

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61511-1

Première édition
First edition
2003-01

**Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le
domaine de la production par processus –**

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

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

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



Numéro de référence
Reference number
CEI/IEC 61511-1:2003

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI** (www.iec.ch)
- **Catalogue des publications de la CEI**

Le catalogue en ligne sur le site web de la CEI (www.iec.ch/searchpub) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.

- **IEC Just Published**

Ce résumé des dernières publications parues (www.iec.ch/online_news/justpub) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.

- **Service clients**

Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

Email: custserv@iec.ch
Tél: +41 22 919 02 11
Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site** (www.iec.ch)
- **Catalogue of IEC publications**

The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

This summary of recently issued publications (www.iec.ch/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61511-1

Première édition
First edition
2003-01

**Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le
domaine de la production par processus –**

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

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

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

© IEC 2003 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission, 3, rue de Varembe, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE **XC**

*Pour prix, voir catalogue en vigueur
For price, see current catalogue*

SOMMAIRE

AVANT-PROPOS.....	8
INTRODUCTION.....	12
1 Domaine d'application	18
2 Références normatives.....	30
3 Abréviations et définitions	30
3.1 Abréviations	30
3.2 Définitions	32
4 Conformité à cette Norme internationale.....	64
5 Gestion de la sécurité fonctionnelle	64
5.1 Objectif	64
5.2 Exigences	64
6 Exigences relatives au cycle de vie de sécurité	74
6.1 Objectifs.....	74
6.2 Exigences	74
7 Vérification	80
7.1 Objectifs.....	80
8 Analyse de danger et de risque relatifs au processus	80
8.1 Objectifs.....	80
8.2 Exigences	82
9 Allocation des fonctions de sécurité aux couches de protection	84
9.1 Objectifs.....	84
9.2 Exigences relatives au processus d'allocation	84
9.3 Exigences supplémentaires pour le niveau 4 d'intégrité de sécurité.....	86
9.4 Exigences relatives au système de commande de processus de base en tant que couche de protection	88
9.5 Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes.....	90
10 Spécification des exigences concernant la sécurité d'un SIS	90
10.1 Objectif	90
10.2 Exigences générales	90
10.3 Exigences concernant la sécurité du SIS.....	90
11 Conception et ingénierie du SIS	94
11.1 Objectif	94
11.2 Exigences générales	94
11.3 Exigences relatives au comportement du système lors de la détection d'une anomalie	96
11.4 Exigences relatives à la tolérance aux anomalies du matériel.....	100
11.5 Exigences relatives au choix des composants et des sous-systèmes.....	102
11.6 Dispositifs de terrain	110
11.7 Interfaces	110
11.8 Exigences relatives à la maintenance ou à la conception des tests	114
11.9 Probabilité de défaillance de la SIF	116

CONTENTS

FOREWORD.....	9
INTRODUCTION.....	13
1 Scope.....	19
2 Normative references	31
3 Abbreviations and definitions.....	31
3.1 Abbreviations	31
3.2 Definitions	33
4 Conformance to this International Standard	65
5 Management of functional safety	65
5.1 Objective	65
5.2 Requirements.....	65
6 Safety life-cycle requirements.....	75
6.1 Objective	75
6.2 Requirements	75
7 Verification	81
7.1 Objective	81
8 Process hazard and risk analysis	81
8.1 Objectives	81
8.2 Requirements.....	83
9 Allocation of safety functions to protection layers	85
9.1 Objective	85
9.2 Requirements of the allocation process	85
9.3 Additional requirements for safety integrity level 4.....	87
9.4 Requirements on the basic process control system as a protection layer.....	89
9.5 Requirements for preventing common cause, common mode and dependent failures	91
10 SIS safety requirements specification	91
10.1 Objective	91
10.2 General requirements.....	91
10.3 SIS safety requirements	91
11 SIS design and engineering.....	95
11.1 Objective	95
11.2 General requirements.....	95
11.3 Requirements for system behaviour on detection of a fault.....	97
11.4 Requirements for hardware fault tolerance	101
11.5 Requirements for selection of components and subsystems	103
11.6 Field devices	111
11.7 Interfaces	111
11.8 Maintenance or testing design requirements.....	115
11.9 SIF probability of failure	117

