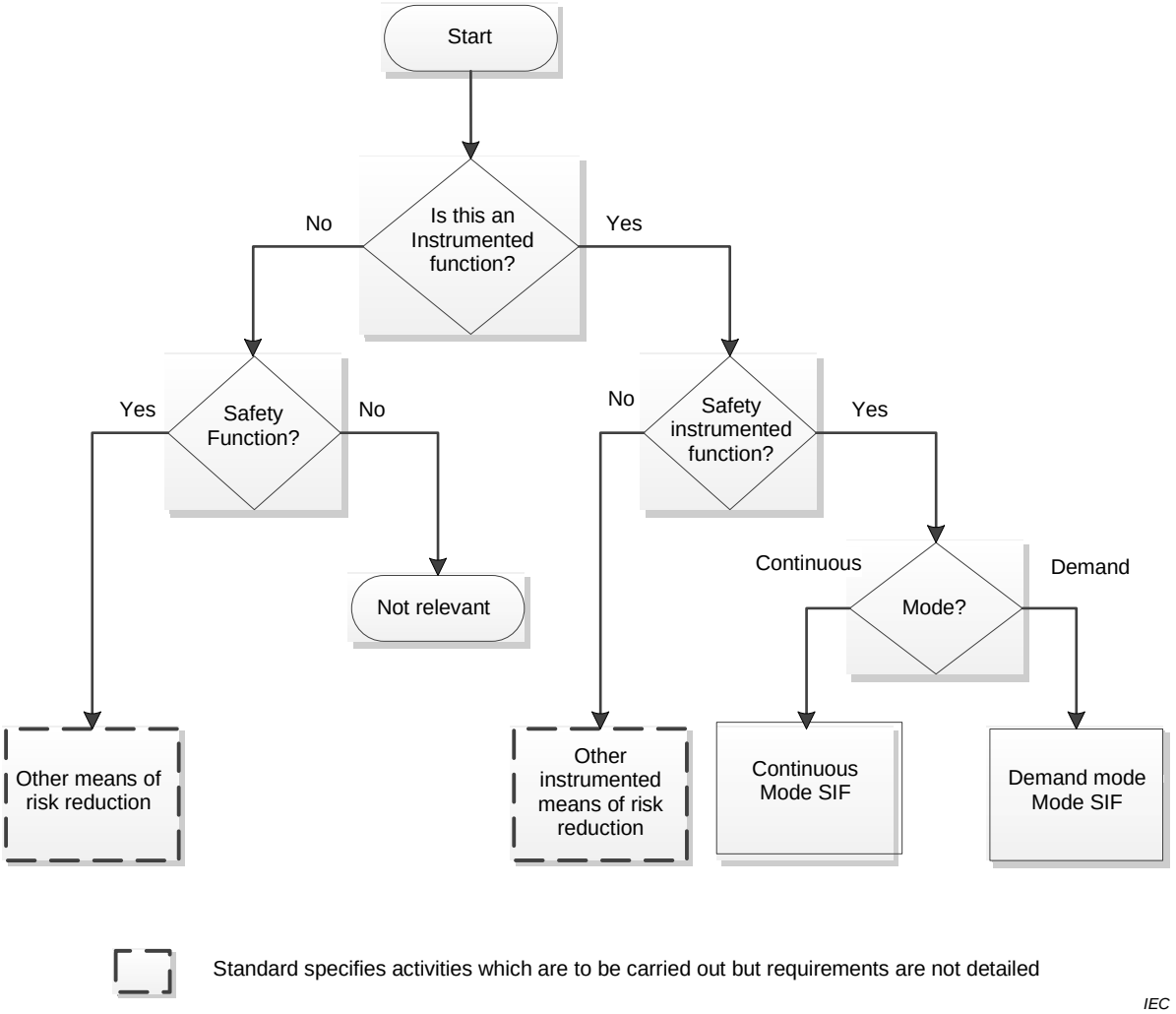
NOTE 3 L'IEC 61508 est également utilisée par les concepteurs, intégrateurs et utilisateurs de SIS lorsque cela est indiqué dans l'IEC 61511.


PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS
PROCESS SECTOR SOFTWARE AND APPLICATION PROGRAM
PROCESS SECTOR HARDWARE
DEVELOPING APPLICATION PROGRAM USING LIMITED VARIABILITY OR FIXED PROGRAM LANGUAGES
FOLLOW IEC 61511
DEVELOPING APPLICATION PROGRAM USING FULL VARIABILITY LANGUAGES
FOLLOW IEC 61508-3
DEVELOPING EMBEDDED (SYSTEM) SOFTWARE
FOLLOW IEC 61508-3
USING HARDWARE DEVELOPED AND ASSESSED ACCORDING TO IEC 61508
FOLLOW IEC 61511
USING PRIOR USE HARDWARE DEVICES
FOLLOW IEC 61511
DEVELOPING NEW HARDWARE DEVICES
FOLLOW IEC 61508
IEC

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.



