Edition 1.0 2003-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XA
CODE PRIX

ICS 25.040.01

ISBN 2-8318-7683-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

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 61511-3 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

This bilingual version, published in 2004-10, corresponds to the English version.

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

FDIS	Report on voting
65A/367/FDIS	65A/370/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 for 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 the maintenance result 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 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 International 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 (E)/Electronic (E)/Programmable Electronic (PE) 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 of IEC 61511-1).

This standard sets out an approach for safety lifecycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy be 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). Any safety strategy should consider each individual safety instrumented system in the context of the other protective systems. 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 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.

This standard deals with guidance in the area of determining the required SIL in hazards and risk analysis (H & RA). The information herein is intended to provide a broad overview of the wide range of global methods used to implement H & RA. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of safety integrity level(s) (SIL) provided in IEC 61511-1 should be reviewed. The annexes in this standard address the following:

Annex A provides an overview of the concepts of tolerable risk and ALARP.

Annex B provides an overview of a semi-quantitative method used to determine the required SIL.

Annex C provides an overview of a safety matrix method to determine the required SIL.

Annex D provides an overview of a method using a semi-qualitative risk graph approach to determine the required SIL.

Annex E provides an overview of a method using a qualitative risk graph approach to determine the required SIL.

Annex F provides an overview of a method using a layer of protection analysis (LOPA) approach to select the required SIL.