12	Exigences relatives au logiciel d'application, incluant les critères de sélection pour le logiciel utilitaire.....	118
12.1	Exigences relatives au cycle de vie de sécurité du logiciel d'application	118
12.2	Spécification des exigences de sécurité du logiciel d'application	130
12.3	Planification de la validation de la sécurité du logiciel d'application	134
12.4	Conception et développement du logiciel d'application	134
12.5	Intégration du logiciel d'application avec le sous-système du SIS	146
12.6	Procédures de modification du logiciel utilisant le FPL et le LVL.....	148
12.7	Vérification du logiciel d'application	148
13	Essais de recette en usine (FAT).....	150
13.1	Objectifs.....	150
13.2	Recommandations.....	152
14	Installation et mise en service du SIS	154
14.1	Objectifs.....	154
14.2	Exigences	154
15	Validation de sécurité du SIS.....	156
15.1	Objectif	156
15.2	Exigences	156
16	Exploitation et maintenance du SIS	162
16.1	Objectifs.....	162
16.2	Exigences	162
16.3	Tests périodiques et inspection	166
17	Modification du SIS	168
17.1	Objectifs.....	168
17.2	Exigences	168
18	Déclassement du SIS	170
18.1	Objectifs.....	170
18.2	Exigences	170
19	Exigences relatives aux informations et à la documentation	170
19.1	Objectifs.....	170
19.2	Exigences	172
	Annexe A (informative) Différences.....	174
	Bibliographie.....	176
	Figure 1 – Structure générale de la présente norme.....	16
	Figure 2 – Relations entre la CEI 61511 et la CEI 61508	22
	Figure 3 – Relations entre la CEI 61511 et la CEI 61508 (voir Article 1).....	24
	Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions	26
	Figure 5 – Relations entre le système, le matériel, et le logiciel dans la CEI 61511-1	28
	Figure 6 – Système électronique programmable (PES): structure et terminologie.....	48
	Figure 7 – Exemple d'architecture SIS	54
	Figure 8 – Phases de cycle de vie de sécurité d'un SIS et étapes d'évaluation de la sécurité fonctionnelle	70
	Figure 9 – Méthodes habituelles de réduction de risque rencontrées dans les industries de processus	88

12	Requirements for application software, including selection criteria for utility software ...	119
12.1	Application software safety life-cycle requirements	119
12.2	Application software safety requirements specification	131
12.3	Application software safety validation planning	135
12.4	Application software design and development	135
12.5	Integration of the application software with the SIS subsystem	147
12.6	FPL and LVL software modification procedures	149
12.7	Application software verification	149
13	Factory acceptance testing (FAT)	151
13.1	Objectives	151
13.2	Recommendations	153
14	SIS installation and commissioning	155
14.1	Objectives	155
14.2	Requirements	155
15	SIS safety validation	157
15.1	Objective	157
15.2	Requirements	157
16	SIS operation and maintenance	163
16.1	Objectives	163
16.2	Requirements	163
16.3	Proof testing and inspection	167
17	SIS modification	169
17.1	Objective	169
17.2	Requirements	169
18	SIS decommissioning	171
18.1	Objectives	171
18.2	Requirements	171
19	Information and documentation requirements	171
19.1	Objectives	171
19.2	Requirements	173
	Annex A (informative) Differences	175
	Bibliography	177
	Figure 1 – Overall framework of this standard	17
	Figure 2 – Relationship between IEC 61511 and IEC 61508	23
	Figure 3 – Relationship between IEC 61511 and IEC 61508 (see 1.2)	25
	Figure 4 – Relationship between safety instrumented functions and other functions	27
	Figure 5 – Relationship between system, hardware, and software of IEC 61511-1	29
	Figure 6 – Programmable electronic system (PES): structure and terminology	49
	Figure 7 – Example SIS architecture	55
	Figure 8 – SIS safety life-cycle phases and functional safety assessment stages	71
	Figure 9 – Typical risk reduction methods found in process plants	89

Figure 10 – Cycle de vie de sécurité du logiciel d'application et ses relations avec le cycle de vie de sécurité du SIS	120
Figure 11 – Cycle de vie de sécurité du logiciel d'application (en phase de réalisation)	124
Figure 12 – Cycle de vie de développement du logiciel (modèle en V)	124
Figure 13 – Relations entre les architectures du matériel et du logiciel du SIS.....	130
Tableau 1 – Abréviations utilisées dans la CEI 61511	30
Tableau 2 – Vue d'ensemble du cycle de vie de sécurité d'un SIS	76
Tableau 3 – Niveaux d'intégrité de sécurité: probabilité de défaillance lors d'une sollicitation	84
Tableau 4 – Niveaux d'intégrité de sécurité: probabilité des défaillances dangereuses de la SIF	86
Tableau 5 – Tolérance minimale aux anomalies du matériel pour les unités logiques de l'électronique programmable (PE)	100
Tableau 6 – Tolérance minimale aux anomalies du matériel pour les capteurs, les éléments terminaux et les unités logiques non-PE.....	102
Tableau 7 – Cycle de vie de sécurité du logiciel d'application: vue d'ensemble	126

Figure 10 – Application software safety life cycle and its relationship to the SIS safety life cycle	121
Figure 11 – Application software safety life cycle (in realization phase)	125
Figure 12 – Software development life cycle (the V-model)	125
Figure 13 – Relationship between the hardware and software architectures of SIS	131
Table 1 – Abbreviations used in IEC 61511.....	31
Table 2 – SIS safety life-cycle overview	77
Table 3 – Safety integrity levels: probability of failure on demand	85
Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF	87
Table 5 – Minimum hardware fault tolerance of PE logic solvers	101
Table 6 – Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers	103
Table 7 – Application software safety life cycle: overview	127

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SÉCURITÉ FONCTIONNELLE – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ POUR LE DOMAINE DE LA PRODUCTION PAR PROCESSUS –

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.

Cette version bilingue (2003-12) remplace la version monolingue anglaise.

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 (2003-12) replaces the English version.

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.

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.

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.

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.