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*

IEC 61511-1

Edition 2.1 2017-08
CONSOLIDATED VERSION

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 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



IEC 61511-12016-02+AMD1:2017-08 CSV(en-fr)

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

© IEC 2017

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.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 61511-1 edition 2.1 contains 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].

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.

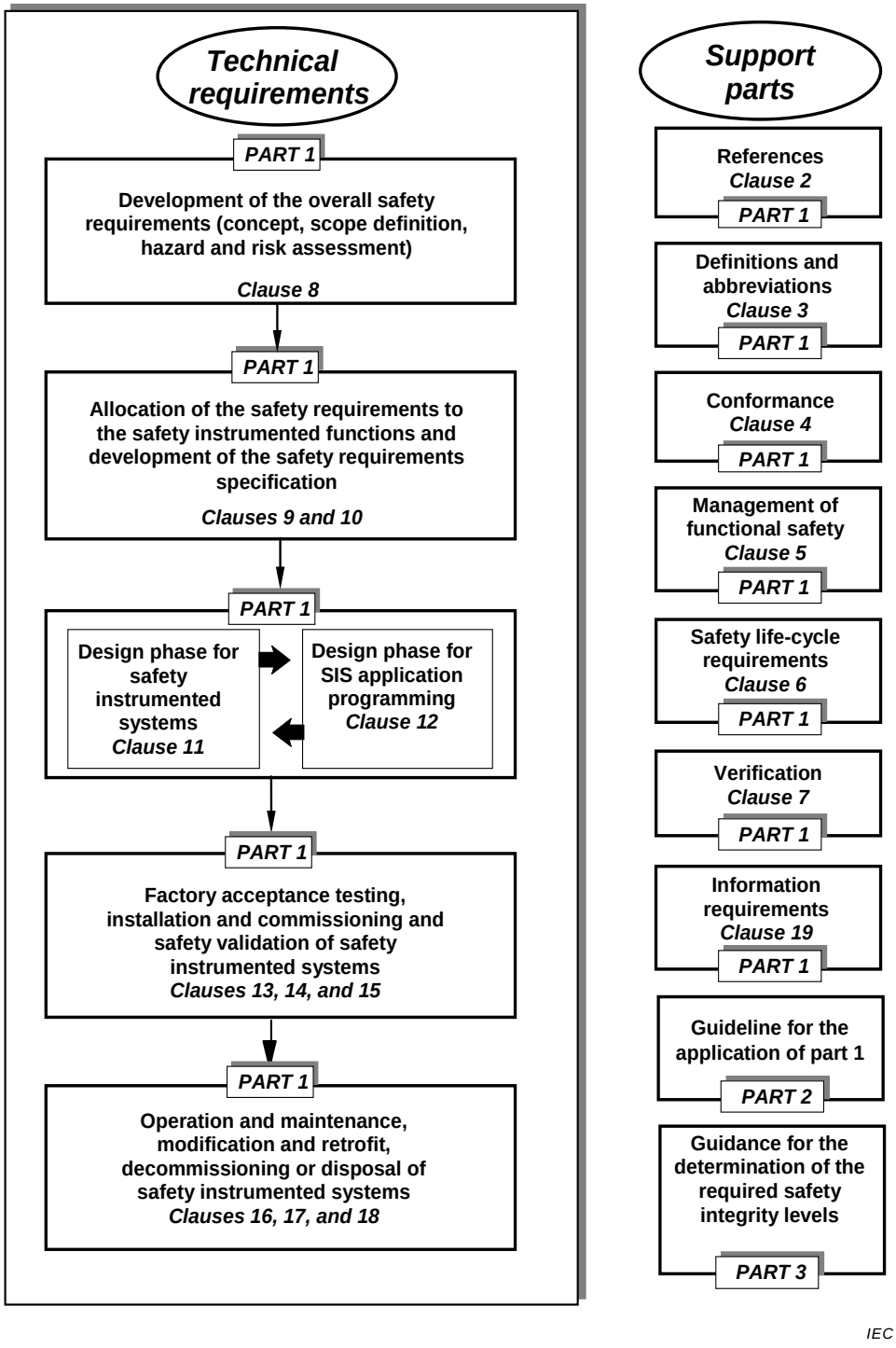


Figure 1 – Overall framework of the IEC 61511 series

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:

