Edition 2.0 2016-07

REDLINE VERSION

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.01

ISBN 978-2-8322-3545-4

Warning! Make sure that you obtained this publication from an authorized distributor.

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

DISCLAIMER
This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

Additional H&RA example(s) and quantitative analysis consideration annexes are provided.

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

FDIS	Report on voting
65A/779/FDIS	65A786/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.

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

A list of all parts in the IEC 61511 series, published under the general title *Functional safety – Safety instrumented systems for the process industry sector*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

The IEC 61511 series addresses the application of SIS for the process industries. ~~It also requires~~ A process hazard and risk assessment ~~to be~~ is carried out to enable the specification for SIS 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 SIS. The SIS includes all ~~components~~ devices and subsystems necessary to carry out the SIF from sensor(s) to final element(s).

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

The IEC 61511 series addresses SIS 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 the IEC 61511 series should be applied. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of IEC 61508:2010 ~~(see Annex A of IEC 61511-1)~~.

The IEC 61511 series sets out an approach for SIS 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, and programmable electronic). Any safety strategy should consider each individual SIS in the context of the other protective systems. To facilitate this approach, the IEC 61511 series covers:

– ~~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 SIS is carried out;
– works within a framework which is applicable to all instrumented ~~methods~~ means of achieving functional safety;
– details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety;

~~This standard on safety instrumented systems for the process industry:~~

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

The IEC 61511 series is intended to lead to a high level of consistency (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~~ regulations, these take precedence over the requirements defined in ~~this standard~~ the IEC 61511-1.

~~This standard~~ The IEC 61511-3 deals with guidance in the area of determining the required SIL in hazards and risk ~~analysis~~ assessment ~~(H & RA)~~. The information herein is intended to provide a broad overview of the wide range of global methods used to implement ~~H & RA~~ hazards and risk assessment. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of SIL provided in IEC 61511-1:2016 should be reviewed. The informative annexes in ~~this standard~~ the IEC 61511-3 address the following:

Annex A provides ~~an overview of the concepts of tolerable risk and ALARP~~ information that is common to each of the hazard and risk assessment methods shown herein.

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.

Annex G provides a layer of protection analysis using a risk matrix.

Annex H provides an overview of a qualitative approach for risk estimation & SIL assignment.

Annex I provides an overview of the basic steps involved in designing and calibrating a risk graph.

Annex J provides an overview of the impact of multiple safety systems on determining the required SIL

