



IEC 62061

Edition 1.2 2015-06

CONSOLIDATED VERSION

VERSION CONSOLIDÉE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-2774-9

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.



REDLINE VERSION

VERSION REDLINE



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

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	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	22
4.1 Objective.....	22
4.2 Requirements.....	22
5 Requirements for the specification of Safety-Related Control Functions (SRCFs).....	23
5.1 Objective.....	23
5.2 Specification of requirements for SRCFs	24
6 Design and integration of the safety-related electrical control system (SRECS).....	26
6.1 Objective.....	26
6.2 General requirements.....	26
6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS.....	27
6.4 Requirements for systematic safety integrity of the SRECS	27
6.5 Selection of safety-related electrical control system	29
6.6 Safety-related electrical control system (SRECS) design and development	29
6.7 Realisation of subsystems.....	35
6.8 Realisation of diagnostic functions	50
6.9 Hardware implementation of the SRECS	52
6.10 Software safety requirements specification.....	52
6.11 Software design and development.....	53
6.12 Safety-related electrical control system integration and testing.....	59
6.13 SRECS installation	61
7 Information for use of the SRECS.....	61
7.1 Objective.....	61
7.2 Documentation for installation, use and maintenance	61
8 Validation of the safety-related electrical control system.....	62
8.1 Objective.....	62
8.2 General requirements.....	62
8.3 Validation of SRECS systematic safety integrity	62
9 Modification.....	63
9.1 Objective.....	63
9.2 Modification procedure	64
9.3 Configuration management procedures	64
10 Documentation	66

Annex A (informative) SIL assignment	68
Annex B (informative) Example of safety-related electrical control system (SRECS) design using concepts and requirements of Clauses 5 and 6	76
Annex C (informative) Guide to embedded software design and development.....	83
Annex D (informative) Failure modes of electrical/electronic components	83
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	98
Annex F (informative) Methodology for the estimation of susceptibility to common cause failures (CCF).....	98
Figure 1 – Relationship of IEC 62061 to other relevant standards	8
Figure 2 – Workflow of the SRECS design and development process	32
Figure 3 – Allocation of safety requirements of the function blocks to subsystems (see 6.6.2.1.1)	33
Figure 4 – Workflow for subsystem design and development (see box 6B of Figure 2)	38
Figure 5 – Decomposition of a function block into redundant function block elements and their associated subsystem elements	39
Figure 6 – Subsystem A logical representation	45
Figure 7 – Subsystem B logical representation	46
Figure 8 – Subsystem C logical representation	46
Figure 9 – Subsystem D logical representation	48
Figure A.1 – Workflow of SIL assignment process.....	69
Figure A.2 – Parameters used in risk estimation	70
Figure A.3 – Example proforma for SIL assignment process	75
Figure B.1 – Terminology used in functional decomposition	76
Figure B.2 – Example machine	77
Figure B.3 – Specification of requirements for an SRCF	77
Figure B.4 – Decomposition to a structure of function blocks	78
Figure B.5 – Initial concept of an architecture for a SRECS	79
Figure B.6 – SRECS architecture with diagnostic functions embedded within each subsystem (SS1 to SS4)	80
Figure B.7 – SRECS architecture with diagnostic functions embedded within subsystem SS3	81
Figure B.8 – Estimation of PFH_D for a SRECS.....	82
Table 1 – Recommended application of IEC 62061 and ISO 13849-1 (under revision)	11
Table 2 – Overview and objectives of IEC 62061	11
Table 3 – Safety integrity levels: target failure values for SRCFs	25
Table 4 – Characteristics of subsystems 1 and 2 used in this example (see Note above)	35
Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem	41
Table 6 – Architectural constraints: SILCL relating to categories	41
Table 7 – Probability of dangerous failure	41

Table 8 – Information and documentation of a SRECS	67
Table A.1 – Severity (Se) classification	70
Table A.2– Frequency and duration of exposure (Fr) classification	71
Table A.3– Probability (Pr) classification	72
Table A.4– Probability of avoiding or limiting harm (Av) classification	73
Table A.5– Parameters used to determine class of probability of harm (CI)	73
Table A.6 – SIL assignment matrix.....	74
Table D.1 – Examples of the failure mode ratios for electrical/electronic components	75
Table E.1 – EM phenomenon and increased immunity levels for SRECS	76
Table E.2 – Selected frequencies for RF field tests	77
Table E.3 – Selected frequencies for conducted RF tests	78
Table F.1 – Criteria for estimation of CCF	99
Table F.2 – Estimation of CCF factor (β)	100

IECNORM.COM : Click to view the full PDF of IEC 62061 Amd 1 & 2 CSV ed 12:2015

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, 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.

