



INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

**Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des
industries de transformation –
Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE **XC**
CODE PRIX

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	10
2 Normative references	16
3 Abbreviations and definitions.....	16
3.1 Abbreviations	16
3.2 Definitions	17
4 Conformance to this International Standard	33
5 Management of functional safety	33
5.1 Objective	33
5.2 Requirements	33
6 Safety life-cycle requirements.....	38
6.1 Objective	38
6.2 Requirements	38
7 Verification	41
7.1 Objective	41
8 Process hazard and risk analysis	41
8.1 Objectives	41
8.2 Requirements	42
9 Allocation of safety functions to protection layers	43
9.1 Objective	43
9.2 Requirements of the allocation process	43
9.3 Additional requirements for safety integrity level 4.....	44
9.4 Requirements on the basic process control system as a protection layer.....	45
9.5 Requirements for preventing common cause, common mode and dependent failures	46
10 SIS safety requirements specification	46
10.1 Objective	46
10.2 General requirements.....	46
10.3 SIS safety requirements	46
11 SIS design and engineering.....	48
11.1 Objective	48
11.2 General requirements.....	48
11.3 Requirements for system behaviour on detection of a fault.....	48
11.4 Requirements for hardware fault tolerance	51
11.5 Requirements for selection of components and subsystems	52
11.6 Field devices	56
11.7 Interfaces	56
11.8 Maintenance or testing design requirements.....	58
11.9 SIF probability of failure	59

12	Requirements for application software, including selection criteria for utility software	60
12.1	Application software safety life-cycle requirements	60
12.2	Application software safety requirements specification	66
12.3	Application software safety validation planning	68
12.4	Application software design and development	68
12.5	Integration of the application software with the SIS subsystem	74
12.6	FPL and LVL software modification procedures	75
12.7	Application software verification	75
13	Factory acceptance testing (FAT)	76
13.1	Objectives	76
13.2	Recommendations	77
14	SIS installation and commissioning	78
14.1	Objectives	78
14.2	Requirements	78
15	SIS safety validation	79
15.1	Objective	79
15.2	Requirements	79
16	SIS operation and maintenance	82
16.1	Objectives	82
16.2	Requirements	82
16.3	Proof testing and inspection	84
17	SIS modification	85
17.1	Objective	85
17.2	Requirements	85
18	SIS decommissioning	86
18.1	Objectives	86
18.2	Requirements	86
19	Information and documentation requirements	86
19.1	Objectives	86
19.2	Requirements	87
	Annex A (informative) Differences	88
	Bibliography	89
	Figure 1 – Overall framework of this standard	9
	Figure 2 – Relationship between IEC 61511 and IEC 61508	12
	Figure 3 – Relationship between IEC 61511 and IEC 61508 (see 1.2)	13
	Figure 4 – Relationship between safety instrumented functions and other functions	14
	Figure 5 – Relationship between system, hardware, and software of IEC 61511-1	15
	Figure 6 – Programmable electronic system (PES): structure and terminology	25
	Figure 7 – Example SIS architecture	28
	Figure 8 – SIS safety life-cycle phases and functional safety assessment stages	36
	Figure 9 – Typical risk reduction methods found in process plants	45

Figure 10 – Application software safety life cycle and its relationship to the SIS safety life cycle	61
Figure 11 – Application software safety life cycle (in realization phase)	63
Figure 12 – Software development life cycle (the V-model)	63
Figure 13 – Relationship between the hardware and software architectures of SIS	66
Table 1 – Abbreviations used in IEC 61511.....	16
Table 2 – SIS safety life-cycle overview	39
Table 3 – Safety integrity levels: probability of failure on demand	43
Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF	44
Table 5 – Minimum hardware fault tolerance of PE logic solvers	51
Table 6 – Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers	52
Table 7 – Application software safety life cycle: overview	64

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 1: Framework, definitions, system, hardware and software 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This bilingual version, published in 2003-12, corresponds to the English version.

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

FDIS	Report on voting
65A/368/FDIS	65A/372/RVD

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

The French version of this standard has not been voted upon.

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

IEC 61511 consists of the following parts, under the general title *Functional safety: Safety instrumented systems for the process industry sector* (see Figure 1):

Part 1: Framework, definitions, system, hardware and software requirements

Part 2: Guidelines in the application of IEC 61511-1

Part 3: Guidance for the determination of the required safety integrity levels

The committee has decided that the contents of this publication will remain unchanged until 2007. At this date, the publication will be

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

The contents of the corrigendum of November 2004 have been included in this copy.

INTRODUCTION

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

This standard addresses the application of safety instrumented systems for the process industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. Other safety systems are only considered so that their contribution can be taken into account when considering the performance requirements for the safety instrumented systems. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

This standard has two concepts which are fundamental to its application; safety lifecycle and safety integrity levels.

This standard addresses safety instrumented systems which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This standard is process industry specific within the framework of IEC 61508 (see Annex A).

This standard sets out an approach for safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. 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, programmable electronic). To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

This standard on safety instrumented systems for the process industry

- addresses all 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 this standard.

This International Standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example, national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