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

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

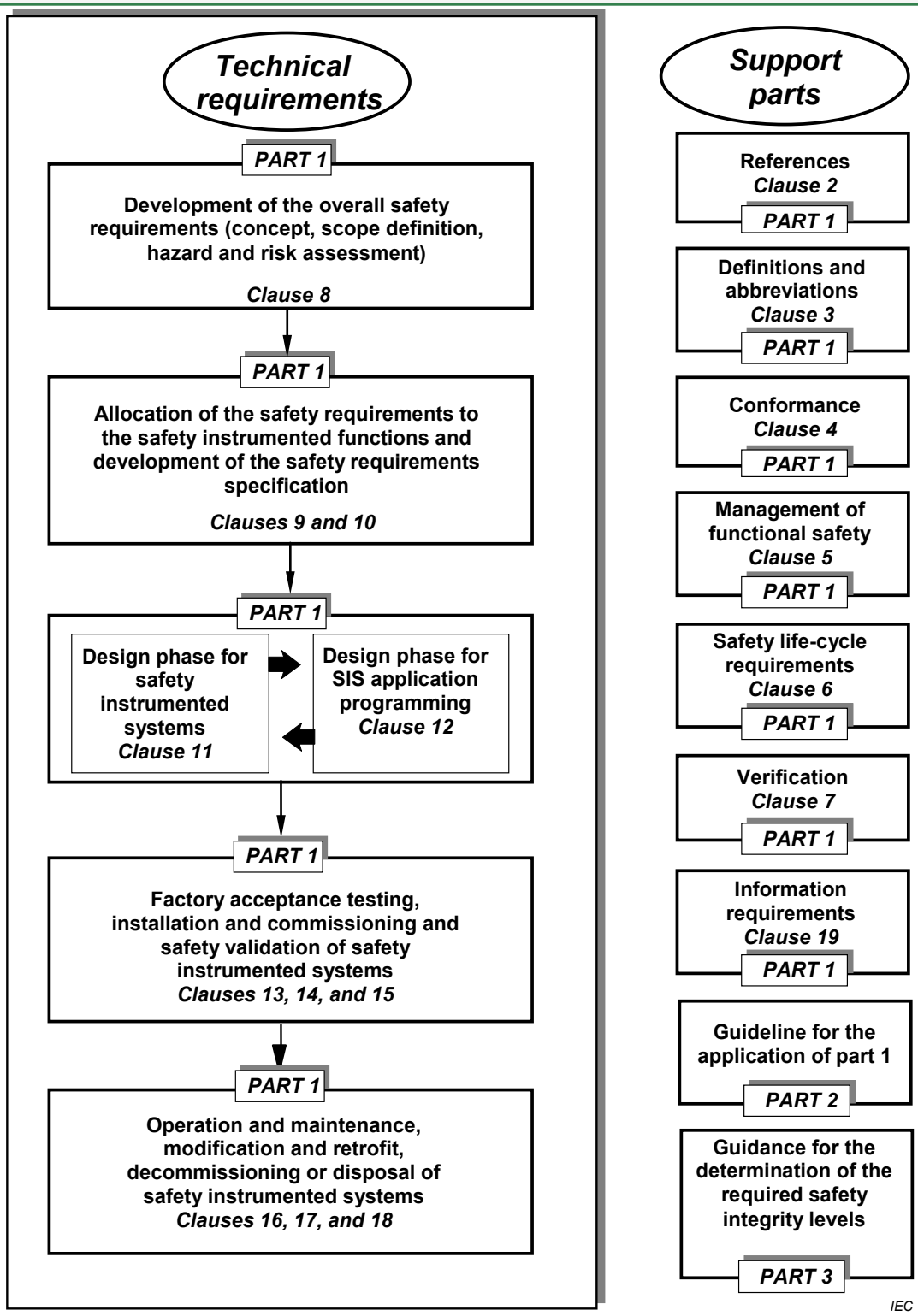


Figure 1 – Overall framework of the IEC 61511 series

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 and the relationship of risk to safety integrity (see Clause A.4);

– the determination of tolerable risk (see Annex K);

– a number of different methods that enable the safety integrity level~~s~~ (SIL) for the safety instrumented functions (SIF) to be determined (see Annexes B through K);

– the impact of multiple safety systems on calculations determining the ability to achieve the desired risk reduction (see Annex J).

In particular, this part of IEC 61511:

a) applies when functional safety is achieved using one or more SIF 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 SIL of each SIF;

d) illustrates techniques/measures available for determining the required SIL;

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

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

NOTE Examples given in the Annexes of this Standard are intended only as case specific examples of implementing IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

Annexes B through K 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 1 Those intending to apply the methods indicated in these annexes ~~should~~ can consult the source material referenced in each annex.

NOTE 2 The methods of SIL determination included in Part 3 may not be suitable for all applications. In particular, specific techniques or additional factors that are not illustrated may be required for high demand or continuous mode of operation.

NOTE 3 The methods as illustrated herein may result in non-conservative results when they are used beyond their underlying limits and when factors such as common cause, fault tolerance, holistic considerations of the application, lack of experience with the method being used, independence of the protection layers, etc., are not properly considered. See Annex J.

Figure 2 gives an overview of typical protection layers and risk reduction ~~methods~~ means.