DISCLAIMER

This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 62061 bears the edition number 1.2. It consists of the first edition (2005-01) [documents 44/460/FDIS and 44/470/RVD], its amendment 1 (2012-11) [documents 44/655/CDV and 44/663/RVC], its amendment 2 (2015-06) [documents 44/718/CDV and 44/725/RVC], the corrigenda 1 (July 2005) and 2 (April 2008). The technical content is identical to the base edition and its amendments.

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendments 1 and 2. Additions and deletions are displayed in red, with deletions being struck through. A separate Final version with all changes accepted is available in this publication.

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

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

The committee has decided that the contents of the base publication and its amendments will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The contents of the corrigendum of August 2015 have been included in this copy.

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 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~~ 12100:2010) 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~~ 12100 and in conjunction with risk assessment according to the principles described in ISO ~~14121 (EN 1050)~~ 12100. A suggested methodology for safety integrity level (SIL) assignment is given in informative Annex A.

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

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

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

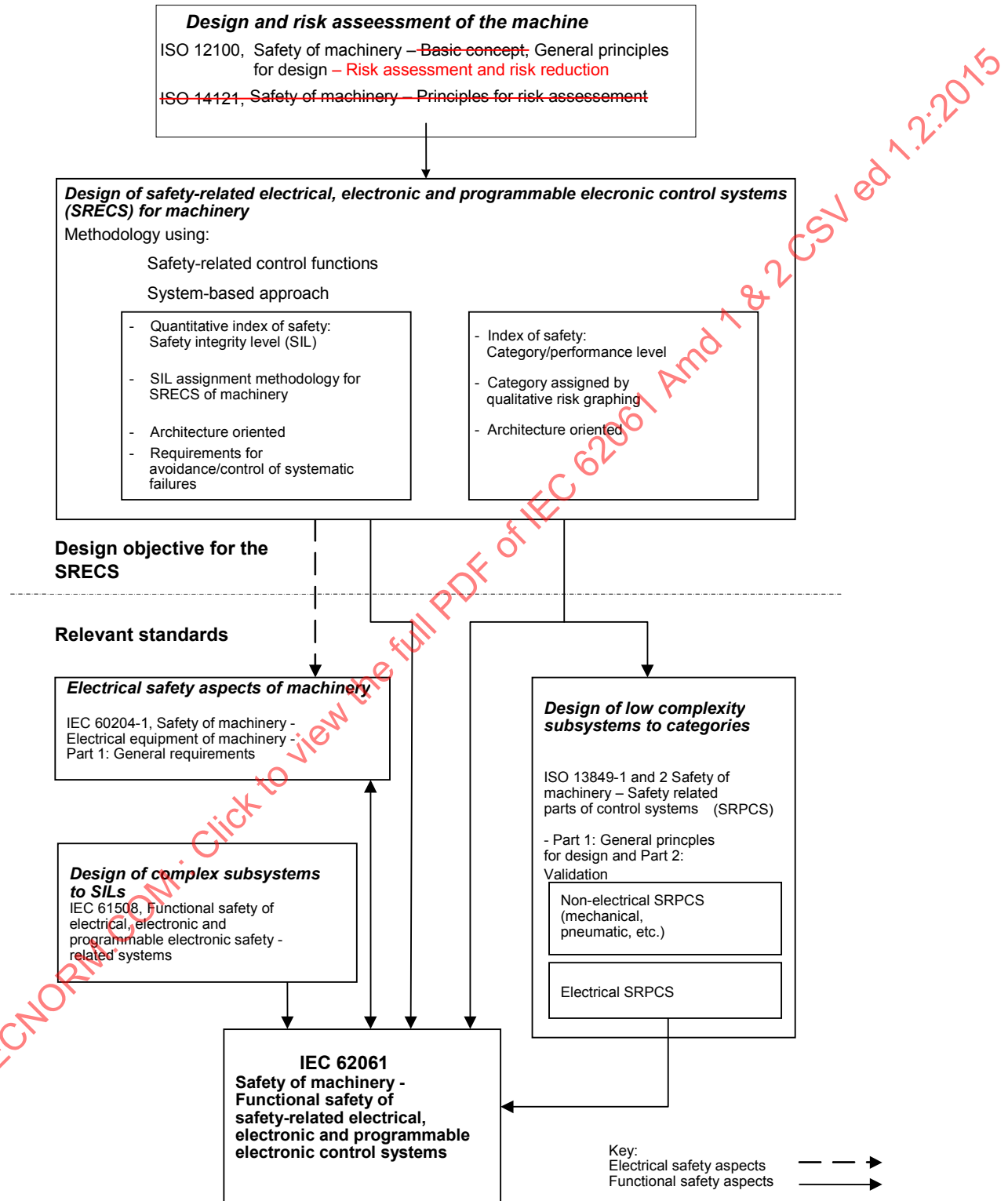


Figure 1 – Relationship of IEC 62061 to other relevant standards

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

IEC 62061:2005

– 9 –

+AMD1:2012+AMD2:2015 CSV © IEC 2015

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

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

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

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

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

1 Scope

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

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

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

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

This standard:

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

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

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

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

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

The objectives of specific Clauses in IEC 62061 are as given in Table 2.

Table 2 – Overview and objectives of IEC 62061

Clause	Objective
4: Management of functional safety	To specify the management and technical activities which are necessary for the achievement of the required functional safety of the SRECS.
5: Requirements for the specification of safety-related control functions	To set out the procedures to specify the requirements for safety-related control functions. These requirements are expressed in terms of functional requirements specification, and safety integrity requirements specification.
6: Design and integration of the safety- related electrical control system	To specify the selection criteria and/or the design and implementation methods of the SRECS to meet the functional safety requirements. This includes: selection of the system architecture, selection of the safety-related hardware and software, design of hardware and software, verification that the designed hardware and software meets the functional safety requirements.
