



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 (CI)	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.

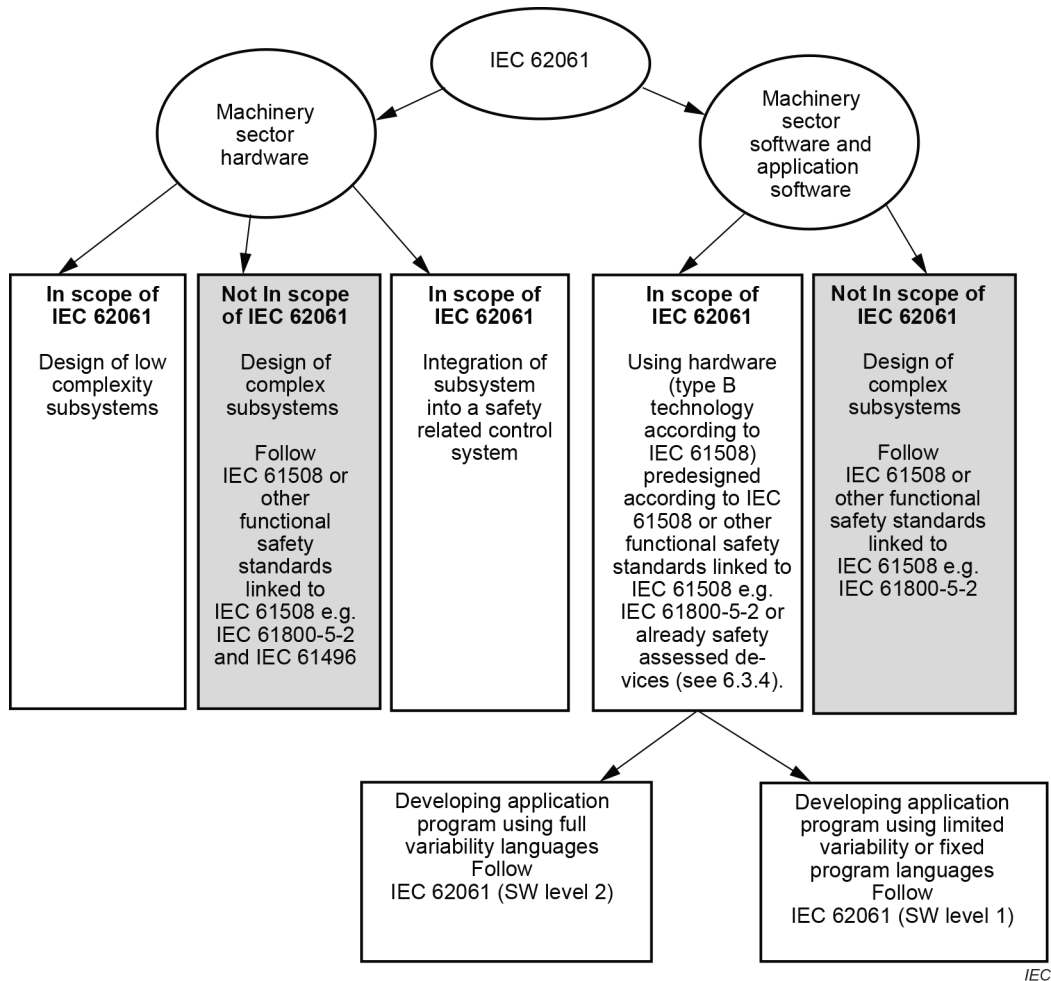


Figure 1 – Scope of this document

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60204-1:2016, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-1-2:2016, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