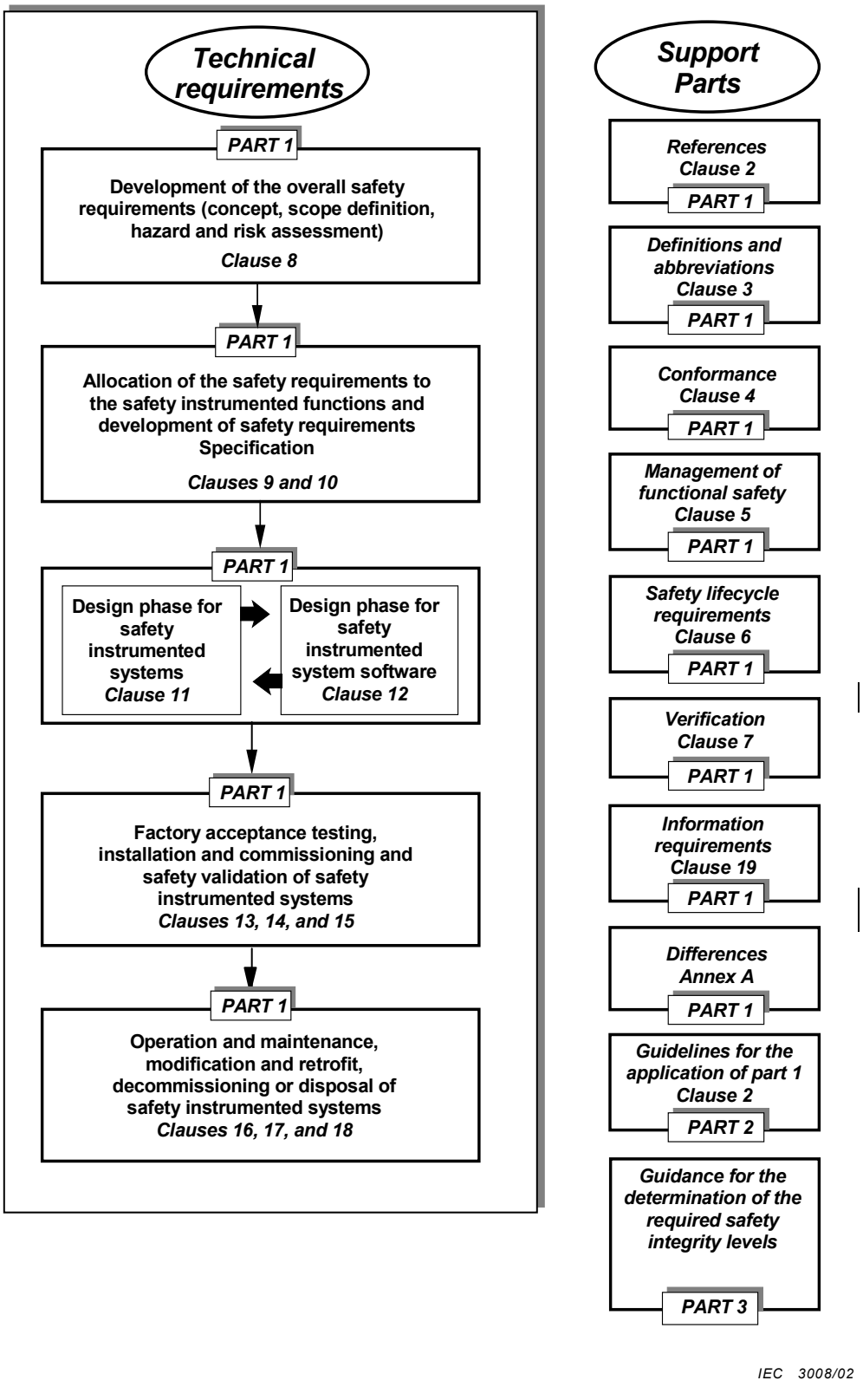


Figure 1 – Overall framework of this standard

FUNCTIONAL SAFETY–

SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

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

1 Scope

This part of IEC 61511 provides information on

– the underlying concepts of risk, the relationship of risk to safety integrity, see Clause 3;

– the determination of tolerable risk, see Annex A;

– a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined, see Annexes B, C, D, E, and F.

In particular, this part

a) applies when functional safety is achieved using one or more safety instrumented functions for the protection of either personnel, the general public, or the environment;

b) may be applied in non-safety applications such as asset protection;

c) illustrates typical hazard and risk assessment methods that may be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;

d) illustrates techniques/measures available for determining the required safety integrity levels;

e) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications;

f) does not give examples of determining the requirements for other methods of risk reduction.

Annexes B, C, D, E, and F illustrate quantitative and qualitative approaches and have been simplified in order to illustrate the underlying principles. These annexes have been included to illustrate the general principles of a number of methods but do not provide a definitive account.

NOTE Those intending to apply the methods indicated in these annexes should consult the source material referenced in each annex.

Figure 1 shows the overall framework for IEC 61511-1, IEC 61511-2 and IEC 61511-3 and indicates the role that this standard plays in the achievement of functional safety for safety instrumented systems.

Figure 2 gives an overview of risk reduction methods.