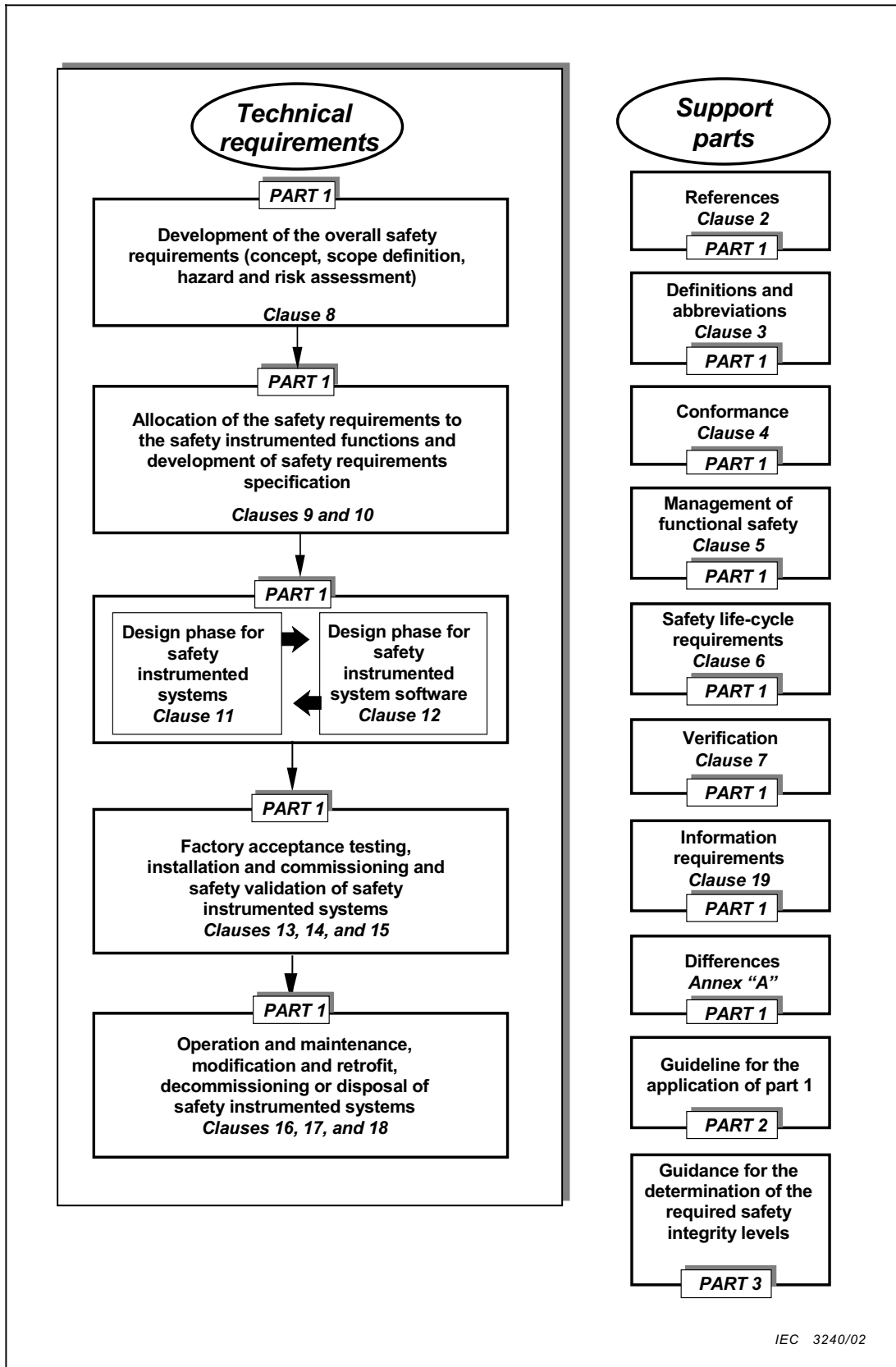


Figure 1 – Overall framework of this standard

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

Part 1: Framework, definitions, system, hardware and software requirements

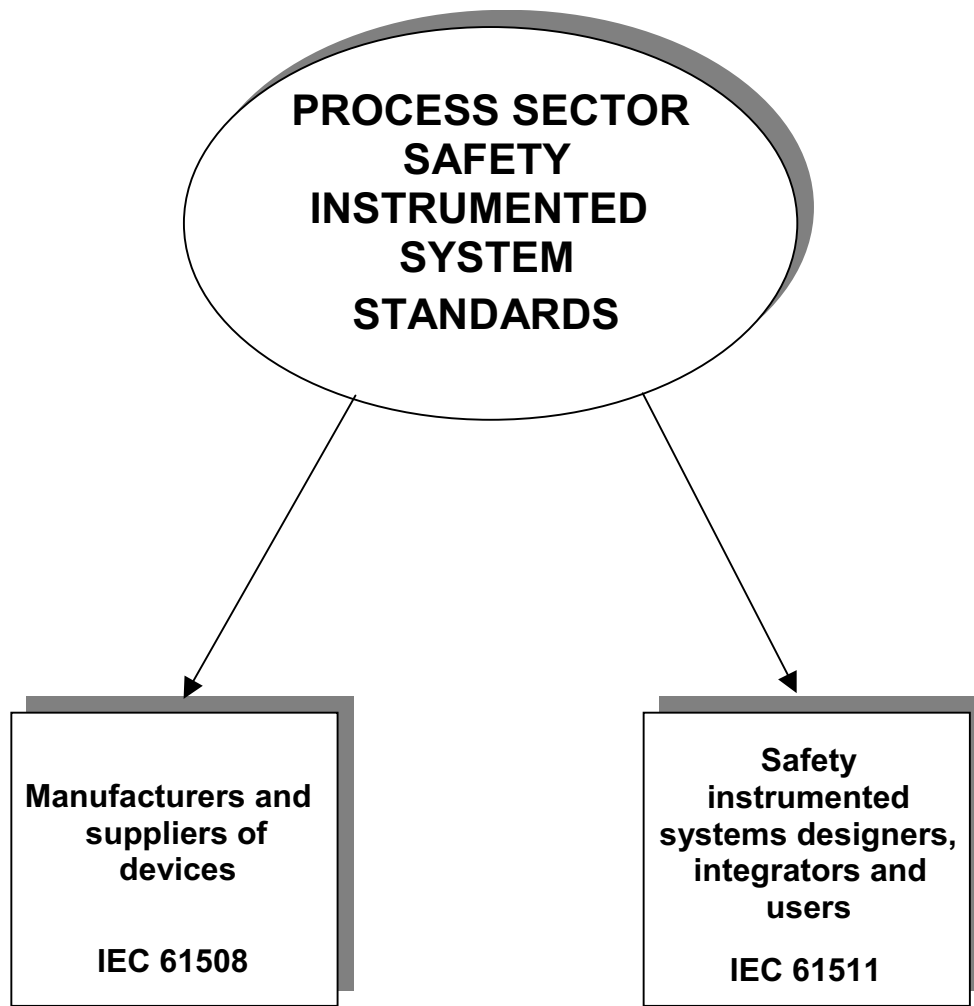
1 Scope

This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.

In particular, this standard

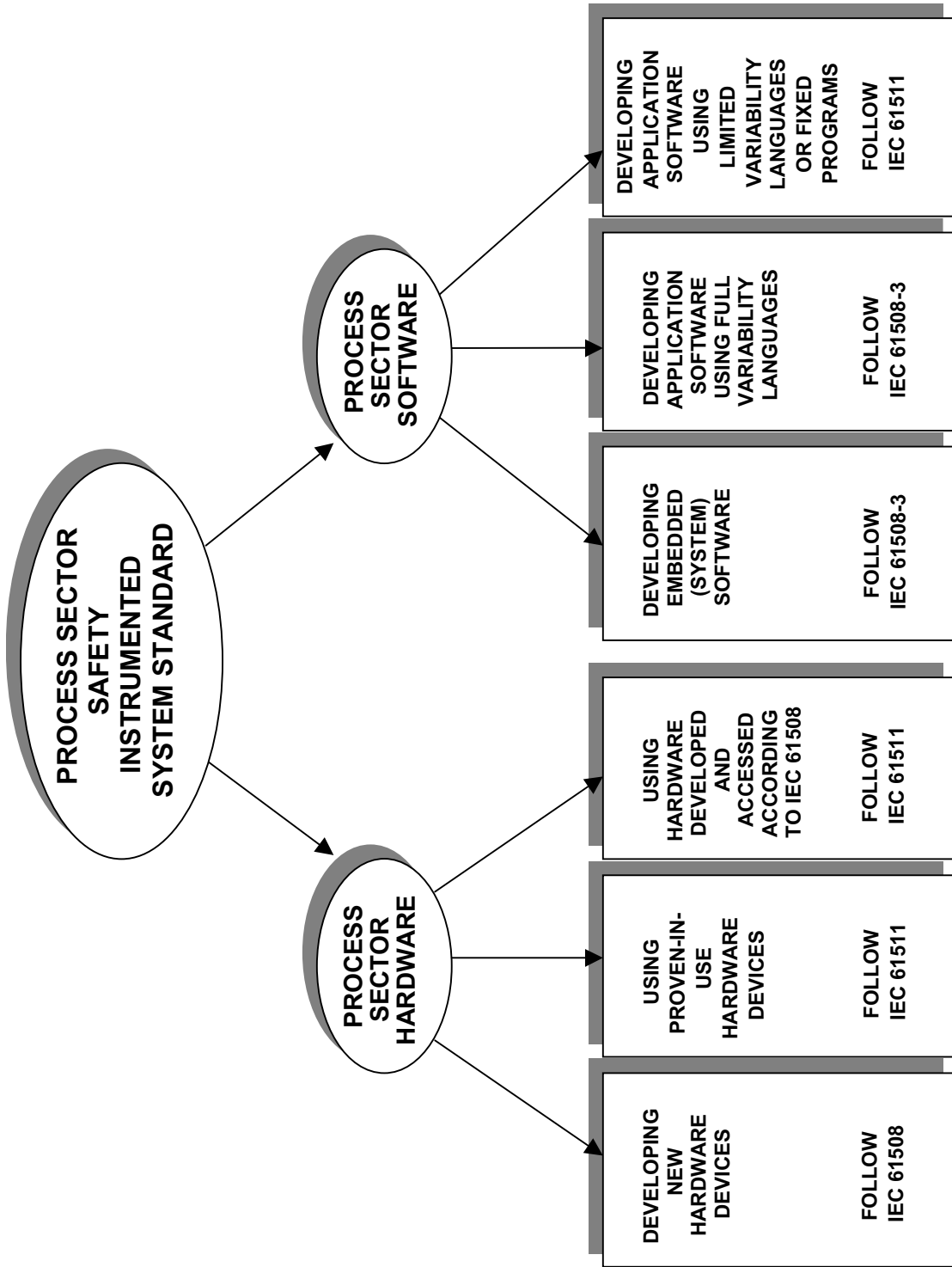
- a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (for example, designers, suppliers, owner/operating company, contractor); this responsibility will be assigned to different parties according to safety planning and national regulations;
- b) applies when equipment that meets the requirements of IEC 61508, or of 11.5 of IEC 61511-1, is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC 61508-2 and IEC 61508-3);
- c) defines the relationship between IEC 61511 and IEC 61508 (Figures 2 and 3);
- d) applies when application software is developed for systems having limited variability or fixed programmes but does not apply to manufacturers, safety instrumented systems designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3);
- e) applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation;
NOTE Within the process sector some applications, (for example, off-shore), may have additional requirements that have to be satisfied.
- f) outlines the relationship between safety instrumented functions and other functions (Figure 4);
- g) results in the identification of the functional requirements and safety integrity requirements for the safety instrumented function(s) taking into account the risk reduction achieved by other means;
- h) specifies requirements for system architecture and hardware configuration, application software, and system integration;
- i) specifies requirements for application software for users and integrators of safety instrumented systems (clause 12). In particular, requirements for the following are specified:

- safety life-cycle phases and activities that are to be applied during the design and development of the application software (the software safety life-cycle model). These requirements include the application of measures and techniques, which are intended to avoid faults in the software and to control failures which may occur;
 - information relating to the software safety validation to be passed to the organization carrying out the SIS integration;
 - preparation of information and procedures concerning software needed by the user for the operation and maintenance of the SIS;
 - procedures and specifications to be met by the organization carrying out modifications to safety software;
- j) applies when functional safety is achieved using one or more safety instrumented functions for the protection of personnel, protection of the general public or protection of the environment;
- k) may be applied in non-safety applications such as asset protection;
- l) defines requirements for implementing safety instrumented functions as a part of the overall arrangements for achieving functional safety;
- m) uses a safety life cycle (Figure 8) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the safety instrumented systems;
- n) requires that a hazard and risk assessment is to be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;
- NOTE See Figure 9 for an overview of risk reduction methods.
- o) establishes numerical targets for average probability of failure on demand and frequency of dangerous failures per hour for the safety integrity levels;
- p) specifies minimum requirements for hardware fault tolerance;
- q) specifies techniques/measures required for achieving the specified integrity levels;
- r) defines a maximum level of performance (SIL 4) which can be achieved for a safety instrumented function implemented according to this standard;
- s) defines a minimum level of performance (SIL 1) below which this standard does not apply;
- t) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications (which should be established based on knowledge of the particular application);
- u) specifies requirements for all parts of the safety instrumented system from sensor to final element(s);
- v) defines the information that is needed during the safety life cycle;
- w) requires that the design of a safety instrumented function takes into account human factors;
- x) does not place any direct requirements on the individual operator or maintenance person.



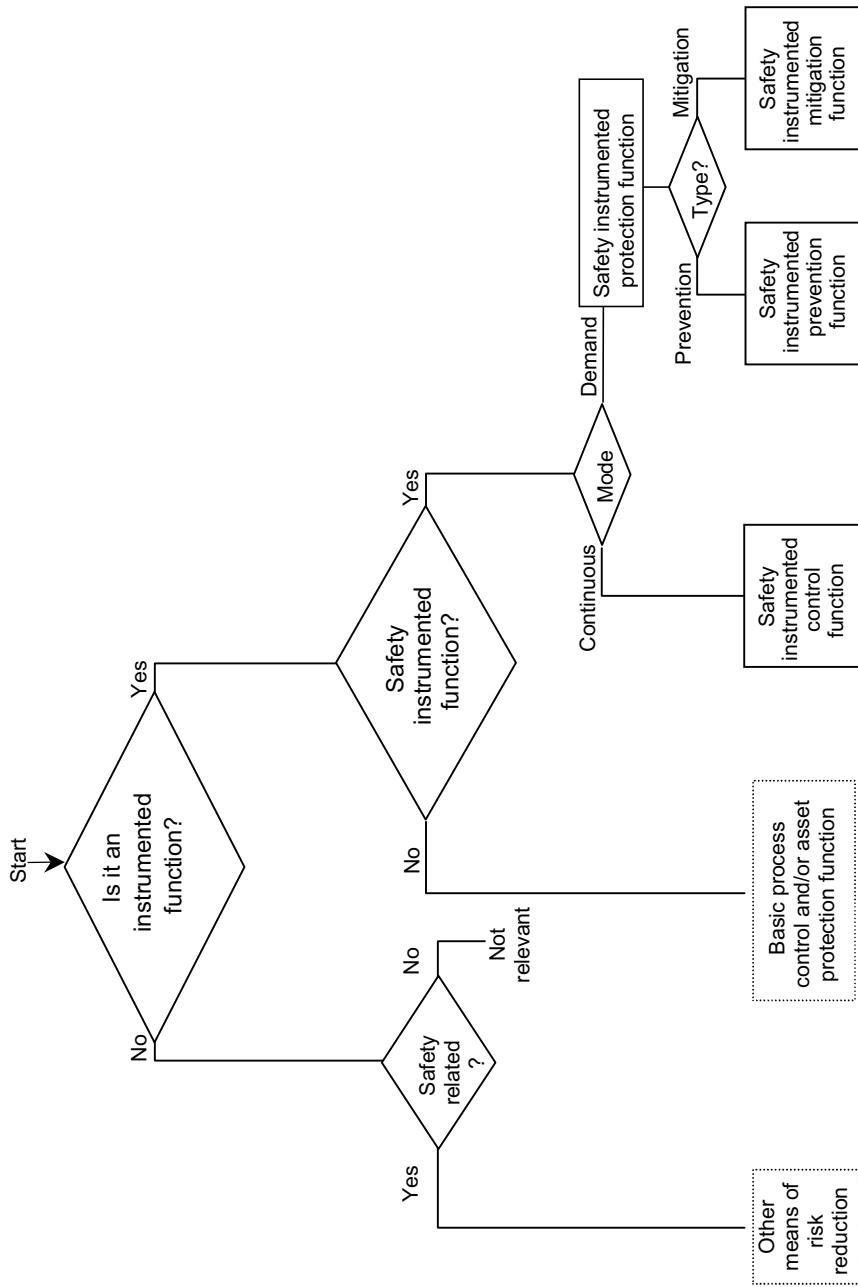
IEC 3241/02

Figure 2 – Relationship between IEC 61511 and IEC 61508



IEC 3242/02

Figure 3 – Relationship between IEC 61511 and IEC 61508 (see clause 1)