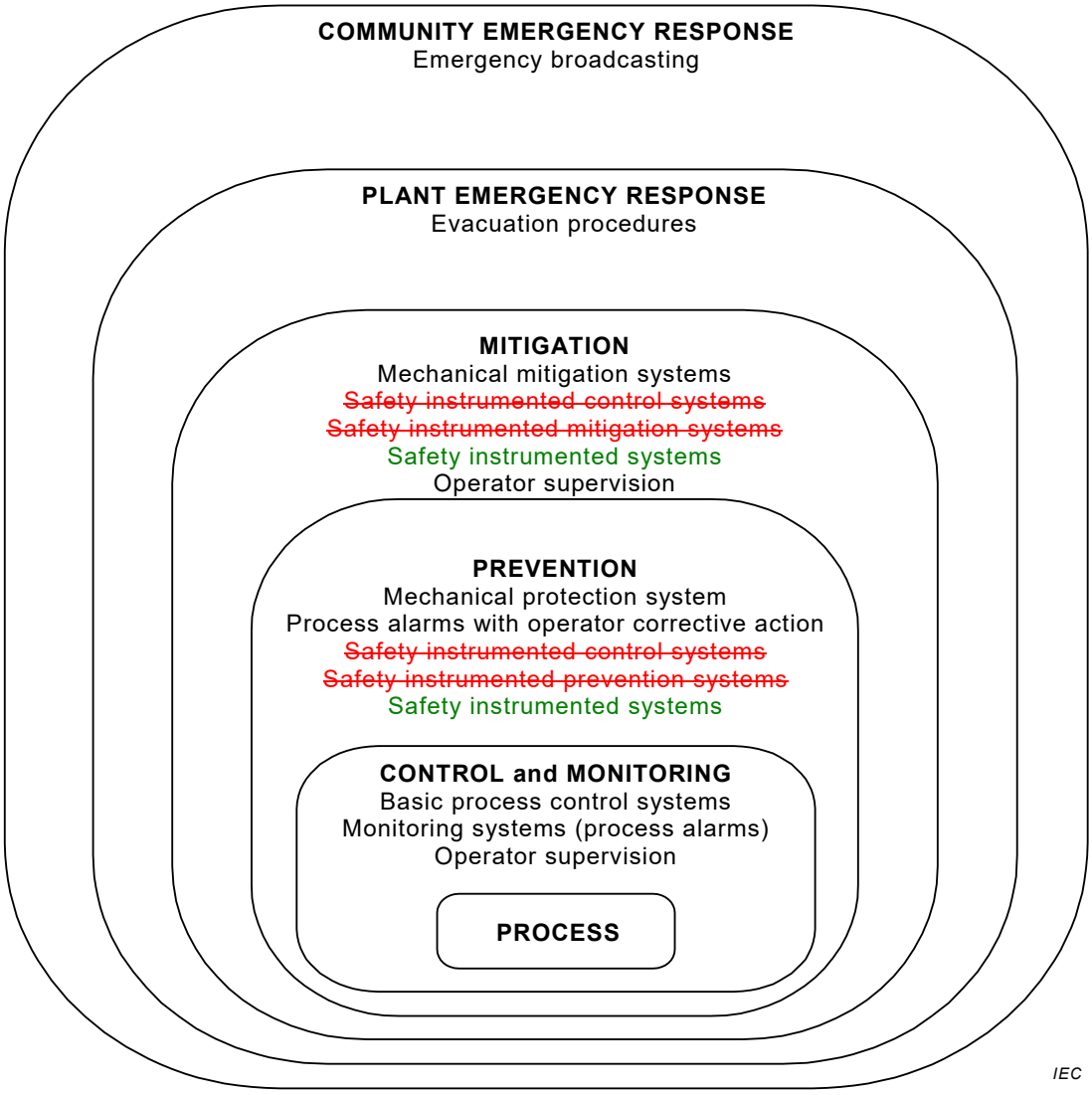


Figure 2 – Typical protection layers and risk reduction ~~methods~~ means ~~found in process plants (for example, protection layer model)~~

2 Normative references

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

IEC 61511-1:2016 *Functional safety – Safety instrumented systems for the process industry sector – Part 1: framework, definitions, system, hardware and application programming requirements*

Edition 2.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

IEC 61511-3:2016-07(en-fr)

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

Additional H&RA example(s) and quantitative analysis consideration annexes are provided.

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

FDIS	Report on voting
65A/779/FDIS	65A786/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.

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

A list of all parts in the IEC 61511 series, published under the general title *Functional safety – Safety instrumented systems for the process industry sector*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

The IEC 61511 series addresses the application of SIS for the process industries. A process hazard and risk assessment is carried out to enable the specification for SIS 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 SIS. The SIS includes all devices and subsystems necessary to carry out the SIF from sensor(s) to final element(s).

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

The IEC 61511 series addresses SIS 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 the IEC 61511 series should be applied. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of IEC 61508:2010.

The IEC 61511 series sets out an approach for SIS 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, and programmable electronic). Any safety strategy should consider each individual SIS in the context of the other protective systems. To facilitate this approach, the IEC 61511 series covers:

– a hazard and risk assessment is carried out to identify the overall safety requirements;
– an allocation of the safety requirements to the SIS is carried out;
– works within a framework which is applicable to all instrumented means of achieving functional safety;
– details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety;
– addressing all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
– enabling existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (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 regulations, these take precedence over the requirements defined in the IEC 61511-1.

The IEC 61511-3 deals with guidance in the area of determining the required SIL in hazards and risk assessment. The information herein is intended to provide a broad overview of the wide range of global methods used to implement hazards and risk assessment. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of SIL provided in IEC 61511-1:2016should be reviewed. The informative annexes in the IEC 61511-3 address the following:

Annex A provides information that is common to each of the hazard and risk assessment methods shown herein.

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.

Annex G provides a layer of protection analysis using a risk matrix.

Annex H provides an overview of a qualitative approach for risk estimation & SIL assignment.

Annex I provides an overview of the basic steps involved in designing and calibrating a risk graph.

Annex J provides an overview of the impact of multiple safety systems on determining the required SIL