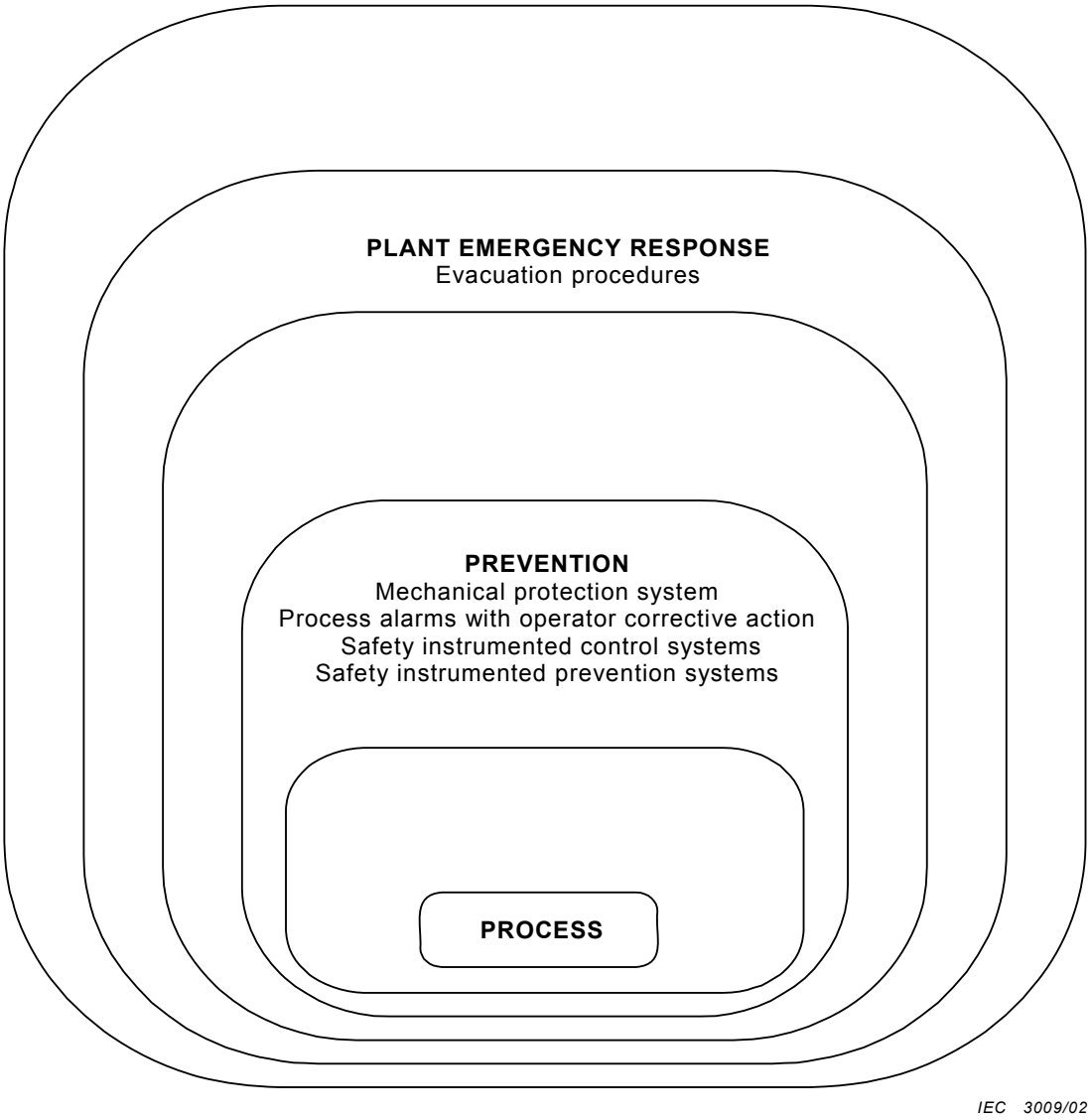


Figure 2 – Typical risk reduction methods found in process plants (for example, protection layer model)

2 Terms, definitions and abbreviations

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

3 Risk and safety integrity – general guidance

3.1 General

This clause provides information on the underlying concepts of risk and the relationship of risk to safety integrity. This information is common to each of the diverse hazard and risk analysis (H & RA) methods shown herein.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité

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 61511-3 a été préparée par le sous-comité 65A: Aspects systèmes, du comité technique 65 de la CEI: Mesure et commande dans les procédés industriels.

Cette version bilingue, publiée en 2004-10, correspond à la version anglaise.

Le texte anglais de cette norme est issu des documents 65A/367/FDIS et 65A/370/RVD.

Le rapport de vote 65A/370/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.

La présente publication a été rédigée conformément aux Directives ISO/CEI, Partie 2.

La CEI 61511 comprend les parties suivantes, présentées sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation* (voir 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: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI 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 sont utilisés dans les industries de transformation depuis de nombreuses années pour remplir des fonctions instrumentées de sécurité. Si l'instrumentation doit réellement être utilisée pour réaliser des fonctions instrumentées de sécurité, il est indispensable qu'elle présente des niveaux minimums de qualité et de performance.

La présente Norme internationale traite de l'utilisation des systèmes instrumentés de sécurité dans les industries de transformation. Elle prescrit également une évaluation du danger et du risque liés aux procédés pour permettre d'en déduire la spécification relative à des systèmes instrumentés de sécurité. D'autres systèmes de sécurité sont considérés uniquement pour que leur contribution puisse être prise en compte lors de l'étude des exigences relatives aux qualités de fonctionnement des systèmes instrumentés de sécurité. Le système instrumenté de sécurité inclut tous les composants et tous les sous-systèmes nécessaires à la réalisation des fonctions instrumentées de sécurité, depuis les capteurs jusqu'aux éléments terminaux.

La présente norme offre deux concepts fondamentaux: le cycle de vie en sécurité et les niveaux d'intégrité de sécurité.

La présente norme traite de systèmes instrumentés de sécurité fondés sur les technologies électrique/électronique/électronique programmable. Il convient d'appliquer les principes de base de la présente norme lorsque d'autres technologies sont utilisées pour l'unité de traitement. La présente norme traite également des capteurs et des éléments terminaux des systèmes instrumentés de sécurité, quelle que soit la technologie utilisée. La présente norme est propre aux industries de transformation, dans le cadre de la CEI 61508 (se reporter à l'Annexe A de la CEI 61511-1).

La présente norme propose des principes pour mener les actions de sécurité tout au long du cycle de vie, afin de mettre en oeuvre une politique technique cohérente et rationnelle et d'obtenir les niveaux de qualité requis.