7: Information for use of the machine	To specify requirements for the information for use of the SRECS, which has to be supplied with the machine. This includes: provision of the user manual and procedures, provision of the maintenance manual and procedures.
8: Validation of the safety- related electrical control system	To specify the requirements for the validation process to be applied to the SRECS. This includes inspection and testing of the SRECS to ensure that it achieves the requirements stated in the safety requirements specification.
9: Modification of the safety- related electrical control system	To specify the requirements for the modification procedure that has to be applied when modifying the SRECS. This includes: modifications to any SRECS are properly planned and verified prior to making the change; the safety requirements specification of the SRECS is satisfied after any modifications have taken place.

2 Normative references

The following referenced documents are indispensable for the application 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, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

IEC 61310 (all parts), *Safety of machinery – Indication, marking and actuation*

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

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

~~ISO 12100-1:2003, Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology~~

~~ISO 12100-2:2003, Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles~~

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

ISO 13849-1: ~~1999~~ 2006, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

ISO 13849-2: ~~2003~~ 2012, Safety of machinery – Safety-related parts of control systems – Part 2: Validation

~~ISO 14121, Safety of machinery – Principles of risk assessment~~

IECNORM.COM : Click to view the full PDF of IEC 62061 Amd 1 & 2 CSV ed 1.2:2015

SOMMAIRE

AVANT-PROPOS	105
INTRODUCTION.....	107
1 Domaine d'application	110
2 Références normatives.....	111
3 Termes, définitions et abréviations	112
3.1 Liste alphabétique des définitions.....	112
3.2 Termes et définitions	114
3.3 Abréviations	122
4 Gestion de la sécurité fonctionnelle	123
4.1 Objectifs.....	123
4.2 Exigences	123
5 Exigences pour la spécification des fonctions de commande relatives à la sécurité (SRCF).....	124
5.1 Objectifs.....	124
5.2 Spécification des exigences pour les SRCF.....	125
6 Conception et intégration des systèmes de commande électrique relatifs à la sécurité (SRECS)	127
6.1 Objectifs.....	127
6.2 Exigences générales	127
6.3 Exigences comportementales (d'un SRECS) lors de la détection d'une anomalie dans le SRECS	128
6.4 Exigences pour l'intégrité de sécurité systématique des SRECS	129
6.5 Choix du système de commande électrique relatif à la sécurité	131
6.6 Conception et développement d'un système de commande électrique relatif à la sécurité (SRECS)	131
6.7 Réalisation des sous-systèmes	136
6.8 Réalisation des fonctions de diagnostic.....	152
6.9 Réalisation du matériel d'un SRECS.....	153
6.10 Spécification des exigences de sécurité du logiciel.....	153
6.11 Conception et développement du logiciel.....	155
6.12 Intégration et test du système de commande électrique relatif à la sécurité	162
6.13 Installation d'un SRECS	163
7 Informations pour l'utilisation du SRECS	163
7.1 Objectifs.....	163
7.2 Documentation pour l'installation, l'utilisation et l'entretien	163
8 Validation du système de commande électrique relatif à la sécurité.....	164
8.1 Objectifs.....	164
8.2 Exigences générales	165
8.3 Validation de l'intégrité de sécurité systématique d'un SRECS	165
9 Modification.....	166
9.1 Objectifs.....	166
9.2 Procédure de modification	166
9.3 Procédures de gestion de la configuration	167
10 Documentation	169