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

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

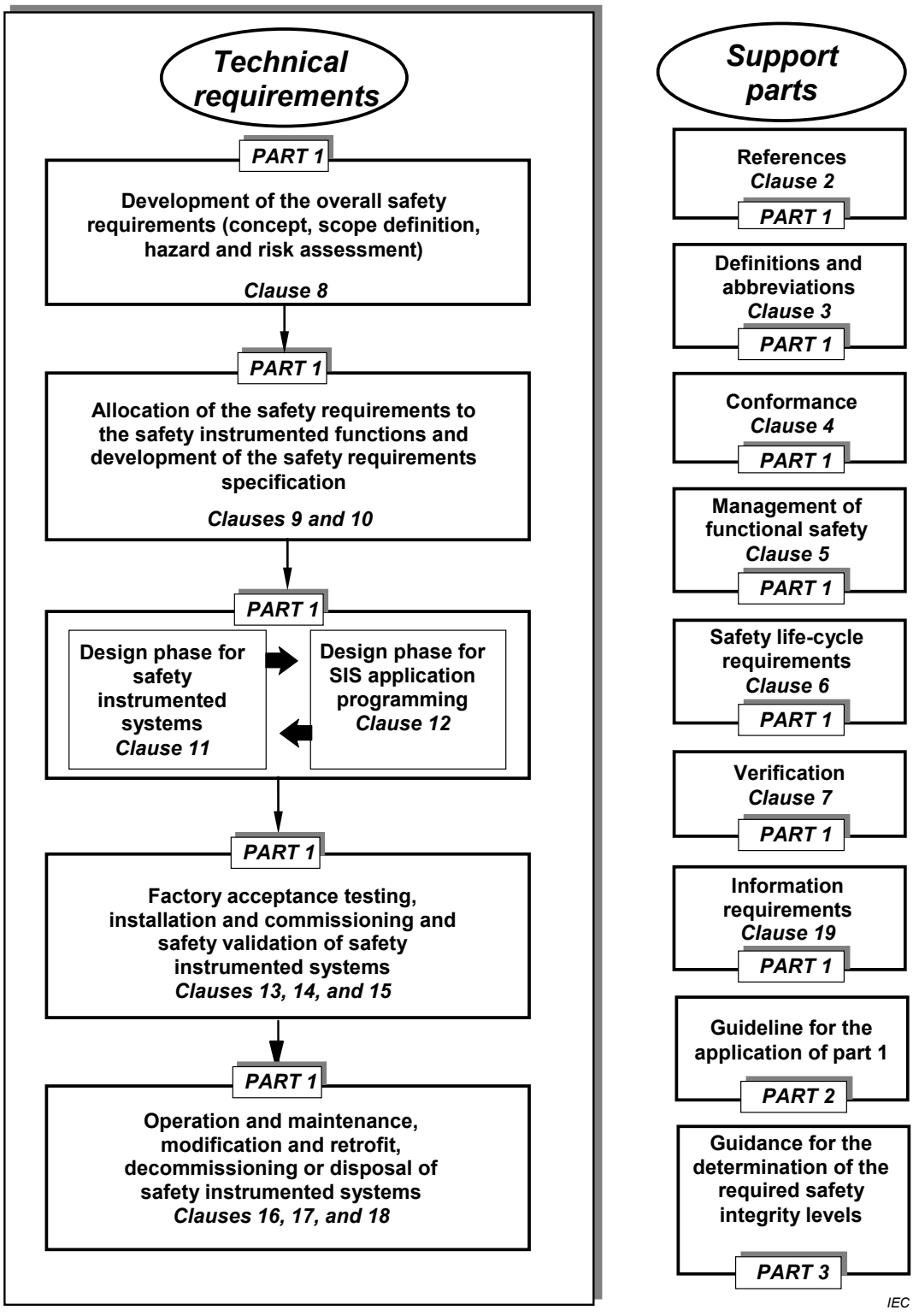


Figure 1 – Overall framework of the IEC 61511 series

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 and the relationship of risk to safety integrity (see Clause A.4);

– the determination of tolerable risk (see Annex K);

– a number of different methods that enable the safety integrity level (SIL) for the safety instrumented functions (SIF) to be determined (see Annexes B through K);

– the impact of multiple safety systems on calculations determining the ability to achieve the desired risk reduction (see Annex J).

In particular, this part of IEC 61511:

a) applies when functional safety is achieved using one or more SIF 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 SIL of each SIF;

d) illustrates techniques/measures available for determining the required SIL;

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

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

NOTE Examples given in the Annexes of this Standard are intended only as case specific examples of implementing IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

Annexes B through K 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 1 Those intending to apply the methods indicated in these annexes can consult the source material referenced in each annex.

NOTE 2 The methods of SIL determination included in Part 3 may not be suitable for all applications. In particular, specific techniques or additional factors that are not illustrated may be required for high demand or continuous mode of operation.

NOTE 3 The methods as illustrated herein may result in non-conservative results when they are used beyond their underlying limits and when factors such as common cause, fault tolerance, holistic considerations of the application, lack of experience with the method being used, independence of the protection layers, etc., are not properly considered. See Annex J.

Figure 2 gives an overview of typical protection layers and risk reduction means.