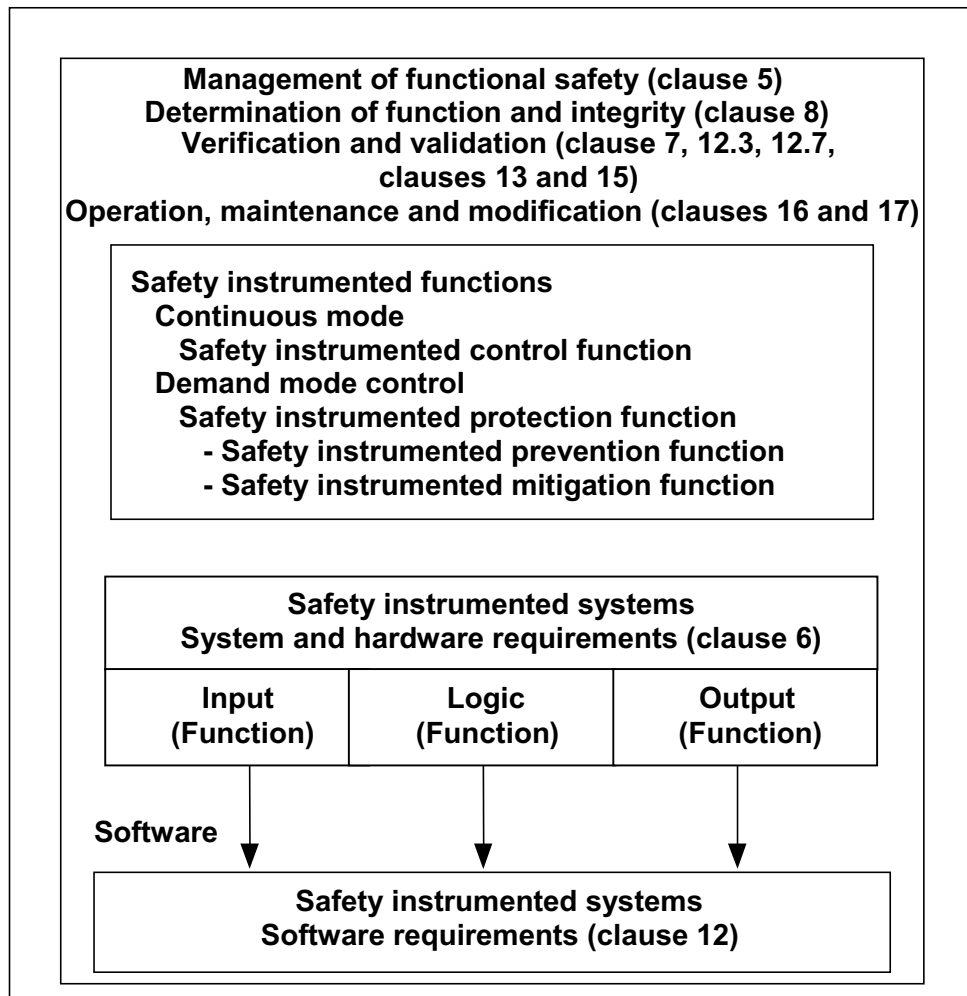


Standard specifies activities which are to be carried out but requirements are not detailed.



IEC 3243/02

Figure 4 – Relationship between safety instrumented functions and other functions



IEC 3244/02

Figure 5 – Relationship between system, hardware, and software of IEC 61511-1

2 Normative references

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

IEC 60654-1:1993, *Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions*

IEC 60654-3:1998, *Industrial-process measurement and control equipment – Operating conditions – Part 3: Mechanical influences*

IEC 61326-1: *Electrical equipment for measurement, control and laboratory use – EMC requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

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

SOMMAIRE

AVANT-PROPOS.....	93
INTRODUCTION.....	95
1 Domaine d'application	98
2 Références normatives.....	104
3 Abréviations et définitions	104
3.1 Abréviations	104
3.2 Définitions	105
4 Conformité à cette Norme internationale.....	121
5 Gestion de la sécurité fonctionnelle	121
5.1 Objectif	121
5.2 Exigences	121
6 Exigences relatives au cycle de vie de sécurité	126
6.1 Objectifs.....	126
6.2 Exigences	126
7 Vérification	129
7.1 Objectifs.....	129
8 Analyse de danger et de risque relatifs au processus	129
8.1 Objectifs.....	129
8.2 Exigences	130
9 Allocation des fonctions de sécurité aux couches de protection	131
9.1 Objectifs.....	131
9.2 Exigences relatives au processus d'allocation	131
9.3 Exigences supplémentaires pour le niveau 4 d'intégrité de sécurité.....	132
9.4 Exigences relatives au système de commande de processus de base en tant que couche de protection	133
9.5 Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes.....	134
10 Spécification des exigences concernant la sécurité d'un SIS	134
10.1 Objectif	134
10.2 Exigences générales	134
10.3 Exigences concernant la sécurité du SIS.....	134
11 Conception et ingénierie du SIS	136
11.1 Objectif	136
11.2 Exigences générales	136
11.3 Exigences relatives au comportement du système lors de la détection d'une anomalie	137
11.4 Exigences relatives à la tolérance aux anomalies du matériel.....	139
11.5 Exigences relatives au choix des composants et des sous-systèmes.....	140
11.6 Dispositifs de terrain	144
11.7 Interfaces	144
11.8 Exigences relatives à la maintenance ou à la conception des tests	146
11.9 Probabilité de défaillance de la SIF	147

12	Exigences relatives au logiciel d'application, incluant les critères de sélection pour le logiciel utilitaire.....	148
12.1	Exigences relatives au cycle de vie de sécurité du logiciel d'application	148
12.2	Spécification des exigences de sécurité du logiciel d'application	154
12.3	Planification de la validation de la sécurité du logiciel d'application	156
12.4	Conception et développement du logiciel d'application	156
12.5	Intégration du logiciel d'application avec le sous-système du SIS	162
12.6	Procédures de modification du logiciel utilisant le FPL et le LVL.....	163
12.7	Vérification du logiciel d'application	163
13	Essais de recette en usine (FAT).....	164
13.1	Objectifs.....	164
13.2	Recommandations.....	164
14	Installation et mise en service du SIS	166
14.1	Objectifs.....	166
14.2	Exigences	166
15	Validation de sécurité du SIS.....	167
15.1	Objectif	167
15.2	Exigences	167
16	Exploitation et maintenance du SIS	170
16.1	Objectifs.....	170
16.2	Exigences	170
16.3	Tests périodiques et inspection	170
17	Modification du SIS	173
17.1	Objectifs.....	173
17.2	Exigences	173
18	Déclassement du SIS	174
18.1	Objectifs.....	174
18.2	Exigences	174
19	Exigences relatives aux informations et à la documentation	174
19.1	Objectifs.....	174
19.2	Exigences	175
	Annexe A (informative) Différences.....	176
	Bibliographie.....	177
	Figure 1 – Structure générale de la présente norme.....	97
	Figure 2 – Relations entre la CEI 61511 et la CEI 61508	100
	Figure 3 – Relations entre la CEI 61511 et la CEI 61508 (voir Article 1).....	101
	Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions ...	102
	Figure 5 – Relations entre le système, le matériel, et le logiciel dans la CEI 61511-1	103
	Figure 6 – Système électronique programmable (PES): structure et terminologie.....	113
	Figure 7 – Exemple d'architecture SIS	116
	Figure 8 – Phases de cycle de vie de sécurité d'un SIS et étapes d'évaluation de la sécurité fonctionnelle	124
	Figure 9 – Méthodes habituelles de réduction de risque rencontrées dans les industries de processus	133

