IEC 61511-2

Edition 1.0 2003-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de la CEI 61511-1

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61511-2

Edition 1.0 2003-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de la CEI 61511-1

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XC
CODE PRIX

ICS 13.110; 25.040.01

ISBN 2-8318-7556-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

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 61511-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

This bilingual version, published in 2004-07, corresponds to the English version.

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

FDIS	Report on voting
65A/387A/FDIS	65A/390/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 series has been developed as a process sector implementation of IEC 61508 series.

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.

This International Standard addresses the application of safety instrumented systems for the Process Industries. It also deals with the interface between safety instrumented systems and other safety systems in requiring that a process hazard and risk assessment be carried out. The safety instrumented system includes sensors, logic solvers and final elements.

This International Standard has two concepts, which are fundamental to its application; safety lifecycle and safety integrity levels. The safety lifecycle forms the central framework which links together most of the concepts in this International Standard.

The safety instrumented system logic solvers addressed include Electrical (E)/Electronic (E)/ and Programmable Electronic (PE) technology. Where other technologies are used for logic solvers, the basic principles of this standard may also be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This International Standard is process industry specific within the framework of the IEC 61508 series.

This International 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 is used. The objective of this standard is to provide guidance on how to comply with IEC 61511-1.

To facilitate use of this standard, the clause and subclause numbers provided are identical to the corresponding normative text in 61511-1 (excluding the annexes).

In most situations, safety is best achieved by an inherently safe process design whenever practicable, combined, if necessary, with a number of protective systems which rely on different technologies (for example, chemical, mechanical, hydraulic, pneumatic, electrical, electronic, thermodynamic (for example, flame arrestors), programmable electronic) which manage any residual identified risk. Any safety strategy considers 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 functions and related safety systems, such as 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 International Standard on safety instrumented systems for the process industry:

- addresses relevant safety lifecycle stages from initial concept, through design, implementation, operation and maintenance and 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.