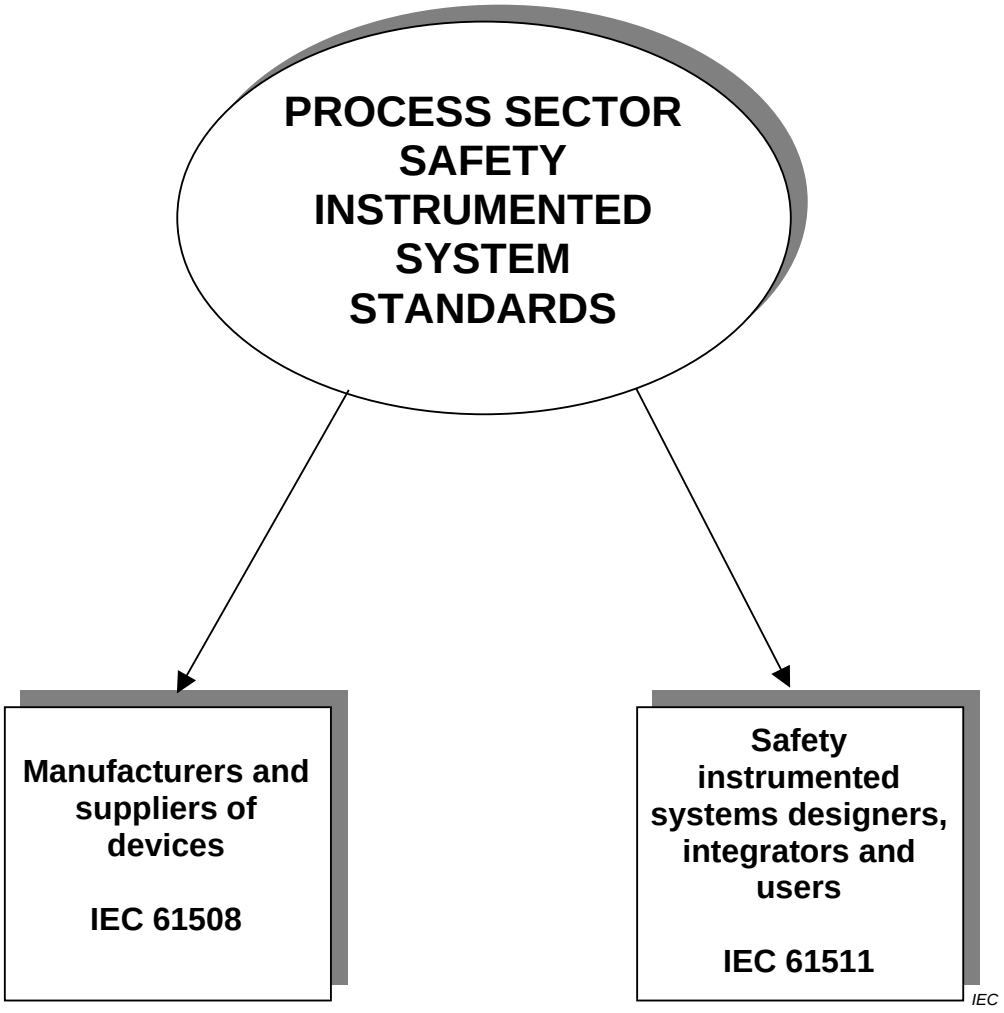


Figure 2 – Relationship between IEC 61511 and IEC 61508

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

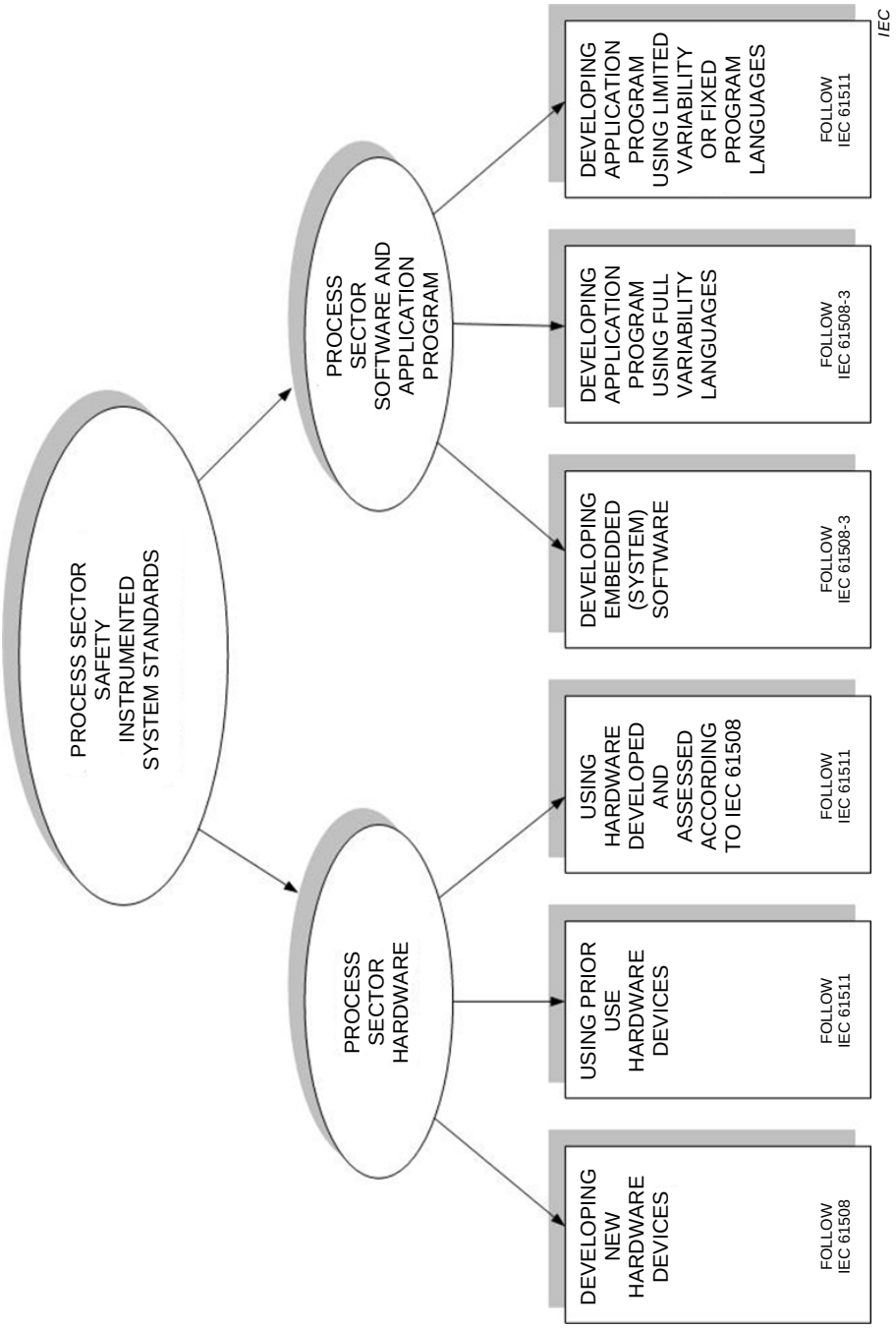


Figure 3 – Detailed relationship between IEC 61511 and IEC 61508

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.).