Figure 10 – Cycle de vie de sécurité du logiciel d'application et ses relations avec le cycle de vie de sécurité du SIS	149
Figure 11 – Cycle de vie de sécurité du logiciel d'application (en phase de réalisation)	151
Figure 12 – Cycle de vie de développement du logiciel (modèle en V)	151
Figure 13 – Relations entre les architectures du matériel et du logiciel du SIS.....	154
Tableau 1 – Abréviations utilisées dans la CEI 61511	104
Tableau 2 – Vue d'ensemble du cycle de vie de sécurité d'un SIS	127
Tableau 3 – Niveaux d'intégrité de sécurité: probabilité de défaillance lors d'une sollicitation	131
Tableau 4 – Niveaux d'intégrité de sécurité: probabilité des défaillances dangereuses de la SIF.....	132
Tableau 5 – Tolérance minimale aux anomalies du matériel pour les unités logiques de l'électronique programmable (PE)	139
Tableau 6 – Tolérance minimale aux anomalies du matériel pour les capteurs, les éléments terminaux et les unités logiques non-PE.....	140
Tableau 7 – Cycle de vie de sécurité du logiciel d'application: vue d'ensemble	152

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI»). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
- 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme Internationale CEI 61511-1 a été préparée par le Sous-comité 65A: Aspects systèmes, du Comité d'Études 65 de la CEI: Mesure et commande dans les processus industriels.

La présente version bilingue, publiée en 2003-12, correspond à la version anglaise.

Le texte anglais de cette norme est issu des documents 65A/368/FDIS et 65A/372/RVD. Le rapport de vote 65A/372/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

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

La CEI 61511 comprend les parties suivantes, sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus* (voir la Figure 1).

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

Partie 2: Lignes directrices pour l'application de la CEI 61511-1

Partie 3: Guide pour la détermination des niveaux d'intégrité de sécurité requis

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2007. A cette date, la publication sera

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

Le contenu du corrigendum de novembre 2004 a été pris en considération dans cet exemplaire.

INTRODUCTION

Les systèmes instrumentés de sécurité sont utilisés depuis des années pour exécuter des fonctions instrumentées liées à la sécurité dans les processus industriels. Si l'instrumentation doit être effectivement utilisée pour les fonctions instrumentées liées à la sécurité, il est important que cette instrumentation satisfasse à certaines normes et à certains niveaux minima de performances.

Cette Norme concerne l'application des systèmes instrumentés de sécurité aux industries de production par processus. Elle exige également de conduire une évaluation de danger et de risque des processus pour permettre d'en déduire des spécifications pour les systèmes instrumentés de sécurité. D'autres systèmes de sécurité ne sont considérés que de manière à ce que leur contribution puisse être prise en compte lors de l'examen des exigences de performances concernant les systèmes instrumentés de sécurité. Le système instrumenté de sécurité inclut tous les composants et les sous-ensembles nécessaires pour remplir la fonction instrumentée de sécurité, du (des) capteur(s) à (aux) l'élément(s) terminal(aux).

Cette norme repose sur deux concepts qui sont fondamentaux vis-à-vis de son application: le cycle de vie de sécurité et les niveaux d'intégrité de sécurité.

Cette norme concerne les systèmes instrumentés de sécurité qui sont basés sur l'utilisation d'une technologie électrique/électronique/électronique programmable. Dans le cas où d'autres technologies sont utilisées pour les unités logiques, il convient aussi d'appliquer les principes fondamentaux de cette norme. Cette norme concerne également les capteurs et les éléments terminaux des systèmes instrumentés de sécurité, quelle que soit la technologie utilisée. Cette norme est spécifique de la production industrielle par processus dans le cadre de la CEI 61508 (voir l'Annexe A).

Cette norme présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente.

Dans la plupart des cas, la meilleure sécurité est obtenue par une conception de processus de sécurité inhérents, chaque fois que cela est possible, combinée, au besoin, avec d'autres systèmes de protection, fondés sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) et qui couvrent tous les risques résiduels identifiés. Pour faciliter cette approche, cette norme:

- nécessite de réaliser une évaluation des dangers et des risques pour identifier les exigences globales de sécurité;
- exige d'effectuer une allocation des exigences de sécurité au(x) système(s) instrumenté(s) de sécurité;
- s'inscrit dans un cadre applicable à toutes les méthodes instrumentées qui permettent d'obtenir la sécurité fonctionnelle;
- détaille l'utilisation de certaines activités, telles que la gestion de la sécurité, qui peuvent être applicables à toute méthode permettant d'obtenir la sécurité fonctionnelle.

Cette norme sur les systèmes instrumentés de sécurité pour l'industrie de la production par processus:

- prend en compte toutes les phases du cycle de vie de sécurité, depuis le concept initial, en passant par la conception, la mise en oeuvre, l'exploitation et la maintenance, jusqu'au déclassement;
- permet d'harmoniser avec la présente norme les normes spécifiques de processus industriels existantes ou de nouveaux pays.

Cette norme conduit à un haut niveau de cohérence (par exemple, pour les principes sous-jacents, la terminologie, l'information) au sein des industries de production par processus. Ceci devrait avoir comme conséquence une amélioration en termes de sécurité et d'économie.

Dans les juridictions où des réglementations (par exemple, nationales, fédérales, étatiques, provinciales, du comté, de la ville) sont applicables aux processus de sécurité, à leur conception, à leur gestion, ou à d'autres exigences, ces réglementations sont prioritaires par rapport aux exigences définies dans cette norme.

