

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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2003 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, 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 either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, 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 la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

FOREWORD.....	7
INTRODUCTION.....	6
1 Scope.....	9
2 Normative references	9
3 Terms, definitions and abbreviations	9
4 Conformance to this International Standard	9
5 Management of functional safety	10
5.1 Objective	10
5.2 Requirements	10
6 Safety lifecycle requirements	17
6.1 Objective	17
6.2 Requirements	17
7 Verification	18
7.1 Objective	18
8 Process hazard and risk assessment.....	18
8.1 Objectives	18
8.2 Requirements	18
9 Allocation of safety functions to protection layers	21
9.1 Objective	21
9.2 Requirements of the allocation process	21
9.3 Additional requirements for safety integrity level 4.....	24
9.4 Requirement on the basic process control system as a layer of protection.....	24
9.5 Requirements for preventing common cause, common mode and dependent failures	25
10 SIS safety requirements specification	26
10.1 Objective.....	26
10.2 General requirements.....	26
10.3 SIS safety requirements	26
11 SIS design and engineering.....	28
11.1 Objective.....	28
11.2 General requirements.....	28
11.3 Requirements for system behaviour on detection of a fault.....	33
11.4 Requirements for hardware fault tolerance	33
11.5 Requirements for selection of components and subsystems	34
11.6 Field devices	37
11.7 Interfaces	37
11.8 Maintenance or testing design requirements.....	40
11.9 SIF probability of failure	41
12 Requirements for application software, including selection criteria for utility software	43
12.1 Application software safety lifecycle requirements	43
12.2 Application software safety requirements specification	47

12.3	Application software safety validation planning.....	49
12.4	Application software design and development	49
12.5	Integration of the application software with the SIS subsystem	57
12.6	FPL and LVL software modification procedures	57
12.7	Application software verification	58
13	Factory acceptance testing (FAT)	59
13.1	Objectives	59
13.2	Recommendations.....	59
14	SIS installation and commissioning.....	60
14.1	Objectives	60
14.2	Requirements	60
15	SIS safety validation.....	60
15.1	Objective	60
15.2	Requirements	60
16	SIS operation and maintenance	61
16.1	Objectives	61
16.2	Requirements	61
16.3	Proof testing and inspection	61
17	SIS modification	63
17.1	Objective	63
17.2	Requirements	63
18	SIS decommissioning	63
18.1	Objectives	63
18.2	Requirements	63
19	Information and documentation requirements	64
19.1	Objectives	64
19.2	Requirements.....	64
	Annex A (informative) Example of techniques for calculating the probability of failure on demand for a safety instrumented function.....	65
	Annex B (informative) Typical SIS architecture development.....	66
	Annex C (informative) Application features of a safety PLC	71
	Annex D (informative) Example of SIS logic solver application software development methodology	73
	Annex E (informative) Example of development of externally configured diagnostics for a safety-configured PE logic solver	78
	Figure 1 – Overall framework of this standard	8
	Figure 2 – BPCS function and initiating cause independence illustration	25
	Figure 3 – Software development lifecycle (the V-model).....	44
	Figure C.1 – Logic solver	72
	Figure E.1 – EWDT timing diagram	80
	Table 1 – Typical Safety Manual organisation and contents	55

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.

Withdrawn