ISO 12100:2010, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

SOMMAIRE

AVANT-PROPOS	151
INTRODUCTION.....	153
1 Domaine d'application	154
2 Références normatives	155
3 Termes, définitions et abréviations	156
3.1 Liste alphabétique des définitions	156
3.2 Termes et définitions	157
3.3 Abréviations.....	172
4 Processus de conception d'un SCS et gestion de la sécurité fonctionnelle.....	173
4.1 Objectifs	173
4.2 Processus de conception	173
4.3 Gestion de la sécurité fonctionnelle à l'aide d'un plan de sécurité fonctionnelle	175
4.4 Gestion de configuration	177
4.5 Modification	177
5 Spécification d'une fonction de sécurité	178
5.1 Objectifs	178
5.2 Spécification des exigences de sécurité (SRS)	178
5.2.1 Généralités	178
5.2.2 Informations à mettre à disposition	178
5.2.3 Spécification des exigences fonctionnelles	179
5.2.4 Estimation du mode de fonctionnement à sollicitation	180
5.2.5 Spécification des exigences d'intégrité de sécurité	180
6 Conception d'un SCS.....	181
6.1 Généralités	181
6.2 Architecture de sous-système en fonction de la décomposition descendante	181
6.3 Méthodologie de base – Utilisation du sous-système	181
6.3.1 Généralités.....	181
6.3.2 Décomposition du SCS	182
6.3.3 Attribution de sous-fonction	184
6.3.4 Utilisation d'un sous-système type	184
6.4 Détermination de l'intégrité de sécurité du SCS	184
6.4.1 Généralités	184
6.4.2 PFH.....	185
6.5 Exigences pour l'intégrité de sécurité systématique du SCS	185
6.5.1 Exigences pour l'évitement des défaillances systématiques du matériel.....	185
6.5.2 Exigences pour la maîtrise des anomalies systématiques	186
6.6 Immunité électromagnétique	187
6.7 Paramétrisation manuelle liée au logiciel	188
6.7.1 Généralités	188
6.7.2 Influences sur les paramètres relatifs à la sécurité	188
6.7.3 Exigences relatives à la paramétrisation manuelle liée au logiciel.....	189
6.7.4 Vérification de l'outil de paramétrisation	190
6.7.5 Performances de la paramétrisation manuelle liée au logiciel	190
6.8 Aspects liés à la sécurité	191
6.9 Aspects des essais périodiques	191

7	Conception et développement d'un sous-système	192
7.1	Généralités	192
7.2	Conception de l'architecture d'un sous-système	193
7.3	Exigences pour le choix et la conception du sous-système et des éléments de sous-système	194
7.3.1	Généralités	194
7.3.2	Intégrité systématique	194
7.3.3	Prise en considération et exclusion des anomalies	197
7.3.4	Taux de défaillance de l'élément de sous-système	199
7.4	Contraintes architecturales d'un sous-système	203
7.4.1	Généralités	203
7.4.2	Estimation de la proportion de défaillances en sécurité (<i>SFF</i>)	204
7.4.3	Comportement (du SCS) lors de la détection d'une anomalie dans un sous-système	205
7.4.4	Réalisation des fonctions de diagnostic	206
7.5	Architectures de conception du sous-système	207
7.5.1	Généralités	207
7.5.2	Architectures de sous-système simple	208
7.5.3	Exigences de base	209
7.6	Fréquence moyenne de défaillance dangereuse par heure (<i>PFH</i>) des sous-systèmes	210
7.6.1	Généralités	210
7.6.2	Méthodes d'estimation de la <i>PFH</i> d'un sous-système	210
7.6.3	Approche simplifiée pour l'estimation de la contribution des défaillances de cause commune (<i>CCF</i>)	211
8	Logiciels	211
8.1	Généralités	211
8.2	Définition des niveaux logiciels	211
8.3	Niveau logiciel 1	213
8.3.1	Cycle de vie de sécurité du logiciel – Niveau logiciel 1	213
8.3.2	Conception du logiciel – Niveau logiciel 1	214
8.3.3	Conception du module – Niveau logiciel 1	216
8.3.4	Codage – Niveau logiciel 1	217
8.3.5	Essai du module – Niveau logiciel 1	217
8.3.6	Essai du logiciel – Niveau logiciel 1	218
8.3.7	Documentation – Niveau logiciel 1	218
8.3.8	Processus de gestion de la configuration et des modifications – Niveau logiciel 1	219
8.4	Niveau logiciel 2	219
8.4.1	Cycle de vie de sécurité du logiciel – Niveau logiciel 2	219
8.4.2	Conception du logiciel – Niveau logiciel 2	221
8.4.3	Conception du système logiciel – Niveau logiciel 2	223
8.4.4	Conception du module – Niveau logiciel 2	224
8.4.5	Codage – Niveau logiciel 2	224
8.4.6	Essai du module – Niveau logiciel 2	225
8.4.7	Essai d'intégration du logiciel – Niveau logiciel 2	225
8.4.8	Essai du logiciel – Niveau logiciel 2	225
8.4.9	Documentation – Niveau logiciel 2	227
8.4.10	Processus de gestion de la configuration et des modifications – Niveau logiciel 2	227

