

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Safety of machinery – Functional safety of safety-related control systems

Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2021 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 l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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

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

IEC Customer Service Centre - 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: sales@iec.ch.

IEC online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) 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 IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC 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.

IEC Just Published - webstore.iec.ch/justpublished

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

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Safety of machinery – Functional safety of safety-related control systems

Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-9333-1

**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.....	8
INTRODUCTION.....	10
1 Scope.....	11
2 Normative references	12
3 Terms, definitions and abbreviations	13
3.1 Alphabetical list of definitions.....	13
3.2 Terms and definitions.....	15
3.3 Abbreviations.....	28
4 Design process of an SCS and management of functional safety.....	28
4.1 Objective	28
4.2 Design process	29
4.3 Management of functional safety using a functional safety plan	31
4.4 Configuration management	33
4.5 Modification	33
5 Specification of a safety function	34
5.1 Objective	34
5.2 Safety requirements specification (SRS).....	34
5.2.1 General	34
5.2.2 Information to be available.....	34
5.2.3 Functional requirements specification	35
5.2.4 Estimation of demand mode of operation	35
5.2.5 Safety integrity requirements specification.....	36
6 Design of an SCS	37
6.1 General.....	37
6.2 Subsystem architecture based on top down decomposition	37
6.3 Basic methodology – Use of subsystem	37
6.3.1 General	37
6.3.2 SCS decomposition	38
6.3.3 Sub-function allocation	39
6.3.4 Use of a pre-designed subsystem.....	39
6.4 Determination of safety integrity of the SCS.....	40
6.4.1 General	40
6.4.2 PFH.....	40
6.5 Requirements for systematic safety integrity of the SCS	41
6.5.1 Requirements for the avoidance of systematic hardware failures	41
6.5.2 Requirements for the control of systematic faults.....	42
6.6 Electromagnetic immunity	43
6.7 Software based manual parameterization.....	43
6.7.1 General	43
6.7.2 Influences on safety-related parameters	43
6.7.3 Requirements for software based manual parameterization	44
6.7.4 Verification of the parameterization tool.....	45
6.7.5 Performance of software based manual parameterization	45
6.8 Security aspects	45
6.9 Aspects of periodic testing	46
7 Design and development of a subsystem.....	46

7.1	General.....	46
7.2	Subsystem architecture design	47
7.3	Requirements for the selection and design of subsystem and subsystem elements	48
7.3.1	General	48
7.3.2	Systematic integrity	48
7.3.3	Fault consideration and fault exclusion	51
7.3.4	Failure rate of subsystem element	52
7.4	Architectural constraints of a subsystem	55
7.4.1	General	55
7.4.2	Estimation of safe failure fraction (<i>SFF</i>)	56
7.4.3	Behaviour (of the SCS) on detection of a fault in a subsystem	57
7.4.4	Realization of diagnostic functions	58
7.5	Subsystem design architectures.....	59
7.5.1	General	59
7.5.2	Basic subsystem architectures.....	59
7.5.3	Basic requirements	61
7.6	<i>PFH</i> of subsystems	62
7.6.1	General	62
7.6.2	Methods to estimate the <i>PFH</i> of a subsystem	62
7.6.3	Simplified approach to estimation of contribution of common cause failure (<i>CCF</i>).....	62
8	Software.....	62
8.1	General.....	62
8.2	Definition of software levels	63
8.3	Software – Level 1	64
8.3.1	Software safety lifecycle – SW level 1	64
8.3.2	Software design – SW level 1	65
8.3.3	Module design – SW level 1.....	67
8.3.4	Coding – SW level 1	67
8.3.5	Module test – SW level 1	68
8.3.6	Software testing – SW level 1	68
8.3.7	Documentation – SW level 1.....	69
8.3.8	Configuration and modification management process – SW level 1.....	69
8.4	Software level 2	70
8.4.1	Software safety lifecycle – SW level 2	70
8.4.2	Software design – SW level 2	71
8.4.3	Software system design – SW level 2	73
8.4.4	Module design – SW level 2.....	73
8.4.5	Coding – SW level 2	74
8.4.6	Module test – SW level 2	75
8.4.7	Software integration testing SW level 2.....	75
8.4.8	Software testing SW level 2.....	75
8.4.9	Documentation – SW level 2.....	76
8.4.10	Configuration and modification management process – SW level 2.....	77
9	Validation	77
9.1	Validation principles.....	77
9.1.1	Validation plan.....	80
9.1.2	Use of generic fault lists	80