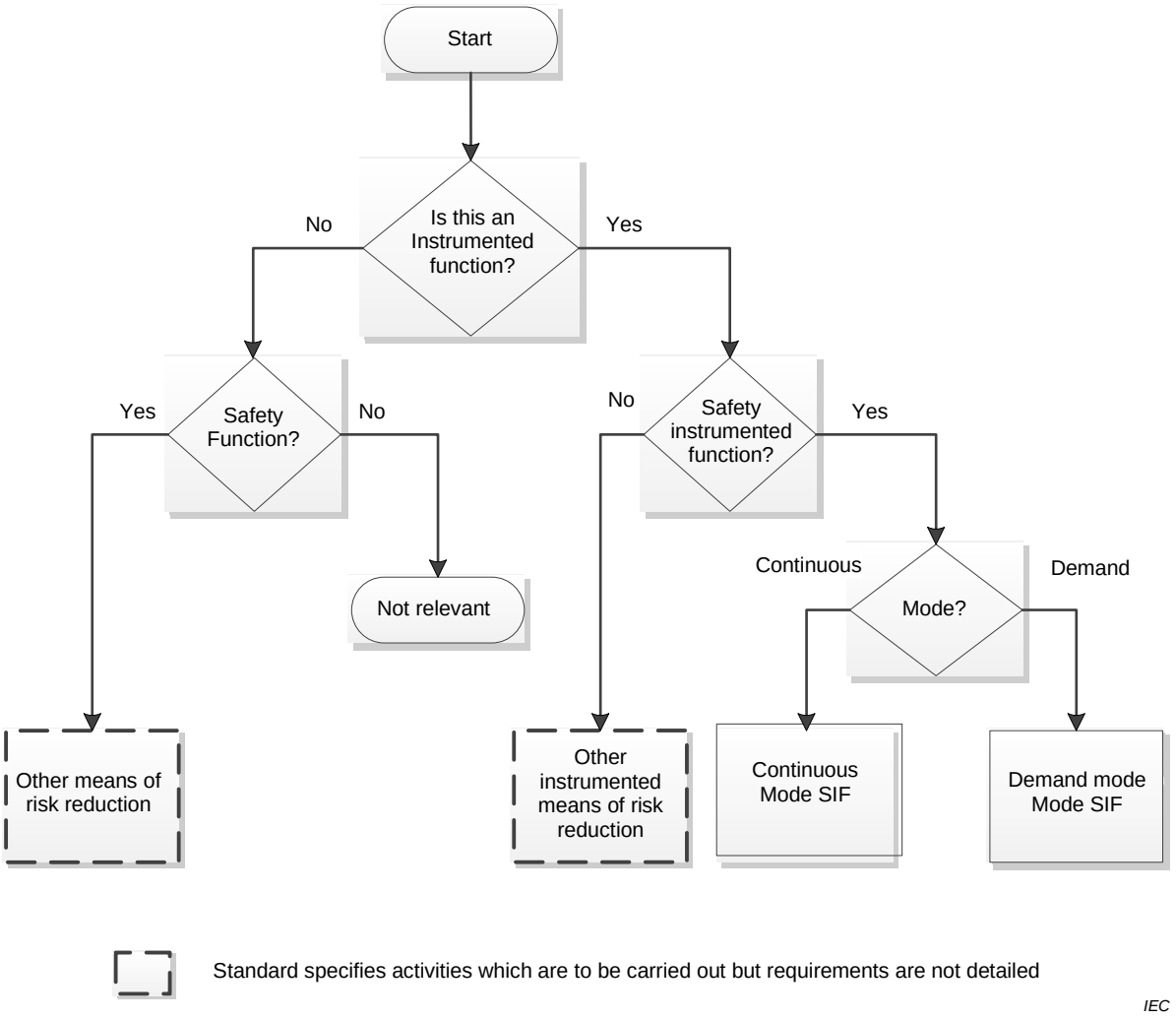


Figure 4 – Relationship between safety instrumented functions and other functions

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*

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

_____

SÉCURITE 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.

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

L'IEC 61511-1 édition 2.1 contient 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].