9	Validation	228
9.1	Principes de validation	228
9.1.1	Plan de validation	230
9.1.2	Utilisation des listes d'anomalies génériques	230
9.1.3	Listes d'anomalies spécifiques.....	230
9.1.4	Informations pour la validation	231
9.1.5	Consignation de la validation	231
9.2	Analyse dans le cadre de la validation	232
9.2.1	Généralités	232
9.2.2	Techniques d'analyse	232
9.2.3	Vérification de la spécification des exigences de sécurité (SRS).....	232
9.3	Essais dans le cadre de la validation	233
9.3.1	Généralités	233
9.3.2	Exactitude de mesure	233
9.3.3	Exigences plus strictes	234
9.3.4	Échantillons d'essai	234
9.4	Validation de la fonction de sécurité.....	234
9.4.1	Généralités	234
9.4.2	Analyses et essais	235
9.5	Validation de l'intégrité de sécurité du SCS.....	235
9.5.1	Généralités	235
9.5.2	Validation du ou des sous-systèmes	236
9.5.3	Validation des mesures contre les défaillances systématiques.....	236
9.5.4	Validation du logiciel relatif à la sécurité	236
9.5.5	Validation de la combinaison de sous-systèmes	237
10	Documentation	238
10.1	Généralités	238
10.2	Documentation technique.....	238
10.3	Informations pour l'utilisation du SCS.....	239
10.3.1	Généralités	239
10.3.2	Informations relatives à l'utilisation données par le fabricant de sous-systèmes	240
10.3.3	Informations relatives à l'utilisation données par l'intégrateur du SCS.....	241
Annexe A (informative)	Détermination de l'intégrité de sécurité exigée	242
A.1	Généralités	242
A.2	Attribution de matrice pour le niveau de SIL exigé	242
A.2.1	Signalisation/Identification d'un phénomène dangereux	242
A.2.2	Estimation du risque	242
A.2.3	Sévérité (Se)	243
A.2.4	Probabilité d'apparition d'un dommage	244
A.2.5	Classe de probabilité d'un dommage (CI)	247
A.2.6	Attribution du niveau de SIL.....	247
A.3	Chevauchement de phénomènes dangereux.....	249
Annexe B (informative)	Exemple de méthodologie de conception de SCS.....	250
B.1	Généralités	250
B.2	Spécification des exigences de sécurité.....	250
B.3	Décomposition de la fonction de sécurité	251
B.4	Conception du SCS à l'aide de sous-systèmes.....	251
B.4.1	Généralités	251