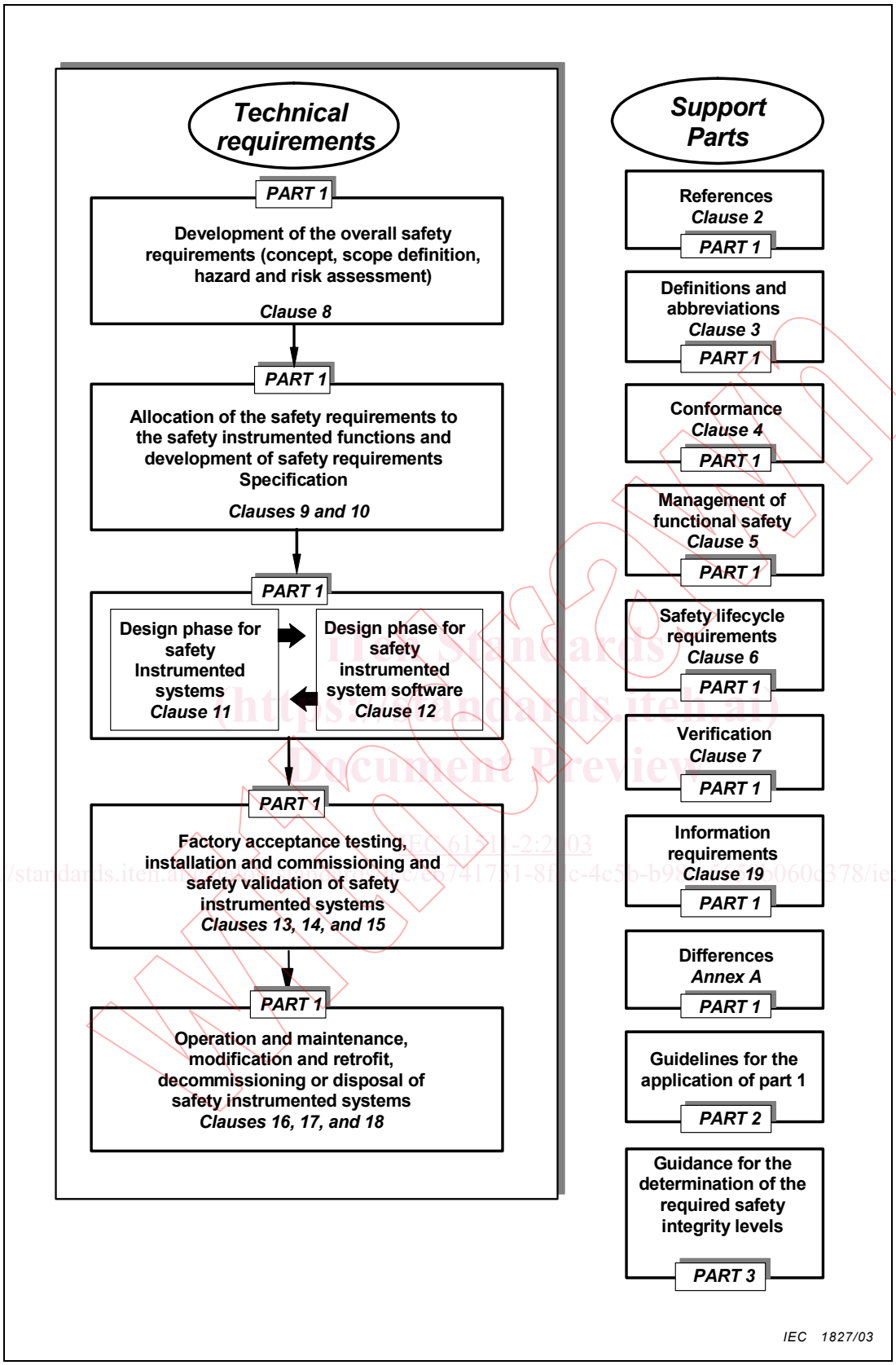

Figure 1 – Overall framework of this standard

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

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

1 Scope

IEC 61511-2 provides guidance on the specification, design, installation, operation and maintenance of Safety Instrumented Functions and related safety instrumented system as defined in IEC 61511-1. This standard has been organized so that each clause and subclause number herein addresses the same clause number in IEC 61511-1 (with the exception of the annexes).

2 Normative references

No further guidance provided.

3 Terms, definitions and abbreviations

No further guidance provided except for 3.2.68 and 3.2.71 of IEC 61511-1.

3.2.68 A safety function should prevent a specified hazardous event. For example, “prevent the pressure in vessel #ABC456 exceeding 100 bar.” A safety function may be achieved by

a) a single safety instrumented system (SIS), or

b) one or more safety instrumented systems and/or other layers of protection.

In case b), each safety instrumented system or other layer of protection has to be capable of achieving the safety function and the overall combination has to achieve the required risk reduction (process safety target).

3.2.71 Safety instrumented functions are derived from the safety function, have an associated safety integrity level (SIL) and are carried out by a specific safety instrumented system (SIS). For example, “close valve #XY123 within 5 s when pressure in vessel #ABC456 reaches 100 bar”. Note that components of a safety instrumented system may be used by more than one safety instrumented function.

4 Conformance to this International Standard

No further guidance provided.

5 Management of functional safety

5.1 Objective

The objective of Clause 5 of IEC 61511-1 is to provide requirements for implementing the management activities that are necessary to ensure that the functional safety objectives are met.

5.2 Requirements

5.2.1 General

5.2.1.1 No further guidance provided.

5.2.1.2 When an organization has responsibility for one or more activities necessary for functional safety and that organization works according to quality assurance procedures, then many of these activities described in this clause will already be carried out for the purposes of quality. Where this is the case, it may be unnecessary to repeat these activities for the purposes of functional safety. In such cases, the quality assurance procedures should be reviewed to establish that they are suitable so that the objectives of functional safety will be achieved.

5.2.2 Organization and resources

5.2.2.1 The organizational structure associated with safety instrumented systems within a Company/Site/Plant/Project should be defined and the roles and responsibilities of each element clearly understood and communicated. Within the structure, individual roles, including their description and purpose should be identified. For each role, unambiguous accountabilities should be identified; and specific responsibilities should be recognised. In addition, whom the individual reports to and who makes the appointment should be identified. The intent is to ensure that everyone in an organization understands their role and responsibilities for safety instrumented systems.

5.2.2.2 The skills and knowledge required to implement any of the activities of the safety life cycle relating to the safety instrumented systems should be identified; and for each skill, the required competency levels should be defined. Resources should be assessed against each skill for competency and also the number of people per skill required. When differences are identified, development plans should be established to enable the required competency levels to be achieved in a timely manner. When shortages of skills arise, suitably qualified and experienced personnel may be recruited or contracted.

