

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems**

**Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité**



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2012 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

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://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.

#### Useful links:

IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

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

Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [csc@iec.ch](mailto:csc@iec.ch).

### 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 de la 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.

#### Liens utiles:

Recherche de publications CEI - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

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

Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [csc@iec.ch](mailto:csc@iec.ch).

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems**

**Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-0487-0

**Warning! Make sure that you obtained this publication from an authorized distributor.  
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

## CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope and object.....	10
2 Normative references .....	11
3 Terms, definitions and abbreviations .....	12
3.1 Alphabetical list of definitions .....	12
3.2 Terms and definitions .....	14
3.3 Abbreviations .....	21
4 Management of functional safety .....	22
4.1 Objective .....	22
4.2 Requirements .....	22
5 Requirements for the specification of Safety-Related Control Functions (SRCFs).....	24
5.1 Objective .....	24
5.2 Specification of requirements for SRCFs .....	24
6 Design and integration of the safety-related electrical control system (SRECS).....	26
6.1 Objective .....	26
6.2 General requirements.....	26
6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS .....	27
6.4 Requirements for systematic safety integrity of the SRECS .....	28
6.5 Selection of safety-related electrical control system .....	30
6.6 Safety-related electrical control system (SRECS) design and development .....	30
6.7 Realisation of subsystems .....	35
6.8 Realisation of diagnostic functions .....	51
6.9 Hardware implementation for SRECS .....	52
6.10 Software safety requirements specification.....	52
6.11 Software design and development.....	53
6.12 Safety-related electrical control system integration and testing.....	60
6.13 SRECS installation.....	62
7 Information for use of the SRECS.....	62
7.1 Objective.....	62
7.2 Documentation for installation, use and maintenance .....	62
8 Validation of the safety-related electrical control system.....	63
8.1 Objective.....	63
8.2 General requirements.....	63
8.3 Validation of SRECS systematic safety integrity .....	64
9 Modification.....	65
9.1 Objective.....	65
9.2 Modification procedure .....	65
9.3 Configuration management procedures .....	65
10 Documentation .....	67

Annex A (informative) SIL assignment .....	69
Annex B (informative) Example of safety-related electrical control system (SRECS) design using concepts and requirements of Clauses 5 and 6 .....	77
Annex C (informative) Guide to embedded software design and development.....	84
<del>Annex D (informative) Failure modes of electrical/electronic components .....</del>	<del>92</del>
<del>Annex E (informative) Electromagnetic (EM) phenomenon and increased immunity levels for SRECS intended for use in an industrial environment according to IEC 61000-6-2 .....</del>	<del>97</del>
Annex F (informative) Methodology for the estimation of susceptibility to common cause failures (CCF) .....	99
Figure 1 – Relationship of IEC 62061 to other relevant standards .....	8
Figure 2 – Workflow of the SRECS design and development process .....	32
Figure 3 – Allocation of safety requirements of the function blocks to subsystems (see 6.6.2.1.1) .....	33
Figure 4 – Workflow for subsystem design and development (see box 6B of Figure 2) .....	38
Figure 5 – Decomposition of a function block into redundant function block elements and their associated subsystem elements .....	39
Figure 6 – Subsystem A logical representation .....	45
Figure 7 – Subsystem B logical representation .....	46
Figure 8 – Subsystem C logical representation .....	46
Figure 9 – Subsystem D logical representation .....	48
Figure A.1 – Workflow of SIL assignment process.....	70
Figure A.2 – Parameters used in risk estimation .....	71
Figure A.3 – Example proforma for SIL assignment process .....	78
Figure B.1 – Terminology used in functional decomposition .....	77
Figure B.2 – Example machine .....	78
Figure B.3 – Specification of requirements for an SRCF .....	78
Figure B.4 – Decomposition to a structure of function blocks .....	79
Figure B.5 – Initial concept of an architecture for a SRECS .....	80
Figure B.6 – SRECS architecture with diagnostic functions embedded within each subsystem (SS1 to SS4) .....	81
Figure B.7 – SRECS architecture with diagnostic functions embedded within subsystem SS2 .....	82
Figure B.8 – Estimation of $PFH_D$ for a SRECS.....	83
<del>Table 1 – Recommended application of IEC 62061 and ISO 13849-1 (under revision) .....</del>	<del>9</del>
Table 2 – Overview and objectives of IEC 62061 .....	11
Table 3 – Safety integrity levels: target failure values for SRCFs .....	26
Table 4 – Characteristics of subsystems 1 and 2 used in this example.....	35
Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem .....	41
<del>Table 6 – Architectural constraints: SILCL relating to categories.....</del>	<del>41</del>
<del>Table 7 – Probability of dangerous failure .....</del>	<del>44</del>
Table 8 – Information and documentation of a SRECS.....	68