B.4.2	Conception du sous-système 1 – "surveillance de la porte de protection"	252
B.4.3	Conception du sous-système 2 – "logique d'évaluation"	254
B.4.4	Conception du sous-système 3 – "commande de moteur"	254
B.4.5	Évaluation du SCS.....	255
B.4.6	PFH.....	255
B.5	Vérification.....	256
B.5.1	Généralités	256
B.5.2	Analyse	256
B.5.3	Essais	256
Annexe C (informative)	Exemples de valeurs $MTTF_D$ pour des composants simples	257
C.1	Généralités	257
C.2	Méthode reposant sur le respect des règles de l'art	257
C.3	Composants hydrauliques	257
C.4	$MTTF_D$ des composants pneumatiques, mécaniques et électromécaniques	258
Annexe D (informative)	Exemples de couverture du diagnostic (DC)	260
Annexe E (informative)	Méthodologie pour l'estimation de la sensibilité aux défaillances de cause commune (CCF).....	263
E.1	Généralités	263
E.2	Méthodologie	263
E.2.1	Exigences pour la CCF	263
E.2.2	Estimation des effets de la CCF.....	263
Annexe F (informative)	Lignes directrices relatives au niveau logiciel 1	266
F.1	Exigences de sécurité du logiciel	266
F.2	Lignes directrices en matière de codage.....	267
F.3	Spécification des fonctions de sécurité	269
F.4	Spécification de la conception du matériel	271
F.5	Spécification de conception du système logiciel.....	272
F.6	Protocoles	276
Annexe G (informative)	Exemples de fonctions de sécurité	278
Annexe H (informative)	Approches simplifiées pour évaluer la valeur PFH d'un sous-système.....	279
H.1	Approche du tableau d'allocation	279
H.2	Formules simplifiées pour l'estimation de PFH	282
H.2.1	Généralités.....	282
H.2.2	Architecture A d'un sous-système simple: simple canal sans fonction de diagnostic.....	282
H.2.3	Architecture B d'un sous-système simple: double canal sans fonction de diagnostic.....	283
H.2.4	Architecture C d'un sous-système simple: simple canal avec fonction de diagnostic.....	283
H.2.5	Architecture D d'un sous-système simple: double canal avec fonction(s) de diagnostic.....	289
H.3	Méthode de comptage des parties	290
Annexe I (informative)	Plan de sécurité fonctionnelle et activités de conception.....	291
I.1	Généralités	291
I.2	Exemple de plan de conception d'une machine incluant un plan de sécurité	291
I.3	Exemple d'activités, de documents et de rôles	291

Annexe J (informative) Indépendance pour les activités d'examen et d'essai/de vérification/de validation	294
J.1 Conception de logiciels	294
J.2 Validation.....	294
Bibliographie.....	296
Figure 1 – Domaine d'application du présent document	155
Figure 2 – Intégration dans le processus de réduction du risque de l'ISO 12100 (extrait).....	173
Figure 3 – Processus itératif de conception du système de commande relatif à la sécurité.....	174
Figure 4 – Exemple de combinaison de sous-systèmes en un SCS.....	175
Figure 5 – Définition possible par hypothèse d'un mode à forte sollicitation par l'activation d'une fonction de sécurité à faible sollicitation au moins une fois par an.....	180
Figure 6 – Exemples de décomposition classique d'une fonction de sécurité en sous-fonctions et de son attribution aux sous-systèmes	183
Figure 7 – Exemple d'intégrité de sécurité d'une fonction de sécurité reposant sur des sous-systèmes attribués en tant que SCS unique	185
Figure 8 – Représentation logique d'un sous-système de type A.....	208
Figure 9 – Représentation logique d'un sous-système de type B.....	208
Figure 10 – Représentation logique d'un sous-système de type C.....	208
Figure 11 – Représentation logique d'un sous-système de type D.....	209
Figure 12 – Modèle en V pour le niveau logiciel 1	213
Figure 13 – Modèle en V pour les modules logiciels personnalisés par le concepteur pour le niveau logiciel 1	214
Figure 14 – Modèle en V du cycle de vie de sécurité du logiciel pour le niveau logiciel 2	220
Figure 15 – Aperçu du processus de validation	229
Figure A.1 – Paramètres utilisés dans l'estimation du risque.....	242
Figure A.2 – Exemple de pro forma pour procédé d'attribution de SIL	249
Figure B.1 – Décomposition de la fonction de sécurité	251
Figure B.2 – Présentation de la conception des sous-systèmes du SCS	251
Figure F.1 – Croquis de l'usine	269
Figure F.2 – Conception de l'architecture modulaire principale.....	273
Figure F.3 – Approche de conception principale de l'évaluation logique	274
Figure F.4 – Exemple de représentation logique (croquis du programme)	275
Figure H.1 – Représentation logique d'un sous-système de type A	282
Figure H.2 – Représentation logique d'un sous-système de type B	283
Figure H.3 – Représentation logique d'un sous-système de type C	283
Figure H.4 – Corrélation entre le sous-système de type C et la fonction de traitement des anomalies correspondante	284
Figure H.5 – Sous-système de type C avec fonction externe de traitement des anomalies	285
Figure H.6 – Sous-système de type C avec diagnostics externes des anomalies	286
Figure H.7 – Sous-système de type C avec réaction externe à l'anomalie	286
Figure H.8 – Sous-système de type C avec diagnostics internes des anomalies et réaction interne à l'anomalie	287