Dans la plupart des cas et lorsque cela est possible, le meilleur moyen d'assurer la sécurité est de concevoir un procédé intrinsèquement sûr, combiné si nécessaire à un certain nombre de systèmes de technologies différentes (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) assurant la protection contre tout risque résiduel identifié. Il convient que les stratégies de sécurité considèrent chaque système instrumenté de sécurité dans le contexte des autres systèmes de protection. Pour faciliter cette approche, la présente norme:

– requiert une évaluation du danger et du risque pour identifier l'ensemble des exigences de sécurité;
– requiert l'allocation des exigences de sécurité au(x) système(s) instrumenté(s) de sécurité;
– se place dans un cadre applicable à toutes les méthodes instrumentées d'obtention de la sécurité fonctionnelle;
– détaille certaines activités, telles que la gestion de la sécurité, qui peuvent s'appliquer à toutes les méthodes d'obtention de la sécurité fonctionnelle.

La présente norme relative aux systèmes instrumentés de sécurité pour le secteur des industries de transformation:

– prend en compte toutes les phases du cycle de vie en sécurité, de la préparation du projet à la conception, la réalisation, l'exploitation, la maintenance et la mise hors service;
– permet l'harmonisation des normes existantes ou nouvelles concernant les industries de transformation et spécifiques à différents pays avec la présente norme.

La présente norme vise à obtenir un haut niveau de cohérence (par exemple, des principes sous-jacents, de la terminologie, de la documentation) dans les industries de transformation. Ceci devrait présenter des avantages tant du point de vue de la sécurité que du point de vue économique.

Lorsque des autorités compétentes (nationales, fédérales, provinciales, cantonales, municipales) ont défini des exigences relatives à la conception de la sécurité des procédés, à la gestion de la sécurité des procédés, ou d'autres exigences, celles-ci priment sur les exigences définies dans la présente norme.

La présente norme donne des conseils pour déterminer le niveau d'intégrité de sécurité (SIL) dans le cadre de l'analyse du danger et du risque (H & RA). Les informations contenues dans le présent document ont pour but de donner un aperçu général de la grande variété de méthodes globales utilisées pour effectuer une analyse du danger et du risque (H & RA). Les informations fournies ne sont pas suffisamment détaillées pour permettre l'utilisation de l'une quelconque de ces méthodes.

Avant d'aller plus loin, il convient de considérer le concept ainsi que la détermination du ou des niveaux d'intégrité de sécurité (SIL) décrits dans la CEI 61511-1. Les annexes de la présente norme traitent des sujets suivants:

Annexe A cette annexe donne un aperçu général des concepts de risque tolérable et d'ALARP (aussi faible que raisonnablement possible).

Annexe B cette annexe donne un aperçu général d'une méthode semi-quantitative utilisée pour déterminer le niveau d'intégrité de sécurité (SIL) requis.

Annexe C cette annexe donne un aperçu général d'une méthode utilisant une matrice de sécurité pour déterminer le niveau d'intégrité de sécurité (SIL) requis.

Annexe D cette annexe donne un aperçu général d'une méthode utilisant un graphe de risque semi-qualitatif pour déterminer le niveau d'intégrité de sécurité (SIL) requis.

Annexe E cette annexe donne un aperçu général d'une méthode utilisant un graphe de risque qualitatif pour déterminer le niveau d'intégrité de sécurité (SIL) requis.

Annexe F cette annexe donne un aperçu général d'une méthode d'analyse des couches de protection (LOPA) pour sélectionner le niveau SIL requis.