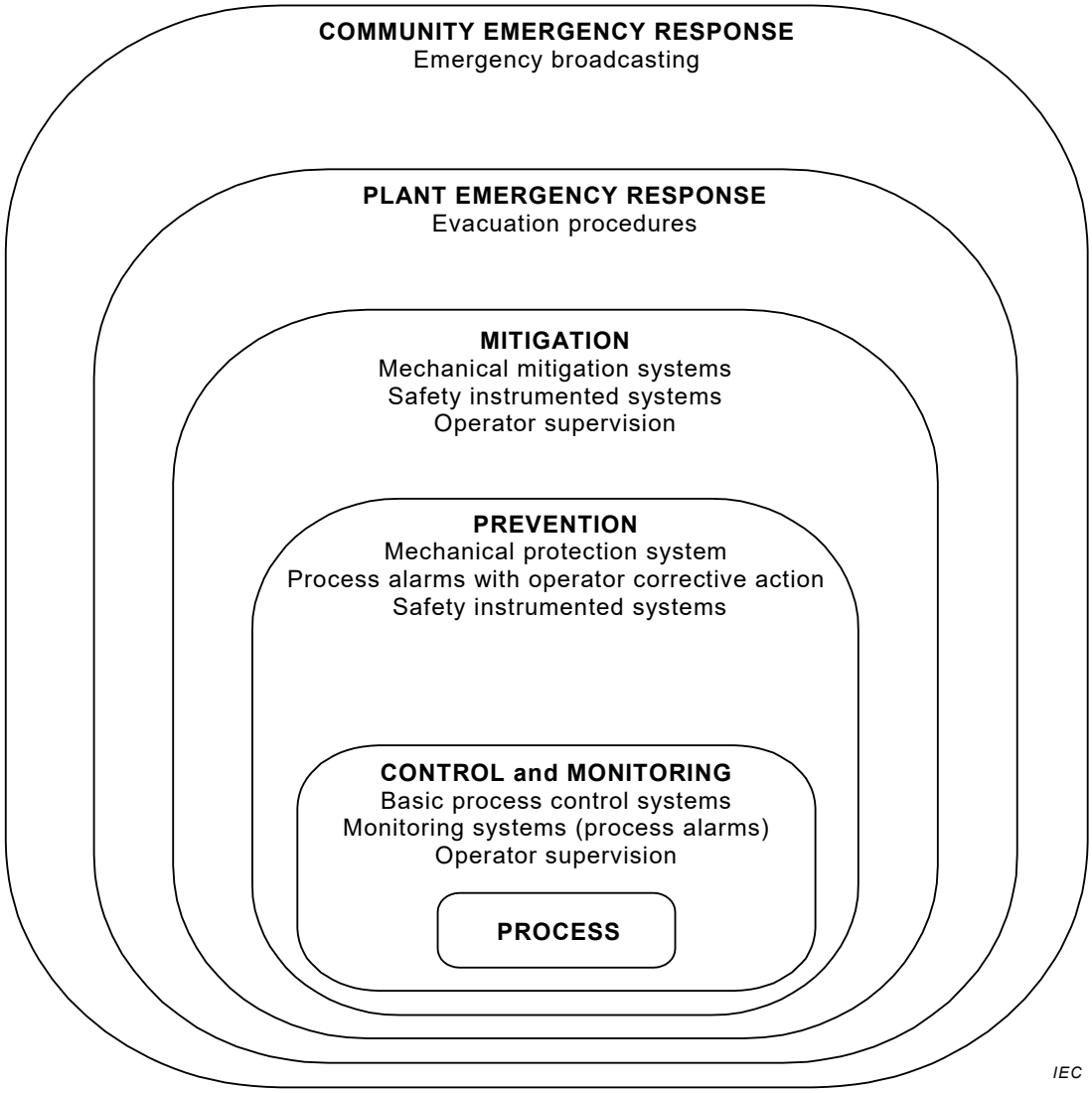


Figure 2 – Typical protection layers and risk reduction means

2 Normative references

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

IEC 61511-1:2016 *Functional safety – Safety instrumented systems for the process industry sector – Part 1: framework, definitions, system, hardware and application programming requirements*

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 (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61511-3 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 2003. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

Réalisation d'exemples additionnels H&RA et d'annexes sur la considération d'analyse quantitative.

Le texte de la présente norme est issu des documents suivants:

FDIS	Rapport de vote
65A/779/FDIS	65A/786/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

Une liste de toutes les parties de la série IEC 61511, publiées sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

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

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Les systèmes instrumentés de sécurité (SIS, *Safety Instrumented System*) sont utilisés dans les industries de transformation depuis de nombreuses années pour remplir des fonctions instrumentées de sécurité (SIF, *Safety Instrumented Function*). Si l'instrumentation doit être effectivement utilisée pour réaliser des SIF, il est essentiel que cette instrumentation satisfasse à certaines normes et certains niveaux de performance minimaux.

La série IEC 61511 concerne l'application du SIS aux industries de transformation. Elle exige également de procéder à une analyse de danger et de risque relative au processus pour en déduire la spécification relative aux SIS. D'autres systèmes de sécurité sont considérés uniquement pour que leur contribution puisse être prise en compte lors de l'étude des exigences de performance des SIS. Le SIS inclut tous les appareils et sous-systèmes nécessaires pour acheminer la SIF à partir du ou des capteurs jusqu'à l'élément terminal ou jusqu'aux éléments terminaux.

La série IEC 61511 aborde deux concepts, qui sont fondamentaux vis-à-vis de son application: le cycle de vie de sécurité du SIS et les niveaux d'intégrité de sécurité (SIL, *Safety Integrity Levels*).

La série IEC 61511 concerne les SIS reposant sur l'utilisation d'une technologie électrique (E)/électronique(E)/électronique programmable (PE). Si d'autres technologies sont utilisées pour les solveurs logiques, il convient d'appliquer les principes fondamentaux de la série IEC 61511. La série IEC 61511 concerne également les capteurs et les éléments terminaux des SIS, quelle que soit la technologie utilisée. La série IEC 61511 est propre aux industries de transformation, dans le cadre de la série IEC 61508:2010.

La série IEC 61511 définit une approche concernant les activités relatives au cycle de vie de sécurité des SIS dans le but de satisfaire à ces normes minimales. Cette approche a été adoptée afin de mettre en œuvre une politique technique cohérente et rationnelle.

Dans la plupart des cas, la sécurité est obtenue de la meilleure façon par une conception de processus à sécurité intrinsèque. Si nécessaire, cette approche peut être combinée à un ou plusieurs systèmes de protection afin de couvrir les risques résiduels identifiés éventuels. Les systèmes de protection peuvent reposer sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). Il convient que toute stratégie de sécurité prenne en compte chacun des SIS individuellement, dans le contexte des autres systèmes de protection. Pour faciliter cette approche, la série IEC 61511 couvre:

– la réalisation d'une analyse de danger et de risque pour identifier les exigences de sécurité globales;
– la prise en compte de l'affectation des exigences de sécurité aux SIS;
– l'inscription dans un cadre applicable à toutes les méthodes instrumentées qui permettent d'obtenir la sécurité fonctionnelle;
– les détails de l'utilisation de certaines activités (la gestion de la sécurité, par exemple) qui peuvent être applicables à toutes les méthodes permettant d'obtenir la sécurité fonctionnelle;
– la prise en compte de toutes les phases relatives au cycle de vie de sécurité du SIS (concept initial, conception, mise en œuvre, fonctionnement, maintenance, jusqu'au déclassement);
– l'harmonisation des normes de l'industrie de transformation nationales existantes ou nouvelles par rapport à la série IEC 61511.