Figure H.9 – Représentation logique d'un sous-système de type D	289
Figure I.1 – Exemple de plan de conception d'une machine incluant un plan de sécurité.....	291
Figure I.2 – Exemple d'activités, de documents et de rôles (1 sur 2)	292
Tableau 1 – Termes utilisés dans l'IEC 62061.....	156
Tableau 2 – Abréviations utilisées dans l'IEC 62061	172
Tableau 3 – SIL et limites des valeurs de <i>PFH</i>	181
Tableau 4 – SIL exigé et <i>PFH</i> du sous-système type.....	184
Tableau 5 – Informations pertinentes pour chaque sous-système	193
Tableau 6 – Contraintes architecturales sur un sous-système: SIL maximal pouvant être revendiqué pour un SCS utilisant ce sous-système.....	204
Tableau 7 – Aperçu des exigences de base et de l'interrelation avec les architectures de sous-système simple.....	210
Tableau 8 – Différents niveaux de logiciels d'application.....	212
Tableau 9 – Documentation d'un SCS.....	239
Tableau A.1 – Classification de la sévérité (Se)	243
Tableau A.2 – Classification de la fréquence et durée de l'exposition (Fr).....	244
Tableau A.3 – Classification de la probabilité (Pr).....	246
Tableau A.4 – Classification de la probabilité d'évitement ou de limitation d'un dommage (Av)	246
Tableau A.5 – Paramètres utilisés pour déterminer la classe de probabilité d'un dommage (CI).....	247
Tableau A.6 – Attribution de matrice pour déterminer le niveau de SIL exigé (ou PL_r) pour une fonction de sécurité.....	248
Tableau B.1 – Spécification des exigences de sécurité – exemple de présentation	250
Tableau B.2 – Intégrité systématique – exemple de présentation	255
Tableau B.3 – Vérification par des essais	256
Tableau C.1 – Normes de référence et valeurs $MTTF_D$ ou B_{10D} des composants.....	258
Tableau D.1 – Estimations de la couverture du diagnostic (<i>DC</i>)(1 sur 2)	261
Tableau E.1 – Critères d'estimation des CCF.....	264
Tableau E.2 – Critères d'estimation des CCF.....	265
Tableau F.1 – Exemple de documents pertinents relatifs au modèle en V simplifié	266
Tableau F.2 – Exemples de lignes directrices en matière de codage.....	268
Tableau F.3 – Fonctions de sécurité spécifiées.....	270
Tableau F.4 – Liste des signaux d'entrée et de sortie	272
Tableau F.5 – Exemple de matrice de cause et effet simplifiée	275
Tableau F.6 – Vérification de la spécification de conception du système logiciel.....	276
Tableau F.7 – Revue de code du logiciel	276
Tableau F.8 – Validation du logiciel	277
Tableau G.1 – Exemples de fonctions de sécurité classiques.....	278
Tableau H.1 – Allocation de la valeur <i>PFH</i> d'un sous-système	280
Tableau H.2 – Relations entre B_{10D} , les opérations et $MTTF_D$	281
Tableau H.3 – Valeur minimale de $1/\lambda_{D FH}$ pour l'applicabilité de l'équation <i>PFH</i> (H.4)	287