Annexe A (informative) Attribution du niveau de SIL	171
Annexe B (informative) Exemple de conception d'un système de commande électrique relatif à la sécurité (SRECS) utilisant les concepts et exigences des Articles 5 et 6	179
Annexe C (informative) Guide pour la conception et le développement de logiciel intégré	186
Annexe D (informative) Modes de défaillance des composants électriques/électroniques	186
Annexe E (informative) Phénomènes électromagnétiques (EM) et niveaux d'immunité augmentés pour les SRECS prévus pour usage en environnement industriel selon l'IEC 61000-6-2	186
Annex F (informative) Méthodologie pour l'estimation de la sensibilité aux défaillances de cause commune (CCF)	202
Figure 1 – Relations de l'IEC 62061 avec les autres normes appropriées	108
Figure 2 – Diagramme du processus de conception et de	133
Figure 3 – Attribution des exigences de sécurité des blocs fonctionnels aux sous-systèmes (voir 6.6.2.1.1)	134
Produire une architecture pour le sous-système en accord avec la structure interne des éléments de sous-systèmes (6.7.4.3.1.1)	139
Figure 4 – Diagramme de conception et développement d'un sous-système (voir case 6B de la Figure 2)	139
Figure 5 – Décomposition d'un bloc fonctionnel en éléments de blocs fonctionnels redondants et leurs éléments de sous-systèmes associés	140
Figure 6 – Représentation logique d'un sous-système de type A	147
Figure 7 – Représentation logique d'un sous-système de type B	147
Figure 8 – Représentation logique d'un sous-système de type C	148
Figure 9 – Représentation logique d'un sous-système de type D	149
Figure A.1 – Schéma d'attribution du niveau de SIL	172
Figure A.2 – Paramètres utilisés dans l'estimation du risque	173
Figure A.3 – Exemple de pro forma pour procédé d'attribution de SIL	178
Figure B.1 – Terminologie employée en décomposition fonctionnelle	179
Figure B.2 – Exemple de machine	180
Figure B.3 – Spécification des exigences pour une SRCF	180
Figure B.4 – Décomposition en une structure de blocs fonctionnels	181
Figure B.5 – Concept initial de l'architecture d'un SRECS	182
Figure B.6 – Architecture d'un SRECS avec fonctions de diagnostic intégrées dans chaque sous-système (SS1 à SS4)	183
Figure B.7 – Architecture d'un SRECS avec fonctions de diagnostic intégrées dans un sous-système SS3	184
Figure B.8 – Estimation de la PFH_D pour un SRECS	185
Tableau 1 – Utilisation recommandée de la CEI 62061 et de l'ISO 13849-1 (révision)	185
Tableau 2 – Vue générale et objectifs de l'IEC 62061	111
Tableau 3 – Niveaux d'intégrité de sécurité: valeurs cibles des défaillances pour les SRCF	127