Table A.1 – Severity (Se) classification.....	72
Table A.2– Frequency and duration of exposure (Fr) classification .....	72
Table A.3– Probability (Pr) classification.....	73
Table A.4– Probability of avoiding or limiting harm (Av) classification .....	74
Table A.5– Parameters used to determine class of probability of harm (Cl) .....	74
Table A.6 – SIL assignment matrix.....	75
<del>Table D.1 – Examples of the failure mode ratios for electrical/electronic components .....</del>	<del>92</del>
<del>Table E.1 – EM phenomenon and increased immunity levels for SRECS .....</del>	<del>97</del>
<del>Table E.2 – Selected frequencies for RF field tests .....</del>	<del>98</del>
<del>Table E.3 – Selected frequencies for conducted RF tests .....</del>	<del>98</del>
Table F.1 – Criteria for estimation of CCF.....	99
Table F.2 – Estimation of CCF factor ( $\beta$ ).....	100

Currently in preview, click buy full version

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SAFETY OF MACHINERY –  
FUNCTIONAL SAFETY OF SAFETY-RELATED ELECTRICAL,  
ELECTRONIC AND PROGRAMMABLE ELECTRONIC  
CONTROL SYSTEMS**

## 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, accept 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.

**This consolidated version of IEC 62061 consists of the first edition (2005) [documents 44/407/FDIS and 44/470/RVD], its amendment 1 (2012) [documents 44/655/CDV and 44/653/RFC] and its corrigenda of July 2005 and April 2008. It bears the edition number 1.1.**

**The technical content is therefore identical to the base edition and its amendment and has been prepared for user convenience. A vertical line in the margin shows where the base publication has been modified by amendment 1. Additions and deletions are displayed in red, with deletions being struck through.**

International Standard IEC 62061 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

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

The committee has decided that the contents of the base publication and its amendments will remain unchanged until the stability 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.

**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 publication using a colour printer.**

## INTRODUCTION

As a result of automation, demand for increased production and reduced operator physical effort, Safety-Related Electrical Control Systems (referred to as SRECS) of machines play an increasing role in the achievement of overall machine safety. Furthermore, the SRECS themselves increasingly employ complex electronic technology.

Previously, in the absence of standards, there has been a reluctance to accept SRECS in safety-related functions for significant machine hazards because of uncertainty regarding the performance of such technology.

This International Standard is intended for use by machinery designers, control system manufacturers and integrators, and others involved in the specification, design and validation of a SRECS. It sets out an approach and provides requirements to achieve the necessary performance.

This standard is machine sector specific within the framework of IEC 61508. It is intended to facilitate the specification of the performance of safety-related electrical control systems in relation to the significant hazards (see 3.8 of ISO 12100-1) of machines.

This standard provides a machine sector specific framework for functional safety of a SRECS of machines. It only covers those aspects of the safety lifecycle that are related to safety requirements allocation through to safety validation. Requirements are provided for information for safe use of SRECS of machines that can also be relevant to later phases of the life of a SRECS.

There are many situations on machines where SRECS are employed as part of safety measures that have been provided to achieve risk reduction. A typical case is the use of an interlocking guard that, when it is opened to allow access to the danger zone, signals the electrical control system to stop hazardous machine operation. Also in automation, the electrical control system that is used to achieve correct operation of the machine process often contributes to safety by mitigating risk associated with hazards arising directly from control system failures. This standard gives a methodology and requirements to

- assign the required safety integrity level for each safety-related control function to be implemented by SRECS;
- enable the design of an SRECS appropriate to the assigned safety-related control function(s);
- integrate safety-related subsystems designed in accordance with ISO 13849 ;
- validate the SRECS.