La série IEC 61511 vise à obtenir un haut niveau de cohérence (des principes sous-jacents, de la terminologie, de l'information, par exemple) dans le secteur des industries de transformation. Il convient qu'il présente des avantages tant du point de vue de la sécurité que du point de vue économique.

Dans les juridictions où les autorités compétentes (nationales, fédérales, étatiques, provinciales, cantonales, municipales, par exemple) ont défini des réglementations relatives à la conception de la sécurité des processus, la gestion de la sécurité des processus ou autres, ces réglementations sont prioritaires par rapport aux exigences définies dans l'IEC 61511-1.

L'IEC 61511-3 donne des lignes directrices pour déterminer le niveau d'intégrité de sécurité (SIL) exigé dans le cadre de l'analyse de danger et de risque. Les informations contenues dans le présent document ont pour but de donner un aperçu général de la grande plage de méthodes globales utilisées pour mettre en œuvre une analyse de danger et de risque. Les informations fournies ne sont pas suffisamment détaillées pour mettre en œuvre ces approches.

Avant de continuer, il convient que le concept et la détermination du SIL présentés dans l'IEC 61511-1 soient passés en revue. Les annexes informatives de l'IEC 61511-3 abordent les points suivants:

L'Annexe A donne les informations communes à chacune des méthodes d'analyse de danger et de risque décrites dans le présent document.

L'Annexe B donne un aperçu général d'une méthode semi-quantitative utilisée pour déterminer le SIL exigé.

L'Annexe C donne un aperçu général d'une méthode utilisant une matrice de sécurité pour déterminer le SIL exigé.

L'Annexe D donne un aperçu général d'une méthode utilisant un graphe de risque semi-qualitatif pour déterminer le SIL exigé.

L'Annexe E donne un aperçu général d'une méthode utilisant un graphe de risque qualitatif pour déterminer le SIL exigé.

L'Annexe F donne un aperçu général utilisant une méthode d'analyse des couches de protection (LOPA, Layer Of Protection Analysis) pour sélectionner le SIL exigé.

L'Annexe G analyse les couches de protection utilisant une matrice de risque.

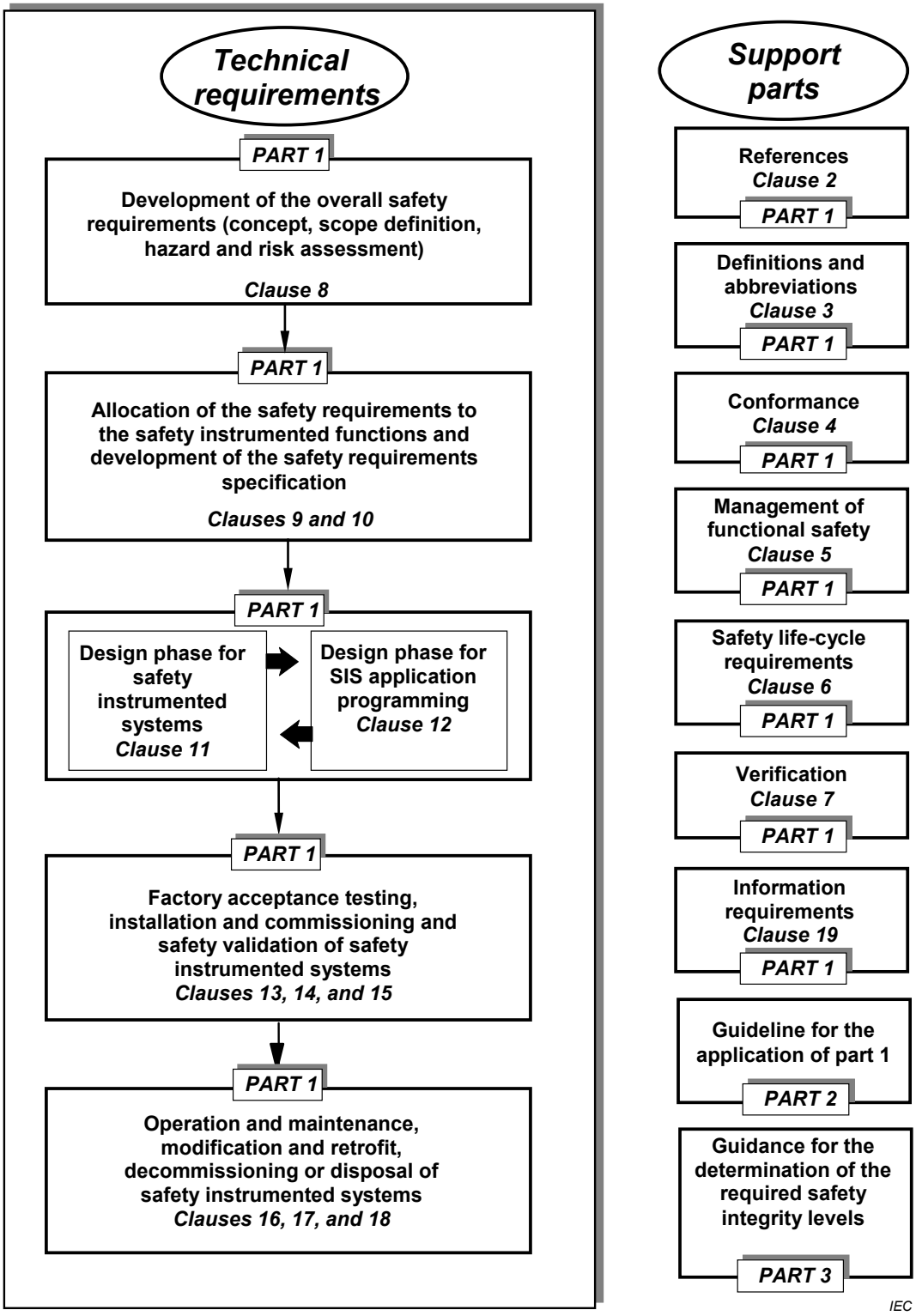
L'Annexe H donne un aperçu général d'une approche qualitative d'estimation du risque et d'allocation du SIL.