Tableau 4 – Caractéristiques des sous-systèmes 1 et 2 utilisés dans cet exemple (voir Note ci-dessus).....	136
Tableau 5 – Contraintes architecturales sur les sous-systèmes: SIL maximal pouvant être revendiqué pour une SRCF utilisant ce sous-système.....	142
Tableau 6 – Contraintes architecturales: SILCL en relation avec les catégories.....	
Tableau 7 – Probabilité de défaillance dangereuse.....	
Tableau 8 – Information et documentation d'un SRECS	170
Tableau A.1 – Classification de la sévérité (Se)	173
Tableau A.2 – Classification de la fréquence et durée de l'exposition (Fr).....	174
Tableau A.3 – Classification de la probabilité (Pr).....	175
Tableau A.4 – Classification de la probabilité d'évitement ou de limitation d'un dommage (AV).....	176
Tableau A.5 – Paramètres utilisés pour déterminer la classe de probabilité d'un dommage (CI).....	176
Tableau A.6 – Attribution du niveau de SIL	177
Tableau D.1 – Exemples de rapports de mode de défaillance pour des composants électriques/électroniques.....	
Tableau E.1 – Phénomènes EM et niveaux d'immunités augmentés pour les SRECS.....	
Tableau E.2 – Fréquences choisies pour les tests de champ électromagnétique RF.....	
Tableau E.3 – Fréquences choisies pour les tests perturbations conduites RF.....	
Tableau F.1 – Critères d'estimation des CCF	203
Tableau F.2 – Estimation du facteur de CCF (β)	204

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SÉCURITÉ DES MACHINES – SÉCURITÉ FONCTIONNELLE DES SYSTÈMES DE COMMANDE ÉLECTRIQUES, ÉLECTRONIQUES ET ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ

AVANT-PROPOS

- 1) La Commission Electrotechnique 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. A 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.

DÉGAGEMENT DE RESPONSABILITÉ

Cette version consolidée n'est pas une Norme IEC officielle, elle a été préparée par commodité pour l'utilisateur. Seules les versions courantes de cette norme et de son(s) amendement(s) doivent être considérées comme les documents officiels.

Cette version consolidée de l'IEC 62061 porte le numéro d'édition 1.2. Elle comprend la première édition (2005-01) [documents 44/460/FDIS et 44/470/RVD], son amendement 1 (2012-11) [documents 44/655/CDV et 44/663/RVC], son amendement 2 (2015-06) [documents 44/718/CDV et 44/725/RVC], et les corrigenda 1 (juillet 2005) et 2 (avril 2008). Le contenu technique est identique à celui de l'édition de base et à ses amendements.

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par les amendements 1 et 2. Les ajouts et les suppressions apparaissent en rouge, les suppressions étant barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

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

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de la publication de base et de ses amendements 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. A cette date, la publication sera

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

Le contenu du corrigendum d'août 2015 a été pris en considération dans cet exemplaire.

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 cette publication en utilisant une imprimante couleur.

INTRODUCTION

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

Auparavant, en l'absence de normes, on a pu observer un manque d'enthousiasme à utiliser les SRECS dans les fonctions relatives à la sécurité pour des phénomènes dangereux significatifs sur les machines, en raison de l'incertitude concernant le fonctionnement d'une telle technologie.

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 SRECS. Elle présente une approche et donne les exigences nécessaires à la réalisation du fonctionnement requis.

La présente norme est spécifique au secteur des machines dans le cadre de l'IEC 61508. Elle est destinée à faciliter la spécification du fonctionnement des systèmes de commande électriques relatifs à la sécurité par rapport aux dangers significatifs (voir 3.8 de l'ISO ~~12100~~ ~~+ 12100:2010~~) des machines.

La présente norme donne un cadre spécifique au secteur des machines pour la sécurité fonctionnelle d'un SRECS de machine. Elle 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 SRECS de machines, lesquelles peuvent aussi être appropriées pour des phases ultérieures de la vie d'un SRECS.

Il existe plusieurs circonstances dans les machines où on utilise les SRECS 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 autoriser l'accès à la zone dangereuse, signale au système de commande électrique d'arrêter le fonctionnement dangereux de la machine. Egalement en automatisation, le système de commande électrique 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. La présente norme donne une méthodologie et les exigences pour:

- assigner le niveau d'intégrité de sécurité prescrit pour chaque fonction de commande relative à la sécurité devant être réalisée par les SRECS;
- permettre la conception des SRECS appropriés à la(aux) fonction(s) de commande relative à la sécurité assignée(s);
- intégrer les sous-systèmes relatifs à la sécurité conçus selon l'ISO 13849;
- valider les SRECS.