This standard is intended to be used within the framework of systematic risk reduction described in ISO 12100-1 and in conjunction with risk assessment according to the principles described in ISO 14121 (EN 1050). A suggested methodology for safety integrity level (SIL) assignment is given in informative Annex A.

Measures are given to co-ordinate the performance of the SRECS with the intended risk reduction taking into account the probabilities and consequences of random or systematic faults within the electrical control system.

Figure 1 shows the relationship of this standard to other relevant standards.

~~Table 1 gives recommendations on the recommended application of this standard and the revision of ISO 13849-1.~~

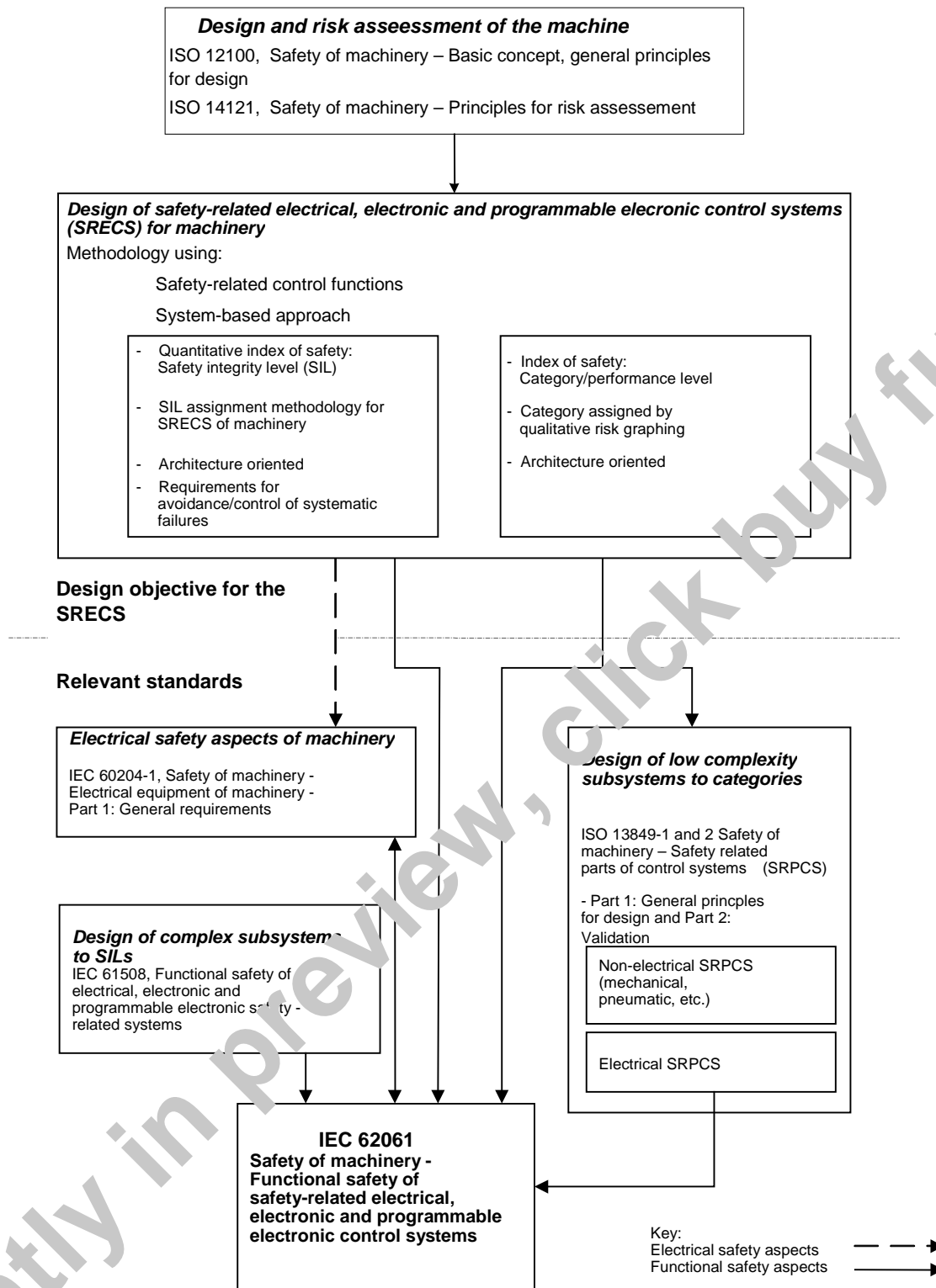


Figure 1 – Relationship of IEC 62061 to other relevant standards

~~Information on the recommended application of IEC 62061 and ISO 13849-1 (under revision)~~