9.1.3	Specific fault lists	80
9.1.4	Information for validation	81
9.1.5	Validation record	81
9.2	Analysis as part of validation	82
9.2.1	General	82
9.2.2	Analysis techniques	82
9.2.3	Verification of safety requirements specification (SRS)	82
9.3	Testing as part of validation	83
9.3.1	General	83
9.3.2	Measurement accuracy	83
9.3.3	More stringent requirements	84
9.3.4	Test samples	84
9.4	Validation of the safety function	84
9.4.1	General	84
9.4.2	Analysis and testing	85
9.5	Validation of the safety integrity of the SCS	85
9.5.1	General	85
9.5.2	Validation of subsystem(s)	85
9.5.3	Validation of measures against systematic failures	86
9.5.4	Validation of safety-related software	86
9.5.5	Validation of combination of subsystems	87
10	Documentation	87
10.1	General	87
10.2	Technical documentation	87
10.3	Information for use of the SCS	89
10.3.1	General	89
10.3.2	Information for use given by the manufacturer of subsystems	89
10.3.3	Information for use given by the SCS integrator	90
Annex A (informative)	Determination of required safety integrity	92
A.1	General	92
A.2	Matrix assignment for the required SIL	92
A.2.1	Hazard identification/indication	92
A.2.2	Risk estimation	92
A.2.3	Severity (Se)	93
A.2.4	Probability of occurrence of harm	93
A.2.5	Class of probability of harm (Cl)	96
A.2.6	SIL assignment	96
A.3	Overlapping hazards	98
Annex B (informative)	Example of SCS design methodology	99
B.1	General	99
B.2	Safety requirements specification	99
B.3	Decomposition of the safety function	99
B.4	Design of the SCS by using subsystems	100
B.4.1	General	100
B.4.2	Subsystem 1 design – “guard door monitoring”	100
B.4.3	Subsystem 2 design – “evaluation logic”	102
B.4.4	Subsystem 3 design – “motor control”	103
B.4.5	Evaluation of the SCS	103
B.4.6	PFH	104

B.5	Verification.....	104
B.5.1	General	104
B.5.2	Analysis.....	104
B.5.3	Tests	105
Annex C (informative)	Examples of $MTTF_D$ values for single components	106
C.1	General.....	106
C.2	Good engineering practices method	106
C.3	Hydraulic components.....	106
C.4	$MTTF_D$ of pneumatic, mechanical and electromechanical components	107
Annex D (informative)	Examples for diagnostic coverage (DC).....	109
Annex E (informative)	Methodology for the estimation of susceptibility to common cause failures (CCF).....	111
E.1	General.....	111
E.2	Methodology	111
E.2.1	Requirements for CCF	111
E.2.2	Estimation of effect of CCF	111
Annex F (informative)	Guideline for software level 1	114
F.1	Software safety requirements.....	114
F.2	Coding guidelines	115
F.3	Specification of safety functions.....	116
F.4	Specification of hardware design	117
F.5	Software system design specification.....	119
F.6	Protocols	121
Annex G (informative)	Examples of safety functions.....	124
Annex H (informative)	Simplified approaches to evaluate the PFH value of a subsystem	125
H.1	Table allocation approach	125
H.2	Simplified formulas for the estimation of PFH	127
H.2.1	General	127
H.2.2	Basic subsystem architecture A: single channel without a diagnostic function	127
H.2.3	Basic subsystem architecture B: dual channel without a diagnostic function	128
H.2.4	Basic subsystem architecture C: single channel with a diagnostic function	128
H.2.5	Basic subsystem architecture D: dual channel with a diagnostic function(s).....	133
H.3	Parts count method.....	134
Annex I (informative)	The functional safety plan and design activities	135
I.1	General.....	135
I.2	Example of a machine design plan including a safety plan	135
I.3	Example of activities, documents and roles.....	135
Annex J (informative)	Independence for reviews and testing/verification/validation activities	138
J.1	Software design	138
J.2	Validation.....	138
Bibliography	140
Figure 1 – Scope of this document	12