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:

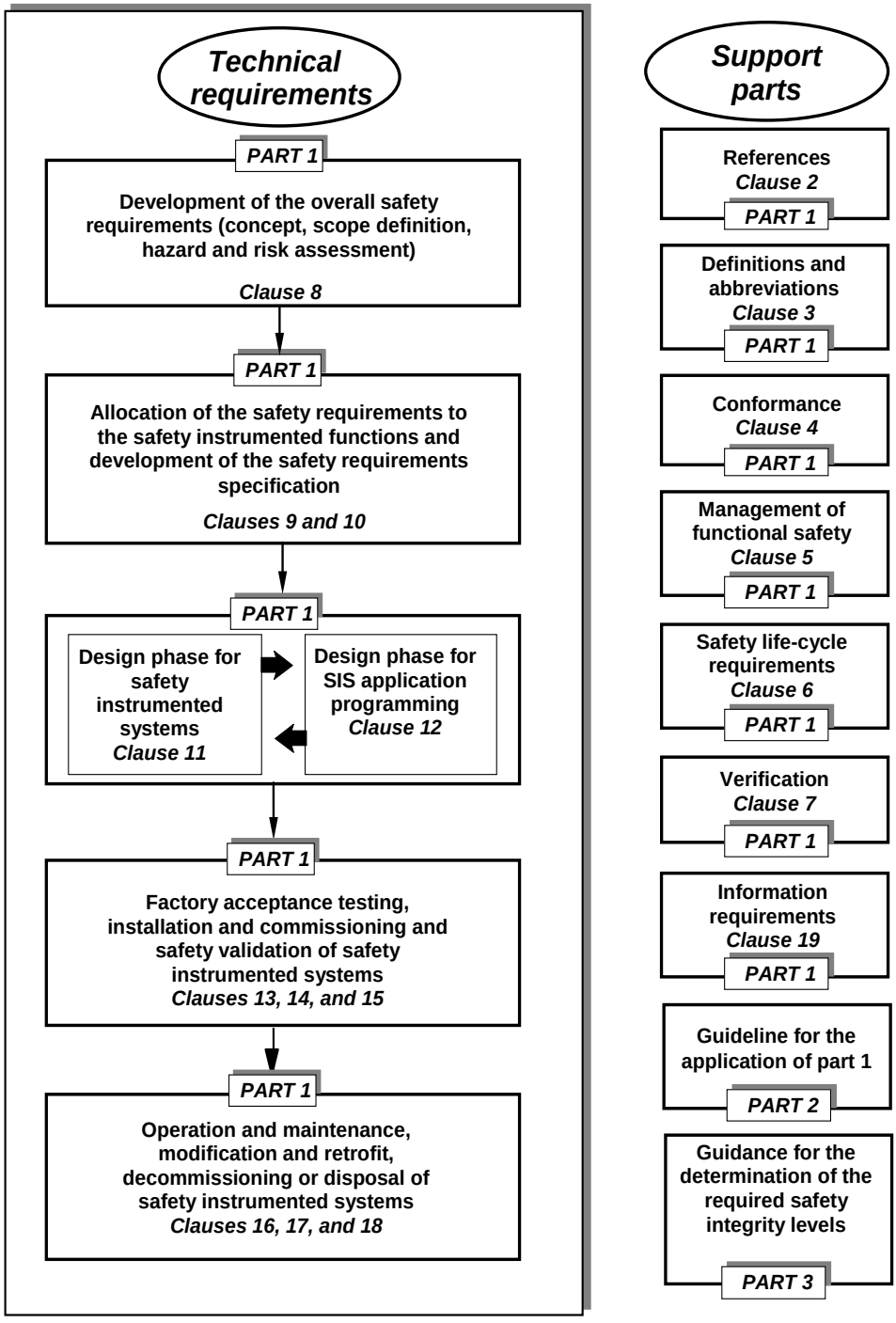
- aborde la réalisation d'une analyse de danger et de risque pour identifier les exigences de sécurité globales;
- prend en compte l'affectation des exigences de sécurité aux SIS;
- s'inscrit dans un cadre applicable à tous les moyens instrumentés qui permettent d'obtenir la sécurité fonctionnelle;
- 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.