La présente norme internationale est prévue pour être utilisée dans le cadre de la réduction systématique du risque décrite dans l'ISO ~~12100~~ ~~+ 12100~~ et conjointement avec l'appréciation du risque selon les principes décrits dans l'ISO ~~14121~~ ~~(EN 1050)~~ ~~12100~~. Une méthodologie conseillée pour l'attribution des niveaux d'intégrité de sécurité (SIL) est donnée dans l'Annexe informative A.

Des mesures sont indiquées pour coordonner le fonctionnement des SRECS avec la réduction de risque prévue en prenant en compte les probabilités et les conséquences d'anomalies systématiques ou aléatoires dans le système de commande électrique.

La Figure 1 montre les relations de la présente norme avec les autres normes appropriées.

~~Le Tableau 1 donne des conseils pour l'utilisation recommandée de la présente norme et de la révision de l'ISO 13849-1.~~

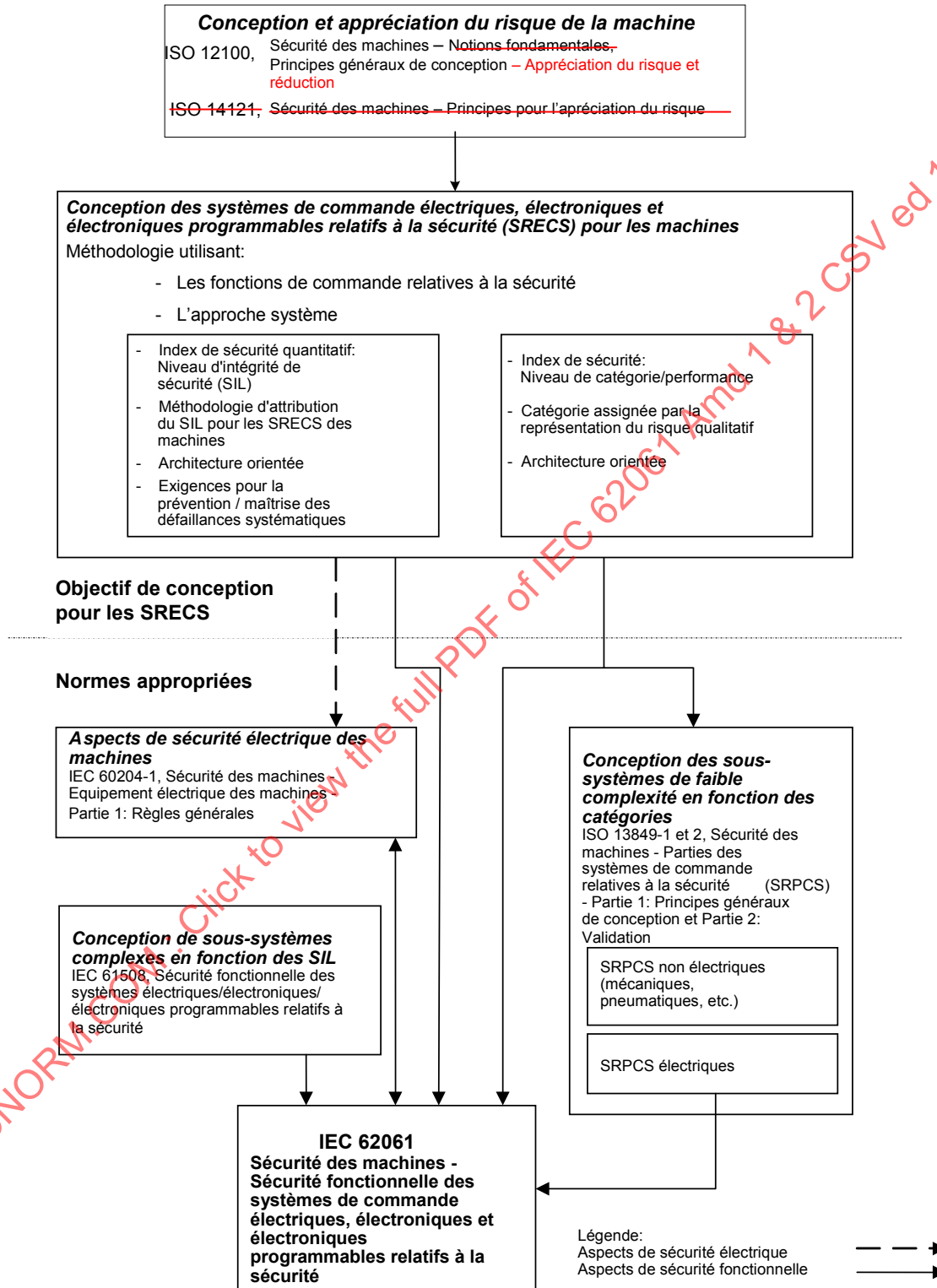


Figure 1 – Relations de l'IEC 62061 avec les autres normes appropriées

~~Information sur l'utilisation recommandée de l'IEC 62061 et de l'ISO 13849-1 (révision)~~