Figure 2 – Integration within the risk reduction process of ISO 12100 (extract)	29
Figure 3 – Iterative process for design of the safety-related control system	30
Figure 4 – Example of a combination of subsystems as one SCS.....	31
Figure 5 – By activating a low demand safety function at least once per year it can be assumed to be high demand	36
Figure 6 – Examples of typical decomposition of a safety function into sub-functions and its allocation to subsystems	39
Figure 7 – Example of safety integrity of a safety function based on allocated subsystems as one SCS	40
Figure 8 – Subsystem A logical representation	60
Figure 9 – Subsystem B logical representation	60
Figure 10 – Subsystem C logical representation	60
Figure 11 – Subsystem D logical representation	61
Figure 12 – V-model for SW level 1.....	64
Figure 13 – V-model for software modules customized by the designer for SW level 1.....	64
Figure 14 – V-model of software safety lifecycle for SW level 2.....	70
Figure 15 – Overview of the validation process	79
Figure A.1 – Parameters used in risk estimation	92
Figure A.2 – Example proforma for SIL assignment process	98
Figure B.1 – Decomposition of the safety function.....	100
Figure B.2 – Overview of design of the subsystems of the SCS	100
Figure F.1 – Plant sketch	116
Figure F.2 – Principal module architecture design.....	119
Figure F.3 – Principal design approach of logical evaluation	120
Figure F.4 – Example of logical representation (program sketch)	121
Figure H.1 – Subsystem A logical representation	127
Figure H.2 – Subsystem B logical representation	128
Figure H.3 – Subsystem C logical representation.....	128
Figure H.4 – Correlation of subsystem C and the pertinent fault handling function	129
Figure H.5 – Subsystem C with external fault handling function	129
Figure H.6 – Subsystem C with external fault diagnostics	131
Figure H.7 – Subsystem C with external fault reaction	131
Figure H.8 – Subsystem C with internal fault diagnostics and internal fault reaction.....	131
Figure H.9 – Subsystem D logical representation.....	133
Figure I.1 – Example of a machine design plan including a safety plan	135
Figure I.2 – Example of activities, documents and roles	136
Table 1 – Terms used in IEC 62061	13
Table 2 – Abbreviations used in IEC 62061.....	28
Table 3 – SIL and limits of <i>PFH</i> values.....	36
Table 4 – Required SIL and <i>PFH</i> of pre-designed subsystem	40
Table 5 – Relevant information for each subsystem	47
Table 6 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem	56

Table 7 – Overview of basic requirements and interrelation to basic subsystem architectures	61
Table 8 – Different levels of application software	63
Table 9 – Documentation of an SCS	88
Table A.1 – Severity (Se) classification	93
Table A.2 – Frequency and duration of exposure (Fr) classification	94
Table A.3 – Probability (Pr) classification	95
Table A.4 – Probability of avoiding or limiting harm (Av) classification	96
Table A.5 – Parameters used to determine class of probability of harm (Cl)	96
Table A.6 – Matrix assignment for determining the required SIL (or PL _r) for a safety function	97
Table B.1 – Safety requirements specification – example of overview	99
Table B.2 – Systematic integrity – example of overview	104
Table B.3 – Verification by tests	105
Table C.1 – Standards references and $MTTF_D$ or B_{10D} values for components	107
Table D.1 – Estimates for diagnostic coverage (DC)	109
Table E.1 – Criteria for estimation of CCF	112
Table E.2 – Criteria for estimation of CCF	113
Table F.1 – Example of relevant documents related to the simplified V-model	114
Table F.2 – Examples of coding guidelines	115
Table F.3 – Specified safety functions	117
Table F.4 – Relevant list of input and output signals	118
Table F.5 – Example of simplified cause and effect matrix	121
Table F.6 – Verification of software system design specification	122
Table F.7 – Software code review	122
Table F.8 – Software validation	123
Table G.1 – Examples of typical safety functions	124
Table H.1 – Allocation of PFH value of a subsystem	126
Table H.2 – Relationship between B_{10D} , operations and $MTTF_D$	127
Table H.3 – Minimum value of $1/\lambda_D F_H$ for the applicability of PFH equation (H.4)	132
Table J.1 – Minimum levels of independence for review, testing and verification activities	138
Table J.2 – Minimum levels of independence for validation activities	138