Technical requirements
PART 1
Development of the overall safety requirements (concept, scope definition, hazard and risk assessment)
Clause 8
PART 1
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification
Clauses 9 and 10
PART 1
Design phase for safety instrumented systems
Clause 11
Design phase for SIS application programming
Clause 12
PART 1
Factory acceptance testing, installation and commissioning and safety validation of safety instrumented systems
Clauses 13, 14, and 15
PART 1
Operation and maintenance, modification and retrofit, decommissioning or disposal of safety instrumented systems
Clauses 16, 17, and 18
Support parts
References
Clause 2
PART 1
Definitions and abbreviations
Clause 3
PART 1
Conformance
Clause 4
PART 1
Management of functional safety
Clause 5
PART 1
Safety life-cycle requirements
Clause 6
PART 1
Verification
Clause 7
PART 1
Information requirements
Clause 19
PART 1
Guideline for the application of part 1
PART 2
Guidance for the determination of the required safety integrity levels
PART 3
IEC

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

SÉCURITE 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 [11.5] 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;

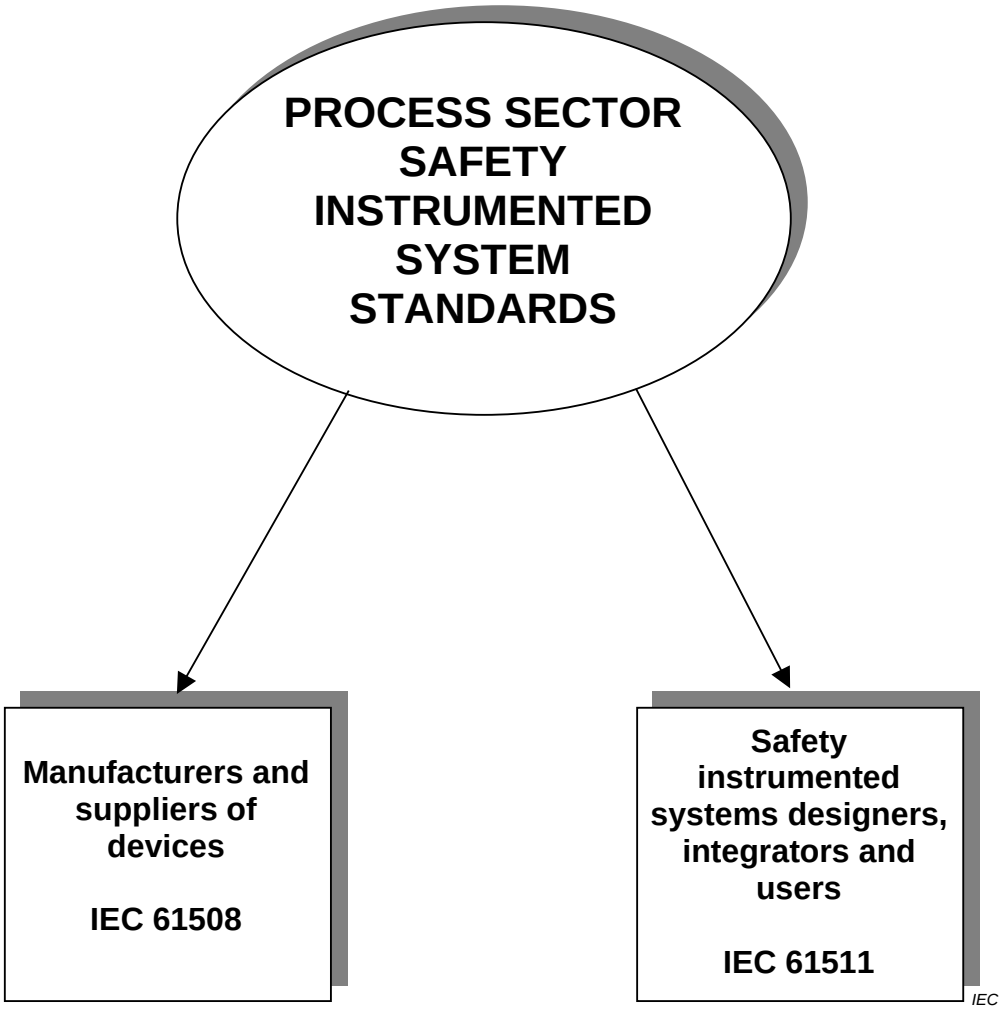
t) fournit un cadre pour l'établissement du SIL, mais ne spécifie pas le SIL exigé pour les applications spécifiques (qu'il convient d'établir sur la base de la connaissance de l'application particulière et par rapport à la réduction de risque globale souhaitée);