5.2.3 Risk evaluation and risk management

The requirement stated in 5.2.3 of IEC 61511 is that hazards are identified, risks evaluated and the necessary risk reduction is determined. It is recognized that there are numerous different methodologies available for conducting these evaluations. IEC 61511-1 does not endorse any particular methodology. Instead, the reader is encouraged to review a number of methodologies on this issue in IEC 61511-3. See 8.2.1 for further guidance.

5.2.4 Planning

The intent of this subclause is to ensure that, within the overall project, adequate safety planning is conducted so that all of the required activities during each phase of the lifecycle (for example, engineering design, plant operation) are addressed. The standard does not require any particular structure for these planning activities, but it does require periodic update or review of them.

5.2.5 Implementing and monitoring

5.2.5.1 The intent of this subclause is to ensure that effective management procedures are in place to

- ensure that all recommendations resulting from hazard analysis, risk assessment, other assessment and auditing activities, verification and validation activities are satisfactorily resolved.
- determine that the SIS is performing in accordance with its safety requirements specification throughout its operational lifetime.

5.2.5.2 Note that, in this context, suppliers could include design contractors and maintenance contractors as well as suppliers of components.

5.2.5.3 A review of the SIS performance should be periodically undertaken to ensure the original assumptions made during the development of the safety requirements specification (SRS) are still adhered to. For example, a periodic review of the assumed failure rate of different components in a SIS should be carried out to ensure that it remains as originally defined. If the failure rates are worse than originally anticipated, a design modification may be necessary. Likewise, the demand rate on the SIS should be reviewed. If the rate is more than that which was originally assumed, then an adjustment in the SIL may be needed.

5.2.6 Assessment, auditing and revision

Assessments and audits are tools targeted at the detection and elimination of errors. The paragraphs below make clear the distinction between these activities

Functional safety assessment aims to evaluate whether provisions made during the assessed lifecycle phases are adequate for the achievement of safety. Judgements are made by assessors on the decisions taken by those responsible for the realisation of functional safety. An assessment would for example be made prior to commissioning as to whether procedures for maintenance are adequate.

Functional safety auditors will determine from project or plant records whether the necessary procedures have been applied at the specified frequency by persons with the necessary competence. Auditors are not required to make judgements on the adequacy of the work they are considering. However, if they became aware that there would be benefits in making changes, then an observation should be included in the report.

It should be noted that in many cases there can be an overlap between the work of the assessor and the auditor. For example an auditor may need to determine not only whether an operator has been given the necessary training but in addition make judgements as to whether the training has resulted in the required competency.

5.2.6.1 Functional safety assessment

5.2.6.1.1 The use of Functional Safety Assessment (FSA) is fundamental in demonstrating that a Safety Instrumented System (SIS) fulfils its requirements regarding safety instrumented function(s) and Safety Integrity Level (SIL). The basic objective of this assessment is to demonstrate compliance with agreed standards and practices through independent assessment of the system's development process. An assessment of a SIS may be needed at different lifecycle stages. In order to conduct an effective assessment, a procedure should be developed that defines the scope of this assessment along with some guidance on the makeup of the assessment team.

The following attributes are considered good practice for Functional Safety Assessment:

- A plan should be generated for each FSA identifying such arrangements as the scope of the assessment, the assessors, the competencies of the assessors and the information to be generated by the assessment.
- The FSA should take into account other standards and practices, which may be contained within external or internal corporate standards, guides, procedures or codes of practice. The FSA plan should define what is to be assessed for the particular assessment/ system/application area.
- The frequency of FSAs may vary across different system developments but as a minimum should always take place before the potential hazards being presented to the system. Some companies also like to conduct an assessment prior to the construction/installation phase to prevent costly rework later in the lifecycle.
- FSA frequency and rigour should be defined taking into account system attributes such as:
  - complexity;
  - safety significance;
  - previous experience of similar systems;
  - standardization of design features.
- Sufficient evidence of design, installation, verification and validation activities should be available prior to the assessment. The availability of sufficient evidence could itself be an assessment criterion. The evidence should represent the current/approved state of system design or installation.
- The independence of the assessor(s) must be appropriate.
- The assessor(s) should have experience and knowledge appropriate to the technology and application area of the system being assessed.
- A systematic and consistent approach to FSA should be maintained throughout the lifecycle and across systems. FSA is a subjective activity therefore detailed guidance, possibly through the use of checklists, as to what is acceptable for an organisation should be defined to remove as much subjectivity as possible.

Records generated from the FSA should be complete and the conclusions agreed with those responsible for the management of functional safety for the SIS prior to commencement of the next lifecycle phase.