IEC 62061 and ISO 13849-1 ~~(under revision)~~ specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. ~~Table 1 summarises the scopes of IEC 62061 and ISO 13849-1 (under revision).~~ IEC/TR 62061-1 provides guidance on the application of IEC 62061 and ISO 13849-1 in the design of safety-related control systems for machinery.

~~NOTE ISO 13849-1 is currently under preparation by ISO TC 199 and CEN TC 114.~~

**Table 1 – Recommended application of IEC 62061 and ISO 13849-1 (under revision)**

	<b>Technology implementing the safety-related control function(s)</b>	<b>ISO-13849-1 (under revision)</b>	<b>IEC 62061</b>
A	Non-electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, or non-complex electronics	Restricted to designated architectures (see Note 1) and up to PL=e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures (see Note 1) and up to PL=e	X see Note 3
E	C combined with B	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X see Note 2	X see Note 3
<p>"X" indicates that this item is dealt with by the standard shown in the column heading.</p> <p>NOTE 1 – Designated architectures are defined in Annex B of EN ISO 13849-1(rev.) to give a simplified approach for quantification of performance level.</p> <p>NOTE 2 – For complex electronics: Use of designated architectures according to EN ISO 13849-1(rev.) up to PL=d or any architecture according to IEC 62061.</p> <p>NOTE 3 – For non-electrical technology use parts according to EN ISO 13849-1(rev.) as subsystems.</p>			

# SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED ELECTRICAL, ELECTRONIC AND PROGRAMMABLE ELECTRONIC CONTROL SYSTEMS

## 1 Scope

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machines (see Notes 1 and 2). It is applicable to control systems used, either singly or in combination, to carry out safety-related control functions on machines that are not portable by hand while working, including a group of machines working together in a co-ordinated manner.

NOTE 1 In this standard, the term “electrical control systems” is used to stand for “Electrical, Electronic and Programmable Electronic (E/E/PE) control systems” and “SRECS” is used to stand for “safety-related electrical, electronic and programmable electronic control systems”.

NOTE 2 In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508 and uses Route 1<sub>H</sub> (see IEC 61508-2:2010, 7.4.4.2). It is considered that Route 2<sub>H</sub> (see IEC 61508-2:2010, 7.4.4.3) is not suitable for general machinery. Therefore, this standard does not deal with Route 2<sub>H</sub>. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of a SRECS.

This standard is an application standard and is not intended to limit or inhibit technological advancement. It does not cover all the requirements (e.g. guarding, non-electrical interlocking or non-electrical control) that are needed or required by other standards or regulations in order to safeguard persons from hazards. Each type of machine has unique requirements to be satisfied to provide adequate safety.

This standard:

- is concerned only with functional safety requirements intended to reduce the risk of injury or damage to the health of persons in the immediate vicinity of the machine and those directly involved in the use of the machine;
- is restricted to risks arising directly from the hazards of the machine itself or from a group of machines working together in a co-ordinated manner;

NOTE 3 Requirements to mitigate risks arising from other hazards are provided in relevant sector standards. For example, where a machine(s) is part of a process activity, the machine electrical control system functional safety requirements should, in addition, satisfy other requirements (e.g. IEC 61511) insofar as safety of the process is concerned.

- does not specify requirements for the performance of non-electrical (e.g. hydraulic, pneumatic) control elements for machines;

NOTE 4 Although the requirements of this standard are specific to electrical control systems, the framework and methodology specified can be applicable to safety-related parts of control systems employing other technologies.

- does not cover electrical hazards arising from the electrical control equipment itself (e.g. electric shock – see IEC 60204–1).