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;

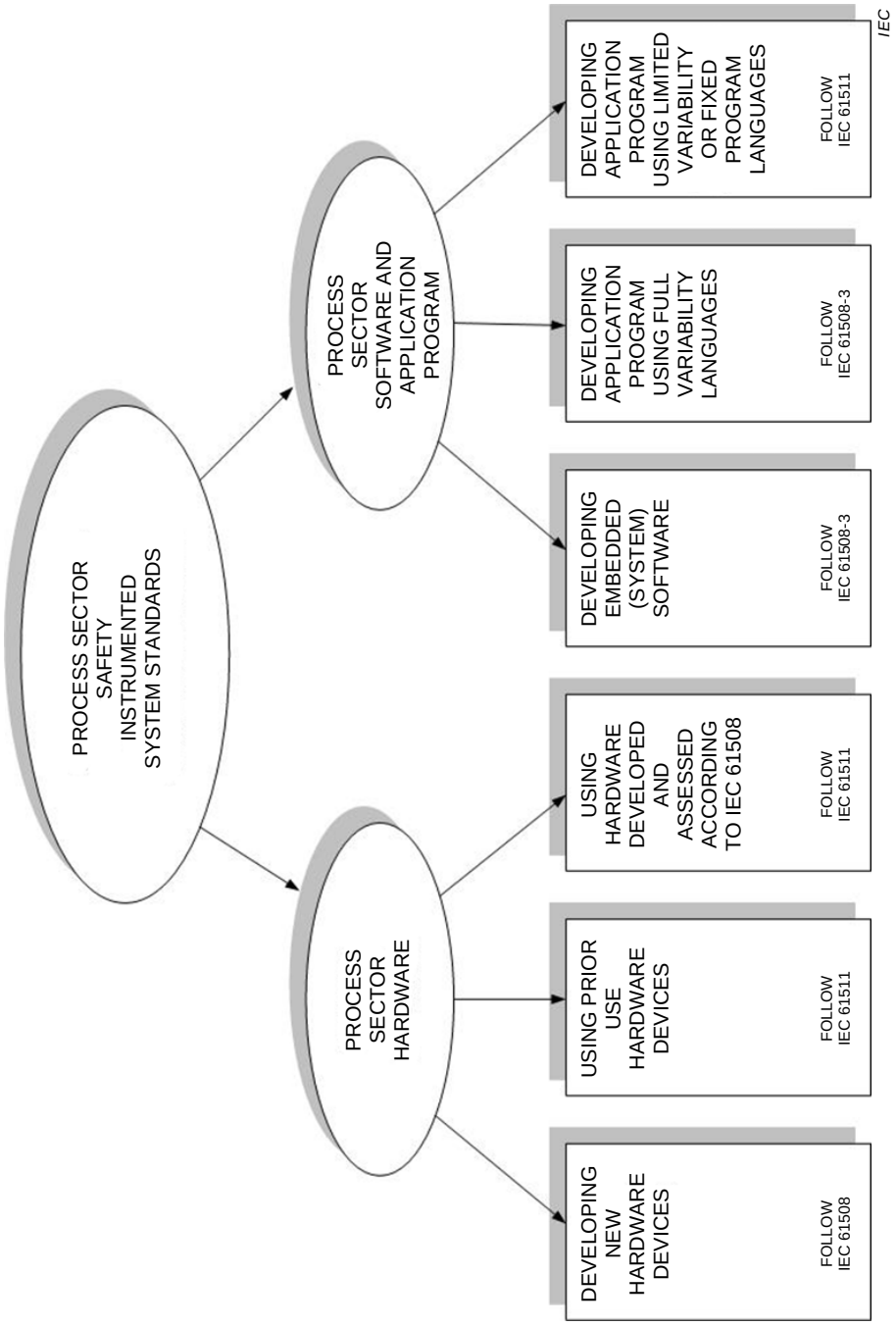
x) n'applique aucune exigence directe relative à l'opérateur individuel ou au technicien de maintenance.