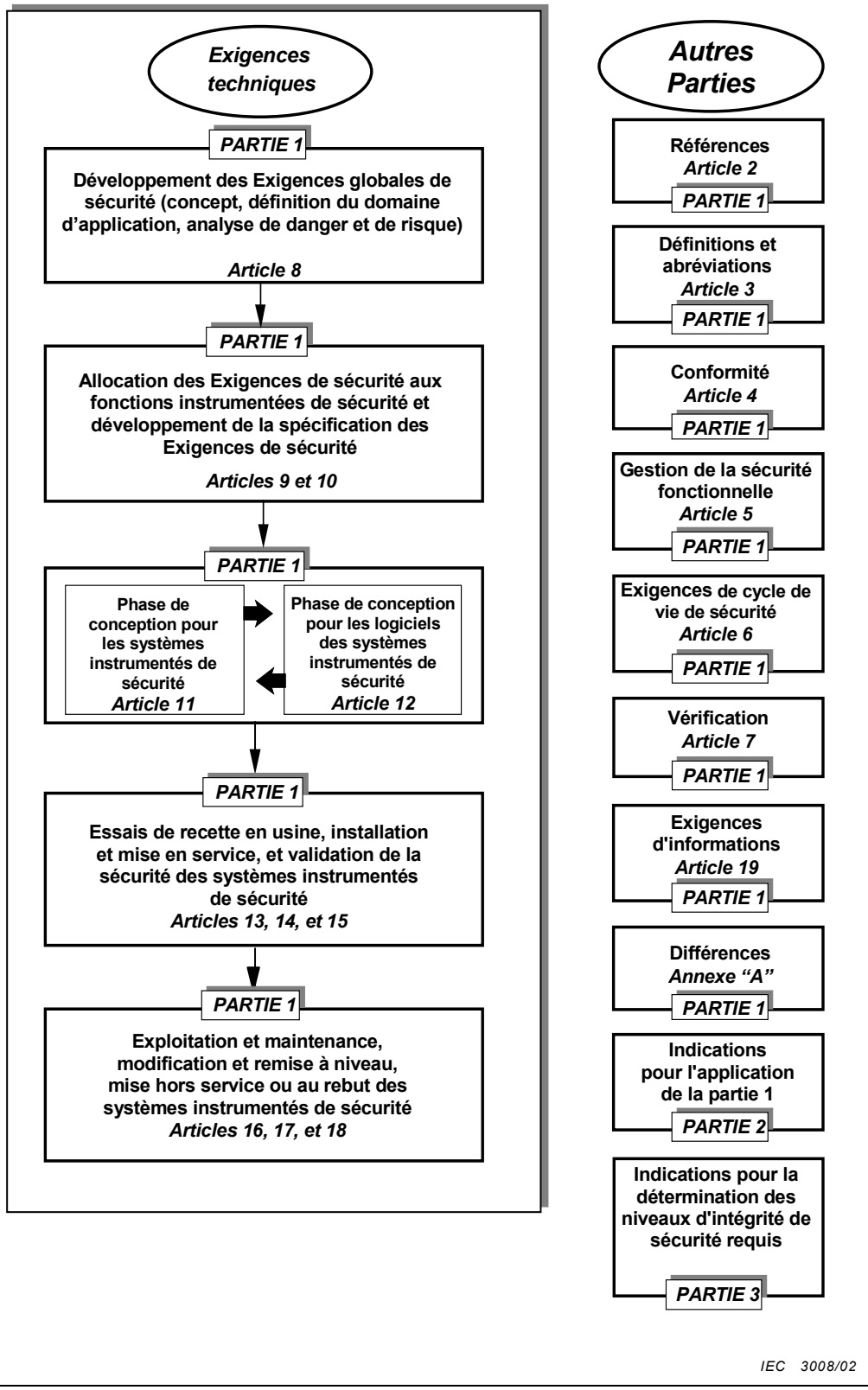


Figure 1 – Structure générale de la présente norme

SÉCURITÉ FONCTIONNELLE –

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

Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité

1 Domaine d'application

La présente partie de la CEI 61511 fournit des informations sur:

– les concepts sous-jacents de risque et la relation entre risque et intégrité, se reporter à l'Article 3;

– la détermination du risque tolérable, se reporter à l'Annexe A;

– différentes méthodes permettant de déterminer les niveaux d'intégrité de sécurité des fonctions instrumentées de sécurité, se reporter aux Annexes B, C, D, E et F.

En particulier, la présente partie:

a) s'applique lorsque la sécurité fonctionnelle est obtenue à l'aide d'une ou plusieurs fonctions instrumentées de sécurité pour la protection du personnel, du public ou de l'environnement;

b) peut être utilisée dans des applications qui ne sont pas liées à la sécurité, comme la protection des biens;

c) décrit des méthodes types d'analyse de danger et de risque, qui peuvent être utilisées pour établir les exigences fonctionnelles de sécurité et les niveaux d'intégrité de sécurité de chaque fonction instrumentée de sécurité;

d) identifie des techniques et mesures disponibles pour déterminer les niveaux d'intégrité de sécurité spécifiés;

e) fournit un cadre pour l'établissement des niveaux d'intégrité de sécurité, mais ne spécifie pas les niveaux d'intégrité de sécurité requis pour des applications spécifiques;