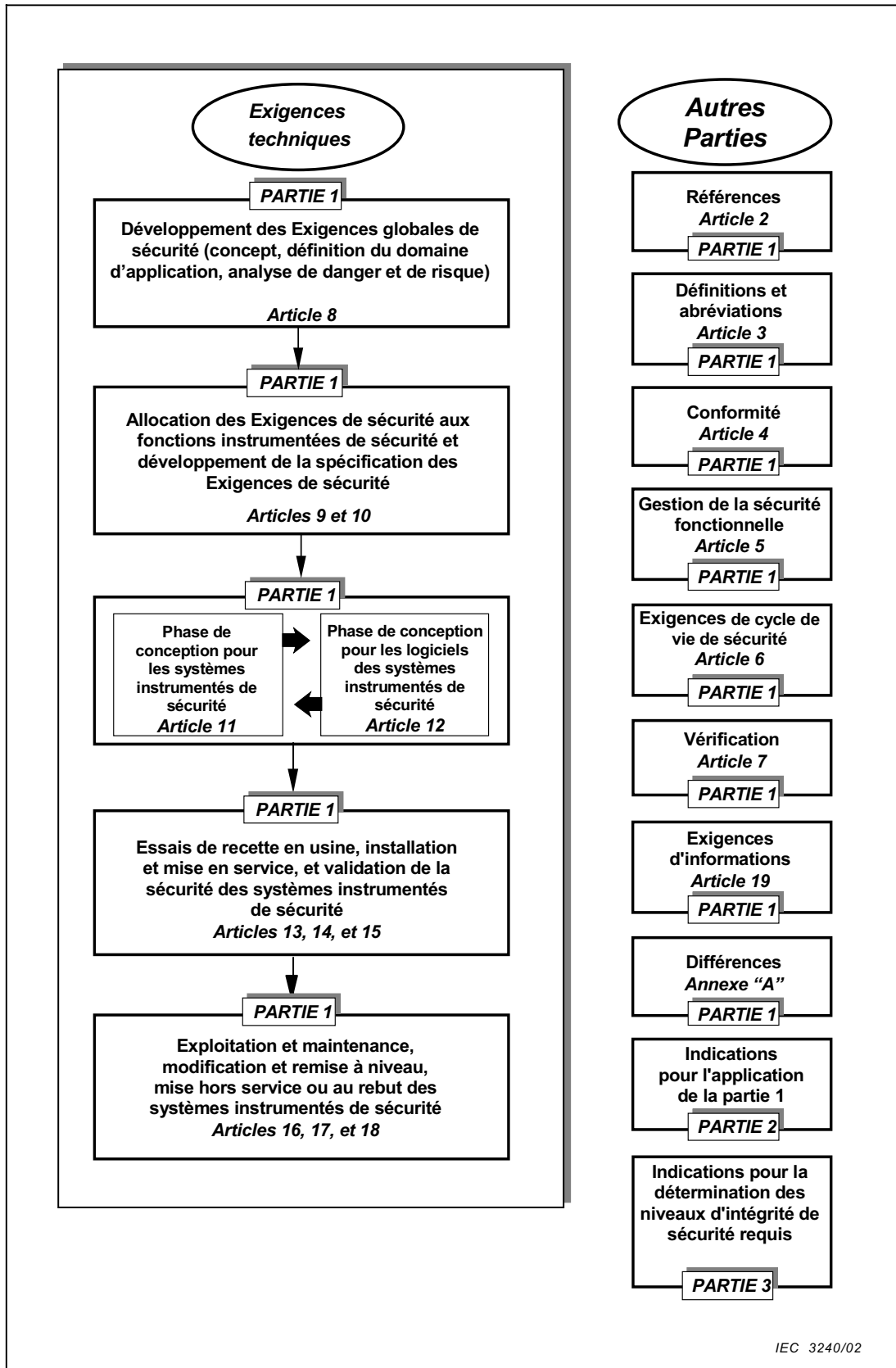


Figure 1 – Structure générale de la présente norme

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

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

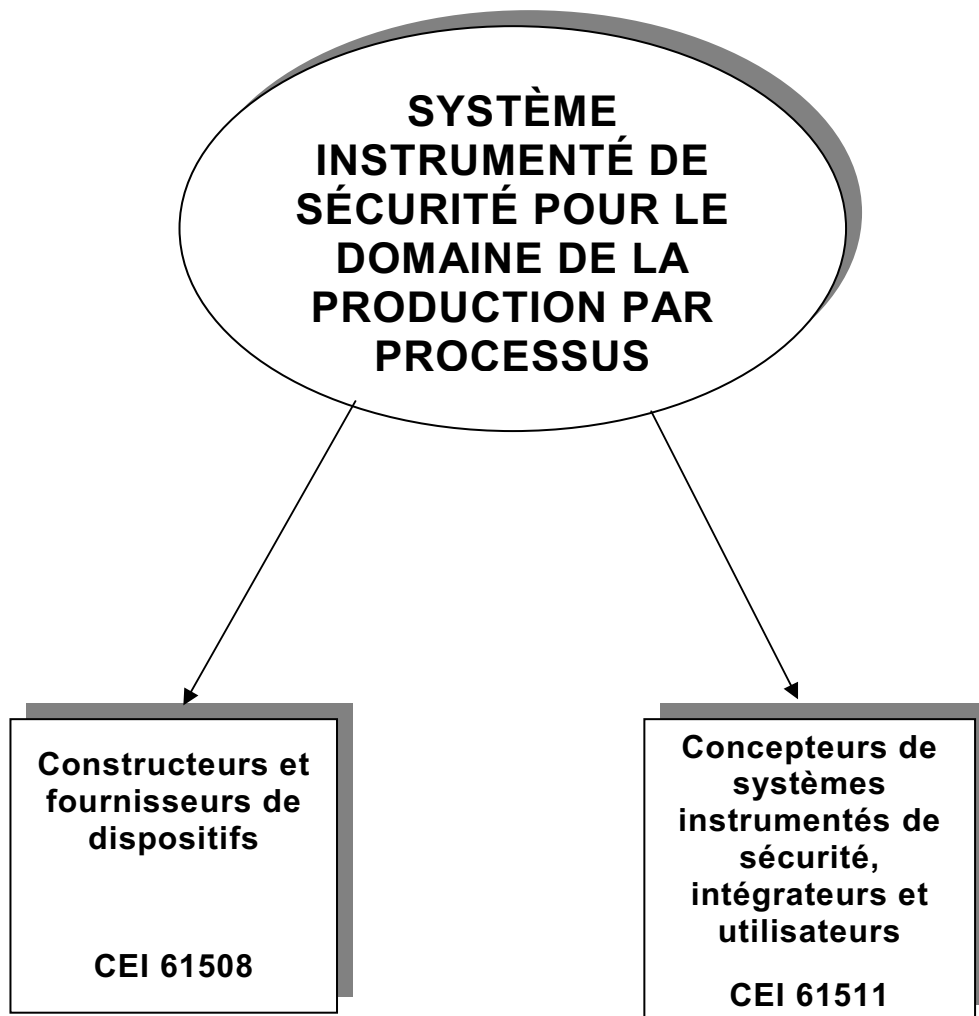
1 Domaine d'application

Cette Norme internationale permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un système instrumenté de sécurité, de telle manière qu'il puisse être mis en oeuvre en toute confiance, et ainsi établir et/ou maintenir les processus dans un état de sécurité convenable. La présente norme a été conçue pour être une mise en oeuvre de la CEI 61508 dans le domaine de l'industrie des processus.

En particulier, cette norme:

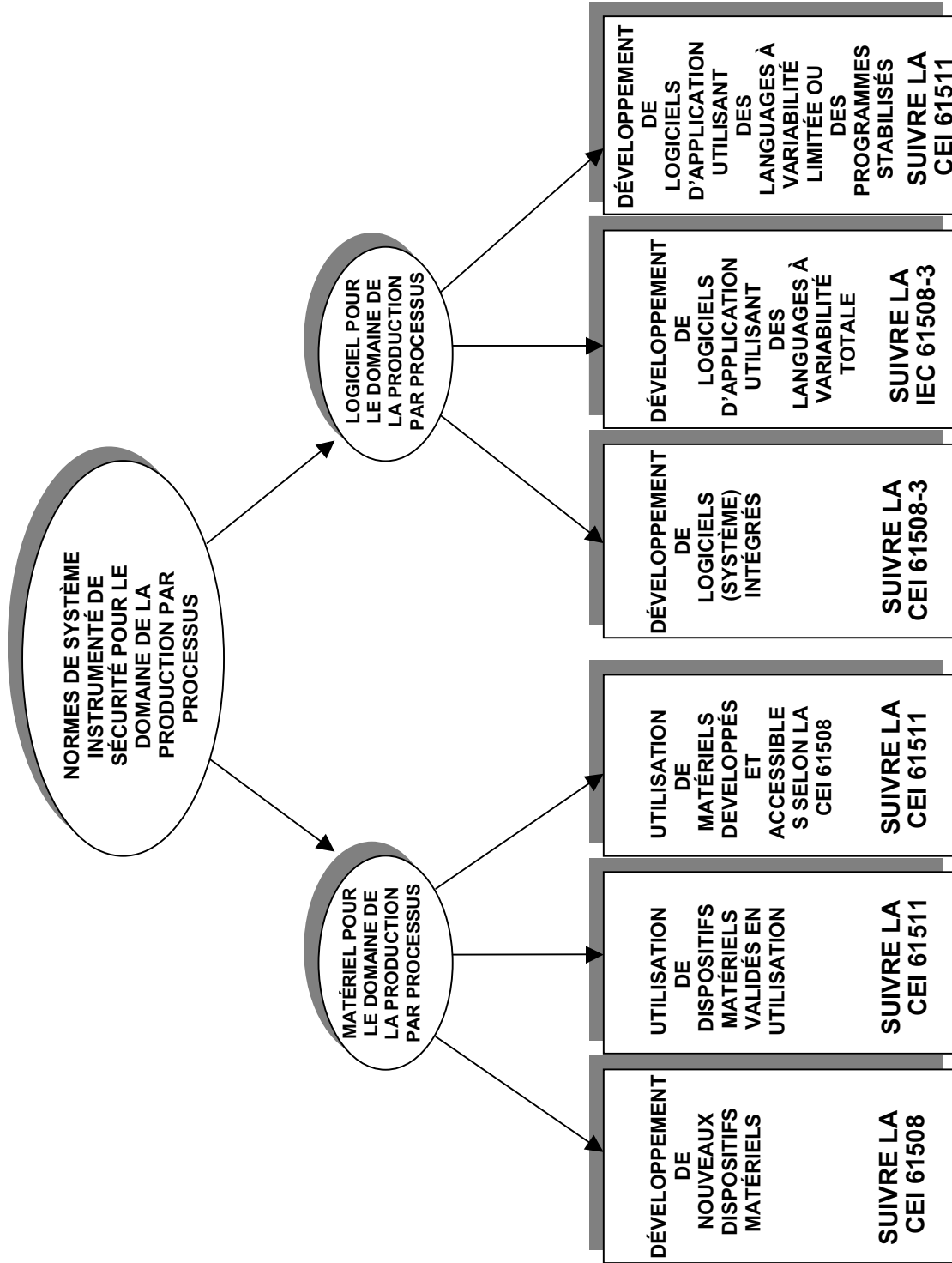
- a) spécifie les exigences permettant d'obtenir la sécurité fonctionnelle, mais ne spécifie pas la responsabilité de la mise en oeuvre des exigences (par exemple, les concepteurs, les fournisseurs, la société propriétaire/exploitante, l'entrepreneur); cette responsabilité sera assignée aux différentes parties selon la planification de la sécurité et des règlements nationaux;
- b) s'applique lorsque les équipements qui satisfont aux exigences de la CEI 61508, ou de 11.5 de la CEI 61511-1, sont intégrés dans un système global, qui doit être utilisé pour une application dans le domaine des processus; ne s'applique pas aux constructeurs qui déclarent leurs dispositifs comme pouvant être utilisés dans les systèmes instrumentés de sécurité dans le domaine des processus (voir la CEI 61508-2 et la CEI 61508-3);
- c) définit les relations entre les normes CEI 61511 et CEI 61508 (Figures 2 et 3);
- d) s'applique lorsque le logiciel d'application est développé pour des systèmes ayant une variabilité limitée ou des programmes figés; ne s'applique pas aux constructeurs, aux concepteurs de systèmes instrumentés de sécurité, aux intégrateurs et aux utilisateurs qui développent un logiciel intégré (logiciel système) ou utilisent des langages de variabilité totale (voir la CEI 61508-3);
- e) s'applique à de nombreuses industries différentes dans le domaine des processus, comprenant celles des produits chimiques, du raffinage de pétrole, de la production de pétrole et de gaz, de la pâte à papier et du papier, de la production d'électricité non nucléaire;
NOTE Dans le domaine des processus, certaines applications (par exemple, en mer) peuvent avoir des exigences supplémentaires, qui doivent être satisfaites.
- f) met en évidence les relations entre les fonctions instrumentées de sécurité et d'autres fonctions (Figure 4);
- g) aboutit à l'identification des exigences fonctionnelles et des exigences concernant l'intégrité de sécurité relatives à la (aux) fonction(s) instrumentée(s) de sécurité, en tenant compte de la réduction de risque obtenue par d'autres moyens;
- h) spécifie les exigences relatives à l'architecture du système et à la configuration du matériel, au logiciel d'application et à l'intégration du système;
- i) spécifie les exigences relatives au logiciel d'application pour les utilisateurs et les intégrateurs des systèmes instrumentés de sécurité (Article 12). En particulier, les exigences pour les points suivants sont spécifiées;

- les phases du cycle de vie de sécurité et les activités qui doivent être mises en oeuvre pendant la conception et le développement du logiciel d'application (modèle de cycle de vie de sécurité du logiciel). Ces exigences incluent l'application de mesures et de techniques, prévues pour éviter des anomalies de logiciel et pour maîtriser les défaillances qui peuvent se produire;
 - les informations concernant la validation de la sécurité du logiciel à effectuer vis-à-vis de l'organisme réalisant l'intégration du SIS;
 - la préparation des informations et des procédures concernant le(s) logiciel(s) dont l'utilisateur a besoin pour l'exploitation et la maintenance du SIS;
 - les procédures et les spécifications à respecter par l'organisme réalisant les modifications du logiciel de sécurité;
- j) s'applique lorsque la sécurité fonctionnelle est obtenue en utilisant une ou plusieurs fonctions instrumentées de sécurité, pour la protection du personnel, la protection du public ou la protection de l'environnement;
- k) peut être appliqué dans des applications non sécuritaires, telle que la protection des biens;
- l) définit des exigences destinées à mettre en oeuvre les fonctions instrumentées de sécurité, faisant partie des dispositions globales pour obtenir la sécurité fonctionnelle;
- m) utilise un cycle de vie de sécurité (Figure 8) et définit une liste d'activités, nécessaires pour déterminer les exigences fonctionnelles et les exigences concernant l'intégrité de sécurité, relatives aux systèmes instrumentés de sécurité;
- n) prescrit qu'une évaluation de danger et de risque doit être effectuée pour définir les exigences fonctionnelles de sécurité et les niveaux d'intégrité de sécurité de chaque fonction instrumentée de sécurité;
- NOTE Voir la Figure 9 pour avoir une vue d'ensemble des méthodes de réduction de risque.
- o) établit des objectifs quantitatifs relatifs à la probabilité moyenne de défaillance lors d'une sollicitation et à la probabilité des défaillances dangereuses par heure pour les niveaux d'intégrité de sécurité;
- p) spécifie des exigences minimales pour la tolérance aux anomalies du matériel;
- q) spécifie les techniques/mesures nécessaires pour obtenir les niveaux d'intégrité spécifiés;
- r) définit un niveau maximal de performances (SIL 4), qui peut être atteint pour une fonction instrumentée de sécurité, mise en oeuvre conformément à cette norme;
- s) définit un niveau minimal de performances (SIL 1) au-dessous duquel cette norme ne s'applique pas;
- t) fournit un cadre pour l'établissement des niveaux d'intégrité de sécurité, mais ne spécifie pas les niveaux d'intégrité de sécurité exigés pour les applications spécifiques (qu'il convient d'établir sur la base de la connaissance de l'application particulière);
- u) spécifie les exigences pour toutes les parties du système instrumenté de sécurité, depuis le capteur jusqu'à l'élément terminal ou aux éléments terminaux;
- v) définit les informations qui sont nécessaires pendant le cycle de vie de sécurité;
- w) prescrit que la conception d'une fonction instrumentée de sécurité tient compte de l'ergonomie;
- x) ne met en place aucune prescription directe relative à un opérateur individuel ou à la personne en charge de la maintenance.