~~L'IEC 62061 et l'ISO 13849-1 (révision) spécifient les exigences pour la conception et la réalisation des systèmes de commande électriques relatifs à la sécurité des machines. Utiliser l'une quelconque de ces normes, en accord avec leurs domaines d'application, peut présumer de la satisfaction des exigences essentielles de sécurité appropriées. Le Tableau 1 résume les domaines d'application de l'IEC 62061 et de l'ISO 13849-1 (révision).~~

L'IEC 62061 et l'ISO 13849-1 spécifient les exigences pour la conception et la réalisation des systèmes de commande des machines relatifs à la sécurité. L'utilisation de l'une de ces deux normes, selon le domaine d'application, peut impliquer la conformité aux exigences essentielles de sécurité appropriées. L'IEC/TR 62061-1 donne des lignes directrices relatives à l'application de l'IEC 62061 et de l'ISO 13849-1 dans la conception des systèmes de commande des machines relatifs à la sécurité.

~~NOTE L'ISO 13849-1 (révision) est en cours de préparation au sein de l'ISO TC 199 et du CEN TC 114.~~

Tableau 1 – Utilisation recommandée de l'IEC 62061 et de l'ISO 13849-1 (révision)

	Technologie mettant en œuvre la(les) fonction(s) de commande relative(s) à la sécurité		ISO 13849-1 (révision)	IEC 62061
A	Non électrique, par exemple hydraulique		X	Non couvert
B	Electromécanique, par exemple relais ou électronique non complexe		Limité aux architectures désignées (voir Note 1) et jusqu'à PL=e	Toutes architectures et jusqu'à SIL 3
C	Electronique complexe, par exemple programmable		Limité aux architectures désignées (voir Note 1) et jusqu'à PL=d	Toutes architectures et jusqu'à SIL 3
D	A combiné avec B		Limité aux architectures désignées (voir Note 1) et jusqu'à PL=e	X voir Note 3
E	C combiné avec B		Limité aux architectures désignées (voir Note 1) et jusqu'à PL=d	Toutes architectures et jusqu'à SIL 3
F	C combiné avec A, ou C combiné avec A et B		X voir Note 2	X voir Note 3

"X" indique que ce cas est traité par la norme indiquée en tête de colonne.

NOTE 1 Les architectures désignées sont définies dans l'Annexe B de l'EN ISO 13849-1 (révision) afin de fournir une approche simplifiée de la quantification du niveau de performance.

NOTE 2 Pour l'électronique complexe: utilisation des architectures désignées selon l'EN ISO 13849-1 (révision) jusqu'à PL=d ou toute architecture selon l'IEC 62061.

NOTE 3 Pour la technologie non électrique, utilisation des parties en tant que sous-systèmes selon l'EN ISO 13849-1 (révision).

SÉCURITÉ DES MACHINES – SÉCURITÉ FONCTIONNELLE DES SYSTÈMES DE COMMANDE ÉLECTRIQUES, ÉLECTRONIQUES ET ÉLECTRONIQUES PROGRAMMABLES 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 électriques, électroniques et électroniques programmables relatifs à la sécurité (SRECS) pour les machines (voir Notes 1 et 2). Elle s'applique aux systèmes de commande utilisés, séparément ou en combinaison, pour assurer des fonctions de commande relatives à la 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.