Anglais	Français
PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS	NORMES RELATIVES AUX SYSTEMES INSTRUMENTES DE SECURITE DANS LE SECTEUR DES INDUSTRIES DE TRANSFORMATION
Manufacturers and suppliers of devices	Fabricants et fournisseurs d'appareils
IEC 61508	IEC 61508
Safety instrumented systems designers, integrators and users	Concepteurs, intégrateurs et utilisateurs de systèmes instrumentés de sécurité
IEC 61511	IEC 61511

Figure 2 – Relations entre l'IEC 61511 et l'IEC 61508

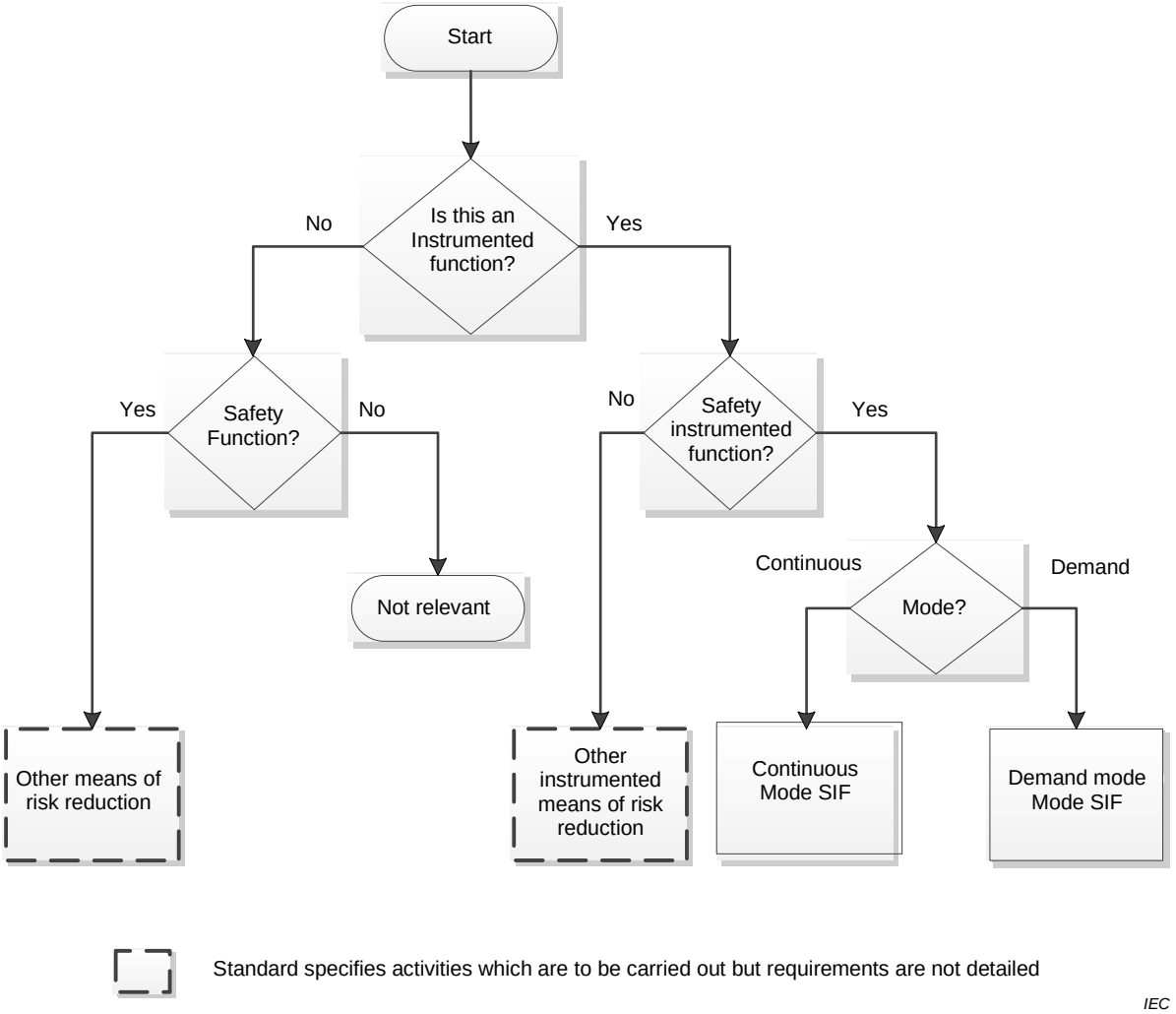
NOTE 3 L'IEC 61508 est également utilisée par les concepteurs, intégrateurs et utilisateurs de SIS lorsque cela est indiqué dans l'IEC 61511.


PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS
PROCESS SECTOR SOFTWARE AND APPLICATION PROGRAM
PROCESS SECTOR HARDWARE
DEVELOPING APPLICATION PROGRAM USING LIMITED VARIABILITY OR FIXED PROGRAM LANGUAGES
FOLLOW IEC 61511
DEVELOPING APPLICATION PROGRAM USING FULL VARIABILITY LANGUAGES
FOLLOW IEC 61508-3
DEVELOPING EMBEDDED (SYSTEM) SOFTWARE
FOLLOW IEC 61508-3
USING HARDWARE DEVELOPED AND ASSESSED ACCORDING TO IEC 61508
FOLLOW IEC 61511
USING PRIOR USE HARDWARE DEVICES
FOLLOW IEC 61511
DEVELOPING NEW HARDWARE DEVICES
FOLLOW IEC 61508
IEC

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.



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*