Tableau J.1 – Niveaux minimaux d'indépendance pour les activités d'examen, d'essai et de vérification	294
Tableau J.2 – Niveaux minimaux d'indépendance pour les activités de validation	295

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SÉCURITÉ DES MACHINES – SÉCURITÉ FONCTIONNELLE DES SYSTÈMES DE COMMANDE RELATIFS À LA SÉCURITÉ

AVANT-PROPOS

- 1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

L'IEC 62061 a été établie par le comité d'études 44 de l'IEC: Sécurité des machines – Aspects électrotechniques. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2005, l'Amendement 1:2012 ainsi que l'Amendement 2:2015. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- la structure a été modifiée et le contenu a été mis à jour pour refléter le processus de conception de la fonction de sécurité,
- la norme a été étendue aux technologies non électriques,
- définitions mises à jour pour être alignées sur l'IEC 61508-4,

- plan de sécurité fonctionnelle introduit et gestion de configuration mise à jour (Article 4),
- exigences relatives au paramétrage étendues (Article 6),
- référence aux exigences relatives à la sécurité ajoutée (Paragraphe 6.8)
- exigences relatives aux essais périodiques ajoutées (Paragraphe 6.9),
- différentes améliorations et clarifications relatives aux architectures et aux calculs de fiabilité (Article 6 et Article 7),
- décalage entre le "SILCL" et le "SIL maximal" d'un sous-système (Article 7),
- cas d'utilisation pour les logiciels décrits, y compris les exigences (Article 8),
- exigences relatives à l'indépendance des activités de vérification (Article 8) et de validation (Article 9) du logiciel ajoutées,
- nouvelle annexe informative avec des exemples (Annex G),
- nouvelles annexes informatives relatives aux valeurs $MTTF_D$, aux diagnostics et aux méthodes de calcul des architectures (Annex C, Annex D et Annex H).

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
44/885/FDIS	44/888/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer ce document en utilisant une imprimante couleur.

INTRODUCTION

Par suite de l'automatisation, ainsi que de la demande d'une production plus élevée avec une réduction des efforts physiques des opérateurs, les systèmes de commande relatifs à la sécurité (appelés SCS ci-après) des machines jouent un rôle croissant dans la réalisation de la sécurité d'ensemble des machines. De ce fait, les SCS eux-mêmes utilisent de plus en plus souvent une technologie électronique complexe.

L'IEC 62061 spécifie les exigences pour la conception et la réalisation des systèmes de commande des machines relatifs à la sécurité. Le présent document est spécifique au secteur des machines dans le cadre de l'IEC 61508.

NOTE Bien que l'IEC 62061 et l'ISO 13849-1 utilisent des méthodologies différentes en matière de conception des systèmes de commande relatifs à la sécurité, elles visent à réaliser le même objectif de réduction de risque.

La présente Norme internationale est destinée à être utilisée par les concepteurs de machines, les fabricants et les intégrateurs de systèmes de commande, et autres, impliqués dans la spécification, la conception et la validation d'un SCS. Elle présente une approche et donne les exigences nécessaires à la réalisation du fonctionnement requis et facilite la spécification des fonctions de sécurité destinées à réaliser la réduction de risque.

Le présent document donne un cadre spécifique au secteur des machines pour la sécurité fonctionnelle d'un SCS de machine. Il couvre uniquement les aspects du cycle de vie de sécurité relatifs à l'allocation des exigences de sécurité jusqu'à la validation de la sécurité. Des exigences sont données pour information pour une utilisation sûre des SCS de machines, lesquelles peuvent aussi être appropriées pour des phases ultérieures de la vie d'un SCS.