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SAFETY OF MACHINERY –
FUNCTIONAL SAFETY OF SAFETY-RELATED 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, 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.

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

This second edition cancels and replaces the first edition, published in 2005, Amendment 1:2012 and Amendment 2:2015. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- structure has been changed and contents have been updated to reflect the design process of the safety function,
- standard extended to non-electrical technologies,
- definitions updated to be aligned with IEC 61508-4,
- functional safety plan introduced and configuration management updated (Clause 4),
- requirements on parametrization expanded (Clause 6),
- reference to requirements on security added (Subclause 6.8),
- requirements on periodic testing added (Subclause 6.9),

- various improvements and clarification on architectures and reliability calculations (Clause 6 and Clause 7),
- shift from "SILCL" to "maximum SIL" of a subsystem (Clause 7),
- use cases for software described including requirements (Clause 8),
- requirements on independence for software verification (Clause 8) and validation activities (Clause 9) added,
- new informative annex with examples (Annex G),
- new informative annexes on typical $MTTF_D$ values, diagnostics and calculation methods for the architectures (Annex C, Annex D and Annex H).

The text of this International Standard is based on the following documents:

Draft	Report on voting
44/885/FDIS	44/888/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this publication 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 document using a colour printer.

INTRODUCTION

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

IEC 62061 specifies requirements for the design and implementation of safety-related control systems of machinery. This document is machine sector specific within the framework of IEC 61508.

NOTE While IEC 62061 and ISO 13849-1 are using different methodologies for the design of safety related control systems, they intend to achieve the same risk reduction.

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 an SCS. It sets out an approach and provides requirements to achieve the necessary performance and facilitates the specification of the safety functions intended to achieve the risk reduction.

This document provides a machine sector specific framework for functional safety of an SCS 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 SCS of machines that can also be relevant to later phases of the lifecycle of an SCS.

There are many situations on machines where SCS 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 safety related parts of the machine control system to stop hazardous machine operation. In automation, the machine 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 document gives a methodology and requirements to:

- assign the required safety integrity for each safety function to be implemented by SCS;
- enable the design of the SCS appropriate to the assigned safety (control) function(s);
- integrate safety-related subsystems designed in accordance with other applicable functional safety-related standards (see 6.3.4);
- validate the SCS.

This document is intended to be used within the framework of systematic risk reduction, in conjunction with risk assessment described in ISO 12100. Suggested methodologies for a safety integrity assignment are given in informative Annex A.

SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

1 Scope

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

This document is a machinery sector specific standard within the framework of IEC 61508 (all parts).

The design of complex programmable electronic subsystems or subsystem elements is not within the scope of this document. This is in the scope of IEC 61508 or standards linked to it; see Figure 1.

NOTE 1 Elements such as systems on chip or microcontroller boards are considered complex programmable electronic subsystems.

The main body of this sector standard specifies general requirements for the design, and verification of a safety-related control system intended to be used in high/continuous demand mode.

This document:

- is concerned only with functional safety requirements intended to reduce the risk of hazardous situations;
- 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 2 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, additional information is available in IEC 61511.

This document does not cover

- electrical hazards arising from the electrical control equipment itself (e.g. electric shock – see IEC 60204-1);
- other safety requirements necessary at the machine level such as safeguarding;
- specific measures for security aspects – see IEC TR 63074.

This document is not intended to limit or inhibit technological advancement.

Figure 1 illustrates the scope of this document.