L'Annexe I donne un aperçu général des étapes de base de la conception et de l'étalonnage d'un graphe de risque.

L'Annexe J donne un aperçu général de l'impact de plusieurs systèmes de sécurité sur la détermination du SIL exigé.

L'Annexe K donne un aperçu général des concepts de risque tolérable et d'ALARP.

La Figure 1 présente le cadre général de l'IEC 61511-1, de l'IEC 61511-2 et de l'IEC 61511-3 et précise le rôle joué par la série IEC 61511 dans l'obtention de la sécurité fonctionnelle du SIS.



Anglais	Français
Technical requirements	Exigences techniques
PART 1	PARTIE 1
Development of the overall safety requirements (concept, scope definition, hazard and risk assessment) Clause 8	Développement des exigences de sécurité globales (concept, définition du domaine d'application, analyse de danger et de risque) Article 8
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification Clauses 9 and 10	Affectation des exigences de sécurité aux fonctions instrumentées de sécurité et développement de la spécification des exigences de sécurité Articles 9 et 10
Design phase for safety instrumented systems Clause 11	Phase de conception pour les systèmes instrumentés de sécurité Article 11
Design phase for SIS application programming Clause 12	Phase de conception pour la programmation d'application du SIS Article 12
Factory acceptance testing, installation and commissioning and safety validation of safety instrumented systems Clauses 13, 14, and 15	Essais de réception en usine, installation et mise en service, et validation de la sécurité des systèmes instrumentés de sécurité Articles 13, 14, et 15
Operation and maintenance, modification and retrofit, decommissioning or disposal of safety instrumented systems Clauses 16,17, and 18	Fonctionnement et maintenance, modification et remise à niveau, déclassement ou mise au rebut des systèmes instrumentés de sécurité Articles 16, 17, et 18
Support parts	Parties de prise en charge
References Clause 2	Références Article 2
Definitions and abbreviations Clause 3	Définitions et abréviations Article 3
Conformance Clause 4	Conformité Article 4
Management of functional safety Clause 5	Gestion de la sécurité fonctionnelle Article 5
Safety life-cycle requirements Clause 6	Exigences relatives au cycle de vie de sécurité Article 6
Verification Clause 7	Vérification Article 7
Information requirements Clause 19	Exigences relatives aux informations Article 19
Guideline for the application of part 1	Ligne directrice pour l'application de la Partie 1
PART 2	PARTIE 2
Guidance for the determination of the required safety integrity levels	Conseils pour la détermination des niveaux exigés d'intégrité de sécurité
PART 3	PARTIE 3

Figure 1 – Cadre général de la série IEC 61511

SÉCURITÉ FONCTIONNELLE – SYSTEMES INSTRUMENTES DE SECURITE 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 l'IEC 61511 donne des informations sur:

– les concepts sous-jacents de risque, et sur la relation entre risque et intégrité de sécurité (voir l'Article A.3);

– la détermination du risque tolérable (voir l'Annexe K);

– les différentes méthodes permettant de déterminer le niveau d'intégrité de sécurité (SIL) des fonctions instrumentées de sécurité (SIF) (voir les Annexes B à K);

– l'impact de plusieurs systèmes de sécurité sur les calculs déterminant la capacité à obtenir la réduction de risque souhaitée (voir l'Annexe J).

En particulier, la présente partie de l'IEC 61511:

a) s'applique lorsque la sécurité fonctionnelle est obtenue en utilisant une ou plusieurs SIF pour la protection du personnel, du grand public ou de l'environnement;

b) peut s'appliquer dans des applications non liées à la sécurité (notamment la protection des biens);

c) présente les méthodes d'analyse de danger et de risque qui peuvent être réalisées pour définir les exigences fonctionnelles de sécurité et le SIL de chaque SIF;

d) identifie des techniques et mesures disponibles pour déterminer le SIL exigé;

e) fournit un cadre pour la détermination du SIL, mais ne spécifie pas le SIL exigé pour des applications spécifiques;

f) ne donne aucun exemple de détermination des exigences relatives à d'autres méthodes de réduction de risque.