Il existe de nombreuses circonstances dans les machines où les SCS sont utilisés comme partie des mesures de sécurité développées pour réaliser la réduction de risque. Un exemple typique est l'utilisation d'un protecteur avec dispositif de verrouillage qui, lorsqu'il est ouvert pour permettre l'accès à la zone dangereuse, signale aux parties relatives à la sécurité du système de commande de la machine d'arrêter le fonctionnement dangereux de la machine. En automatisation, le système de commande de la machine utilisé pour réaliser le fonctionnement correct du processus machine contribue souvent à la sécurité en réduisant les risques associés aux phénomènes dangereux résultant directement de défaillances du système de commande. Le présent document donne une méthodologie et les exigences pour:

- assigner le niveau d'intégrité de sécurité exigé pour chaque fonction de sécurité devant être mise en œuvre par les SCS;
- permettre la conception des SCS appropriés à la ou aux fonctions de commande assignées relatives à la sécurité;
- intégrer les sous-systèmes relatifs à la sécurité conçus selon d'autres normes applicables relatives à la sécurité fonctionnelle (voir 6.3.4);
- valider les SCS.

Le présent document est destiné à être utilisé dans le cadre de la réduction systématique du risque, conjointement avec l'appréciation du risque décrite dans l'ISO 12100. Les méthodologies conseillées pour l'attribution d'intégrité de sécurité sont données dans l'Annex A informative.

SÉCURITÉ DES MACHINES – SÉCURITÉ FONCTIONNELLE DES SYSTÈMES DE COMMANDE RELATIFS À LA SÉCURITÉ

1 Domaine d'application

La présente Norme internationale spécifie les exigences et donne des recommandations pour la conception, l'intégration et la validation des systèmes de commande relatifs à la sécurité (SCS) pour les machines. Elle s'applique aux systèmes de commande utilisés, séparément ou en combinaison, pour assurer les fonctions de sécurité de machines qui ne sont pas portables à la main en fonctionnement, y compris un groupe de machines fonctionnant ensemble d'une manière coordonnée.

Le présent document est spécifique au secteur des machines dans le cadre de l'IEC 61508 (toutes les parties).

La conception de sous-systèmes ou d'éléments de sous-système électroniques programmables complexes ne relève pas du domaine d'application du présent document. Ces éléments relèvent du domaine d'application de l'IEC 61508 ou de normes qui lui sont associées (voir la Figure 1).

NOTE 1 Les éléments tels que les systèmes sur puce ou les cartes de microcontrôleur sont considérés comme des sous-systèmes électroniques programmables complexes.

Le corps principal de la présente norme sectorielle spécifie les exigences générales en matière de conception et de vérification d'un système de commande relatif à la sécurité destiné à être utilisé en mode à forte sollicitation/continu.

Le présent document:

- ne concerne que les exigences de sécurité fonctionnelle destinées à réduire le risque de situations dangereuses;
- se limite aux risques résultant directement des phénomènes dangereux de la machine elle-même ou d'un groupe de machines fonctionnant ensemble d'une manière coordonnée;

NOTE 2 Les exigences pour réduire les risques provenant d'autres phénomènes dangereux sont données dans les normes sectorielles appropriées. Par exemple, pour une ou plusieurs machines qui font partie d'une activité processus, des informations supplémentaires sont disponibles dans l'IEC 61511.

Le présent document ne concerne pas

- les phénomènes dangereux électriques provenant du matériel de commande électrique lui-même (par exemple choc électrique – voir l'IEC 60204-1);
- les autres exigences relatives à la sécurité nécessaires au niveau de la machine (la protection par protecteur, par exemple);
- les mesures particulières pour les aspects liés à la sécurité – voir l'IEC TR 63074.

Le présent document n'est pas destiné à limiter ou inhiber les progrès technologiques.

La Figure 1 donne une représentation du domaine d'application du présent document.