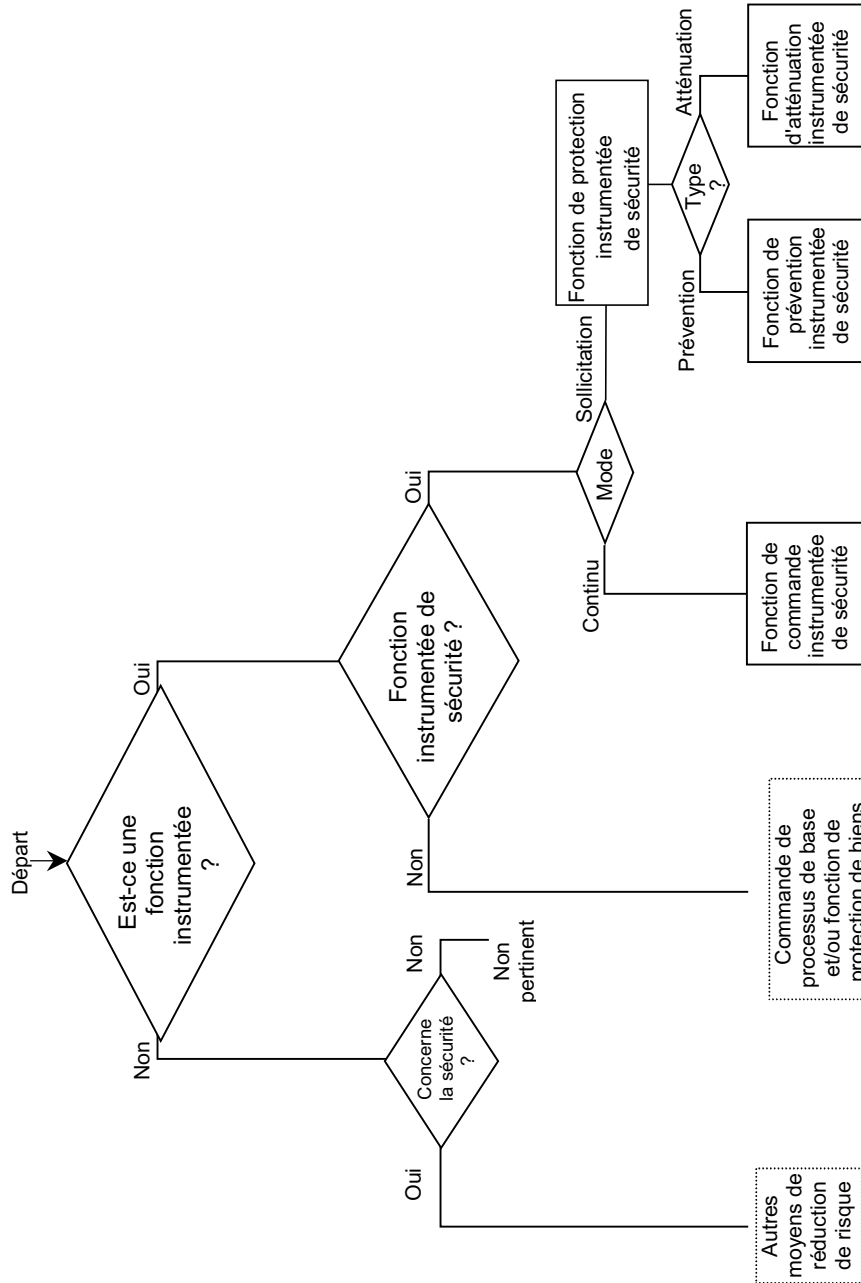
IEC 3241/02

Figure 2 – Relations entre la CEI 61511 et la CEI 61508



IEC 3242/02

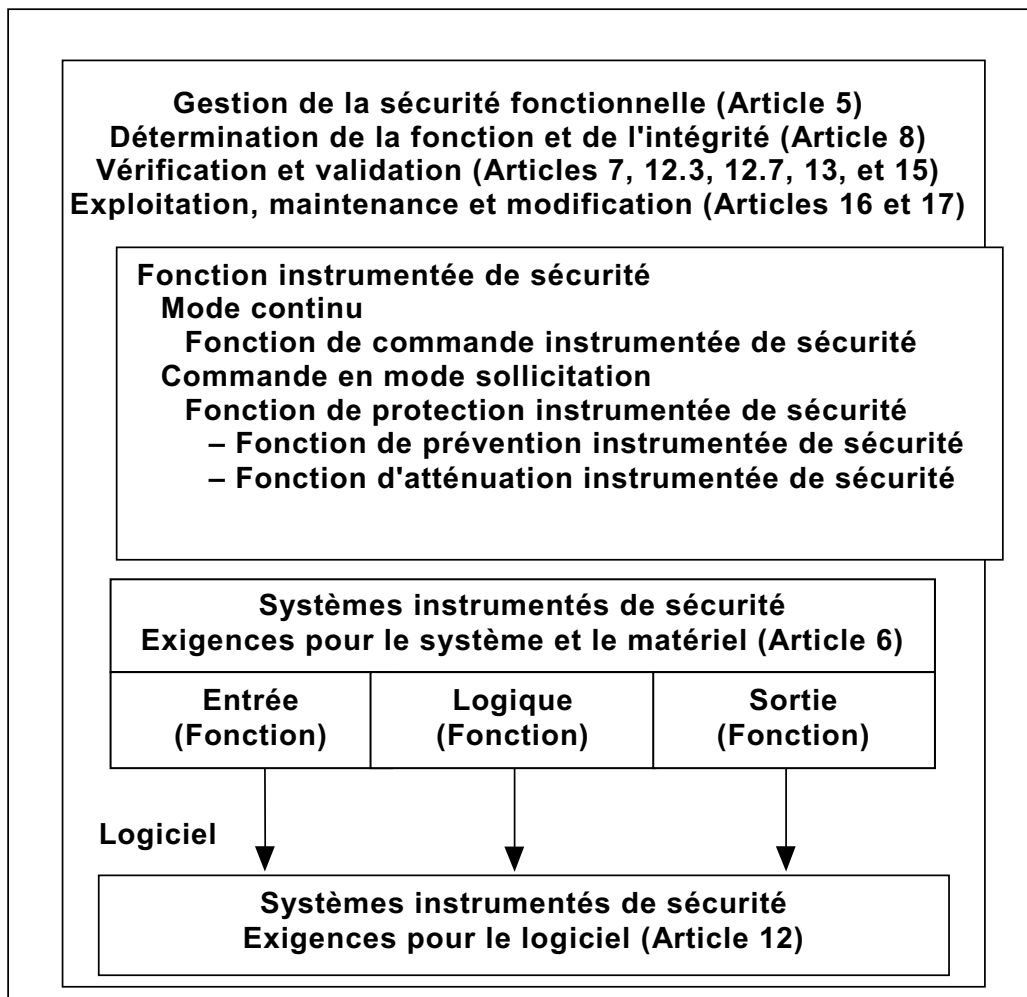
Figure 3 – Relations entre la CEI 61511 et la CEI 61508 (voir Article 1)



La norme spécifie les activités qui sont à conduire, mais les exigences ne sont pas détaillées.

IEC 3243/02

Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions



IEC 3244/02

Figure 5 – Relations entre le système, le matériel, et le logiciel dans la CEI 61511-1

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. 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).

CEI 60654-1:1993, *Matériels de mesure et de commande dans les processus industriels – Conditions de fonctionnement – Partie 1: Conditions climatiques*

CEI 60654-3:1998, *Matériels de mesure et de commande dans les processus industriels – Conditions de fonctionnement – Partie 3: Influences mécaniques*

CEI 61326-1, *Matériels électriques de mesure, de commande et de laboratoire – Prescriptions relatives à la CEM – Partie 1: Prescriptions générales*

CEI 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61511-2, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus – Partie 2: Lignes directrices pour l'application de la CEI 61511-1*