

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 © 2005 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 It also gives information on projects, withdrawn and replaced publications.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

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

PRICE CODE
CODE PRIX

XD

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	22
4 Management of functional safety	23
4.1 Objective	23
4.2 Requirements	23
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).....	27
6.1 Objective	27
6.2 General requirements	27
6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS	28
6.4 Requirements for systematic safety integrity of the SRECS	29
6.5 Selection of safety-related electrical control system	31
6.6 Safety-related electrical control system (SRECS) design and development	31
6.7 Realisation of subsystems	36
6.8 Realisation of diagnostic functions	52
6.9 Hardware implementation of the SRECS	53
6.10 Software safety requirements specification.....	53
6.11 Software design and development.....	54
6.12 Safety-related electrical control system integration and testing.....	62
6.13 SRECS installation	63
7 Information for use of the SRECS.....	63
7.1 Objective	63
7.2 Documentation for installation, use and maintenance	63
8 Validation of the safety-related electrical control system.....	64
8.1 General requirements	65
8.2 Validation of SRECS systematic safety integrity	65
9 Modification	66
9.1 Objective	66
9.2 Modification procedure	66
9.3 Configuration management procedures	67
10 Documentation	69

Annex A (informative) SIL assignment	71
Annex B (informative) Example of safety-related electrical control system (SRECS) design using concepts and requirements of Clauses 5 and 6	79
Annex C (informative) Guide to embedded software design and development.....	86
Annex D (informative) Failure modes of electrical/electronic components	95
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	100
Annex F (informative) Methodology for the estimation of susceptibility to common cause failures (CCF).....	102
Figure 1 – Relationship of IEC 62061 to other relevant standards	8
Figure 2 – Workflow of the SRECS design and development process	33
Figure 3 – Allocation of safety requirements of the function blocks to subsystems (see 6.6.2.1.1)	34
Figure 4 – Workflow for subsystem design and development (see box 6B of Figure 2)	39
Figure 5 – Decomposition of a function block into redundant function block elements and their associated subsystem elements	40
Figure 6 – Subsystem A logical representation	46
Figure 7 – Subsystem B logical representation	47
Figure 8 – Subsystem C logical representation	47
Figure 9 – Subsystem D logical representation	49
Figure A.1 – Workflow of SIL assignment process.....	72
Figure A.2 – Parameters used in risk estimation	73
Figure A.3 – Example proforma for SIL assignment process	78
Figure B.1 – Terminology used in functional decomposition	79
Figure B.2 – Example machine	80
Figure B.3 – Specification of requirements for an SRCF	80
Figure B.4 – Decomposition to a structure of function blocks	81
Figure B.5 – Initial concept of an architecture for a SRECS	82
Figure B.6 – SRECS architecture with diagnostic functions embedded within each subsystem (SS1 to SS4)	83
Figure B.7 – SRECS architecture with diagnostic functions embedded within subsystem SS3.....	84
Figure B.8 – Estimation of PFH_D for a SRECS.....	85
Table 1 – Recommended application of IEC 62061 and ISO 13849-1(under revision)	9
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.....	36
Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem	42
Table 6 – Architectural constraints: SILCL relating to categories.....	43
Table 7 – Probability of dangerous failure	45
Table 8 – Information and documentation of a SRECS	69

Table A.1 – Severity (Se) classification.....	74
Table A.2– Frequency and duration of exposure (Fr) classification	74
Table A.3– Probability (Pr) classification.....	75
Table A.4– Probability of avoiding or limiting harm (Av) classification	76
Table A.5– Parameters used to determine class of probability of harm (Cl).....	76
Table A.6 – SIL assignment matrix.....	76
Table D.1 – Examples of the failure mode ratios for electrical/electronic components	95
Table E.1 – EM phenomenon and increased immunity levels for SRECS	100
Table E.2 – Selected frequencies for RF field tests.....	101
Table E.3 – Selected frequencies for conducted RF tests	101
Table F.1 – Criteria for estimation of CCF.....	102
Table F.2 – Estimation of CCF factor (β).....	103

Withdrawal

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

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

FDIS	Report on voting
44/460/FDIS	44/470/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.

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.

The contents of the corrigenda of July 2005 and April 2008 have been included in this copy.

Withdrawn

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 risks 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 the 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.