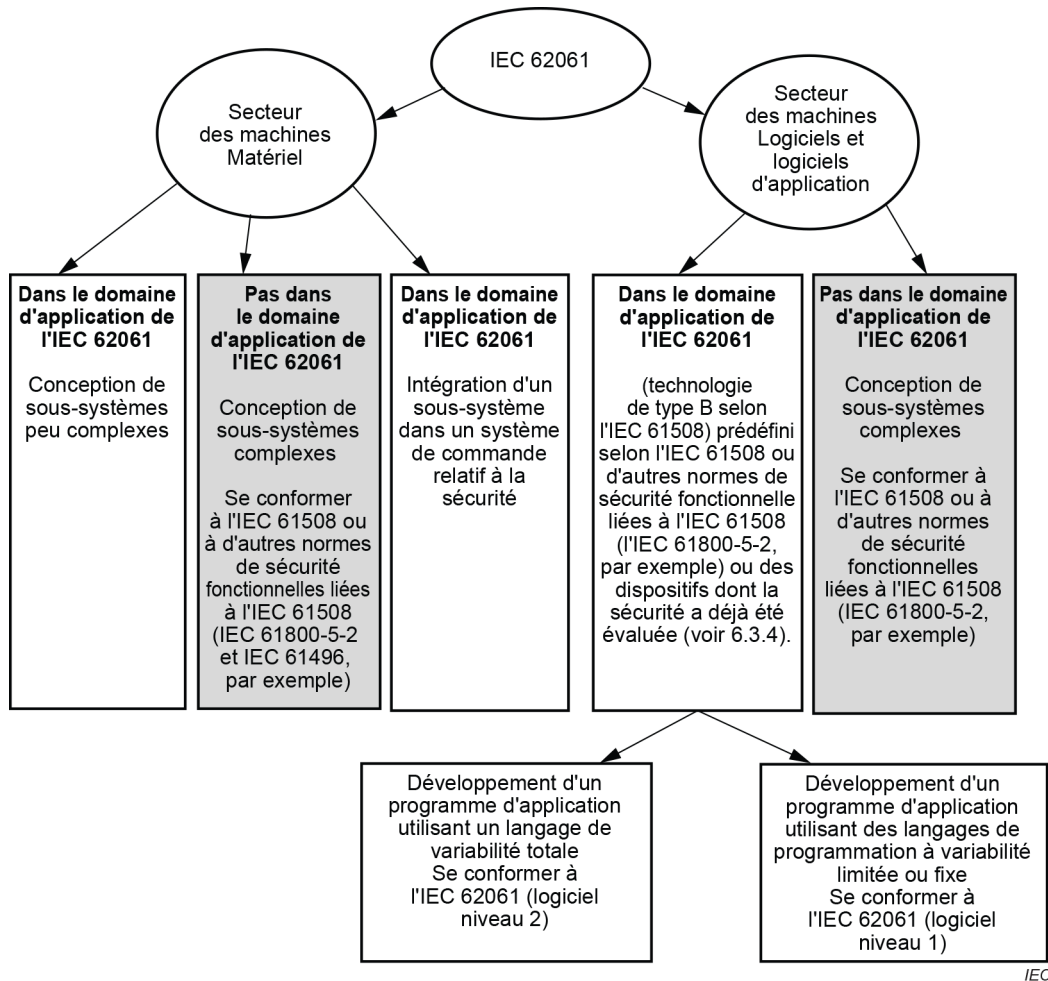


Figure 1 – Domaine d'application du présent document

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60204-1:2016, *Sécurité des machines – Équipement électrique des machines – Partie 1: Exigences générales*

IEC 61000-1-2:2016, *Compatibilité électromagnétique (CEM) – Partie 1-2: Généralités – Méthodologie pour la réalisation de la sécurité fonctionnelle des systèmes électriques et électroniques, y compris les équipements, du point de vue des phénomènes électromagnétiques*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

ISO 12100:2010, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*

ISO 13849 (toutes les parties), *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité*

ISO 13849-1:2015, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*