Les Annexes B à K décrivent des approches quantitatives et qualitatives qui ont été simplifiées pour présenter les principes sous-jacents. Ces annexes ont été incorporées pour présenter les principes généraux d'un certain nombre de méthodes, mais ne constituent pas une description exhaustive.

NOTE 1 Les personnes qui envisagent d'utiliser les méthodes indiquées dans ces annexes peuvent consulter le document source mentionné dans chaque annexe.

NOTE 2 Les méthodes de détermination du SIL incluses dans la Partie 3 peuvent ne pas convenir à toutes les applications. En particulier, des techniques spécifiques ou des facteurs supplémentaires qui ne sont pas présentés peuvent être exigés pour un fonctionnement en mode à sollicitation élevée ou en mode continu.

NOTE 3 Les méthodes décrites dans le présent document peuvent aboutir à des résultats imprudents lorsqu'elles sont utilisées au-delà de leurs limites sous-jacentes et lorsque des facteurs tels que la cause commune, la tolérance aux anomalies, les considérations holistiques de l'application, le manque d'expérience eu égard à la méthode utilisée, l'indépendance des couches de protection, etc. ne sont pas pris en considération correctement. Voir l'Annexe J.

La Figure 2 donne un aperçu général des couches de protection types et des moyens de réduction de risque.

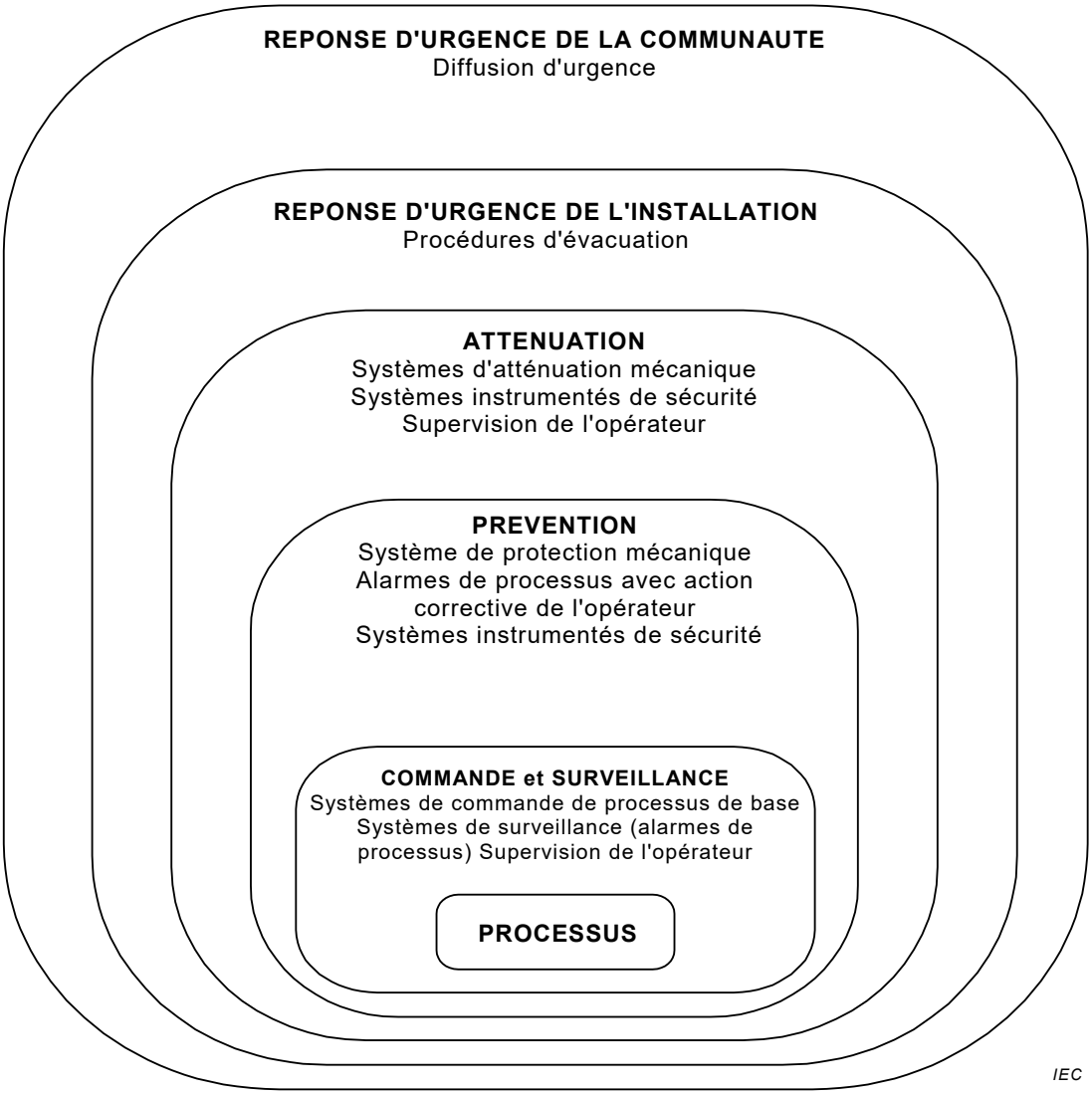


Figure 2 – Couches de protection classiques et moyens de réduction de risque

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61511-1:2016, *Sécurite fonctionnelle – Systèmes instrumentes de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application*