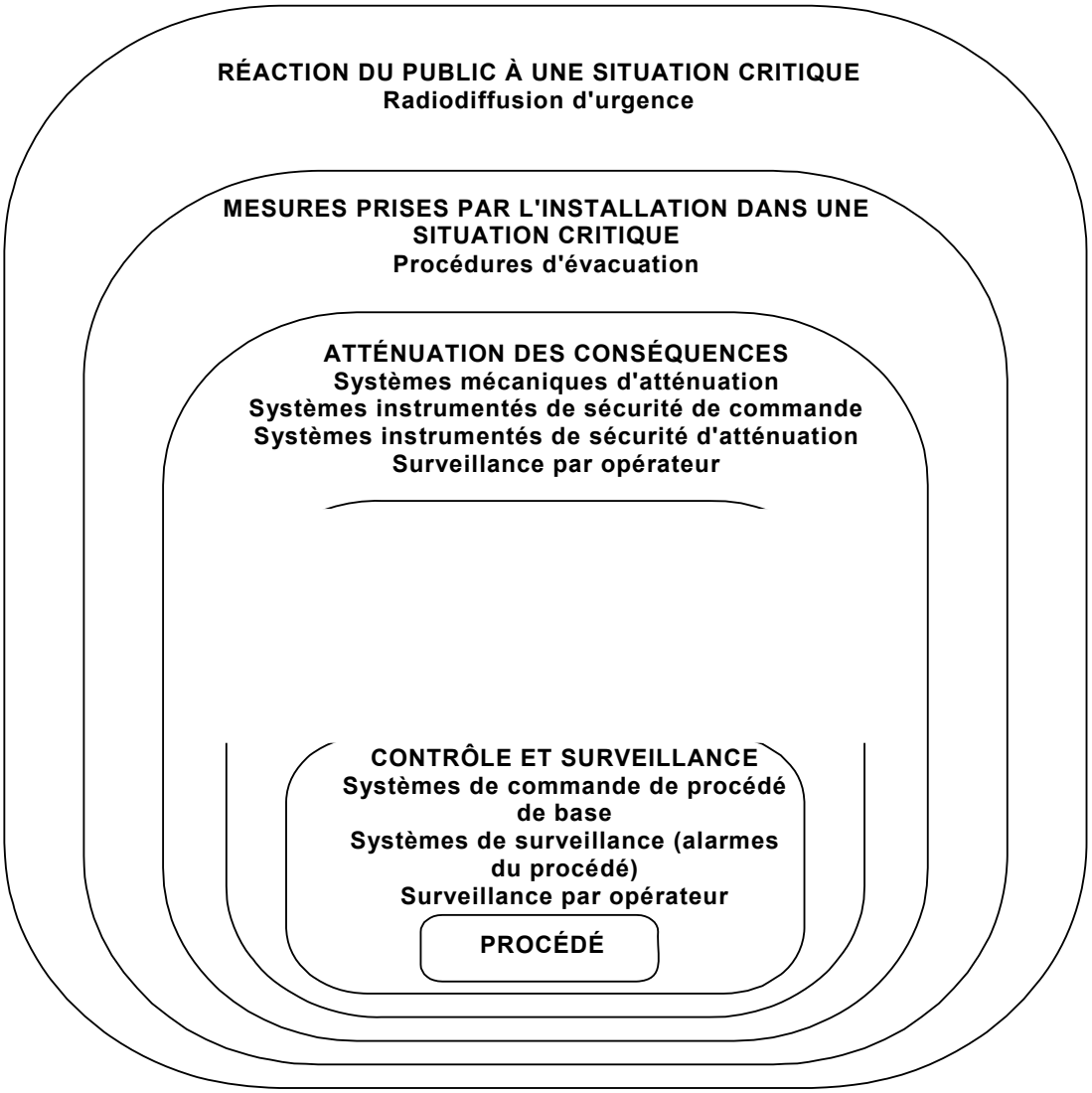
f) ne donne pas d'exemples de détermination des exigences relatives à d'autres méthodes de réduction du risque.

Les Annexes B, C, D, E et F décrivent des méthodes quantitatives et qualitatives sous forme simplifiée, afin d'en illustrer les principes sous-jacents. Ces annexes ont été incorporées pour illustrer les principes généraux d'un certain nombre de méthodes, mais ne constituent pas une description exhaustive.

NOTE Il est souhaitable que ceux qui envisagent d'utiliser les méthodes indiquées dans ces annexes consultent le document source mentionné dans chaque annexe.

La Figure 1 illustre la structure générale des parties 1 à 3 de la présente norme et indique le rôle joué par la partie 3 dans l'obtention de la sécurité fonctionnelle des systèmes instrumentés de sécurité.

La Figure 2 donne un aperçu général des méthodes de réduction du risque.



IEC 3009/02