NOTE 1 Dans la présente norme, le terme "systèmes de commande électrique" est utilisé à la place de "systèmes de commande électrique, électronique et électronique programmable (E/E/PE)" et "SRECS" est utilisé à la place de "systèmes de commande électrique, électronique et électronique programmable relatifs à la sécurité"

~~NOTE 2 Dans la présente norme, il est présumé que la conception des sous-systèmes électroniques programmables complexes ou des éléments de sous-systèmes est conforme aux exigences appropriées de l'IEC 61508. La présente norme fournit une méthodologie pour l'utilisation, plus que pour le développement, de tels sous-systèmes et éléments de sous-systèmes en tant que partie d'un SRECS.~~

NOTE 2 Dans la présente norme, il est supposé que la conception des sous-systèmes ou éléments de sous-système électroniques programmables complexes est conforme aux exigences appropriées de l'IEC 61508 et utilise le parcours 1_H (voir IEC 61508-2:2010, 7.4.4.2). Il est considéré que le parcours 2_H (voir IEC 61508-2:2010, 7.4.4.3) ne convient pas aux machines à usage général. La présente norme ne traite donc pas du parcours 2_H. Elle fournit une méthodologie pour l'utilisation, plus que pour le développement, de tels sous-systèmes et éléments de sous-système en tant que partie d'un SRECS.

La présente norme est une norme d'application et n'est pas destinée à limiter ou inhiber les progrès technologiques. Elle ne couvre pas toutes les exigences (par exemple protection, verrouillage non électrique ou commande non électrique) qui sont nécessaires ou prescrites par d'autres normes ou réglementations destinées à protéger les personnes des dangers. Chaque type de machine a des exigences propres qui doivent être prises en compte pour obtenir une sécurité adéquate.

La présente norme:

- ne concerne que les exigences de sécurité fonctionnelle destinées à réduire le risque de blessure ou d'atteinte à la santé des personnes à proximité immédiate de la machine et de celles directement impliquées dans l'utilisation de la machine;
- 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 3 Les exigences pour réduire les risques provenant d'autres phénomènes dangereux sont données dans les normes sectorielles appropriées. Par exemple, si une(des) machine(s) fait(font) partie d'une activité processus, il convient que les exigences de sécurité fonctionnelle du système de commande électrique de la machine satisfassent, en plus, à d'autres exigences (par exemple l'IEC 61151) sous réserve que le processus soit concerné.

- ne spécifie pas les exigences de fonctionnement des éléments de commande (par exemple hydraulique, pneumatique) non électriques des machines;

NOTE 4 Bien que les exigences de la présente norme soient particulières aux systèmes de commande électriques, le cadre et la méthodologie spécifiés peuvent s'appliquer à des parties de systèmes de commande relatives à la sécurité utilisant d'autres technologies.

- ne couvre pas les phénomènes dangereux électriques provenant du matériel de commande électrique lui-même (par exemple choc électrique – voir l'IEC 60204-1);

Les objectifs des articles particuliers à l'IEC 62061 sont donnés dans le Tableau 2:

Tableau 2 – Vue générale et objectifs de l'IEC 62061

Article	Objectifs
4: Gestion de la sécurité fonctionnelle	Spécifier les activités techniques et de gestion nécessaires pour la réalisation de la sécurité fonctionnelle prescrite des SRECS
5: Exigences pour la spécification des fonctions de commande relatives à la sécurité	Etablir les procédures de spécification des exigences pour les fonctions de commande relatives à la sécurité. Ces exigences s'expriment en termes de spécification des exigences fonctionnelles, et spécification des exigences d'intégrité de sécurité.
6: Conception et intégration des systèmes de commande électrique relatifs à la sécurité	Spécifier les critères de choix et/ou les méthodes de conception et de réalisation des SRECS pour satisfaire aux exigences de sécurité fonctionnelle. Ceci comprend: le choix de l'architecture système le choix des parties matériel et logiciel relatives à la sécurité la conception des parties matériel et logiciel la vérification que les exigences de sécurité fonctionnelle sont satisfaites par les parties matériel et logiciel ainsi conçues
7: Information pour l'utilisation de la machine	Spécifier les exigences pour l'information concernant l'utilisation des SRECS, qui est à fournir avec la machine. Ceci comprend vérifier: la fourniture d'un manuel utilisateur et de procédures pour l'utilisateur la fourniture d'un manuel d'entretien et de procédures d'entretien
8: Validation du système de commande électrique relatif à la sécurité	Spécifier les exigences pour la procédure de validation qui est à appliquer aux SRECS. Ceci comprend vérifier l'examen et l'essai du SRECS mis en service afin de s'assurer qu'il réalise les exigences établies dans la spécification des exigences de sécurité.
9: Modification du système de commande électrique relatif à la sécurité	Spécifier les exigences pour la procédure de modification qui est à appliquer lors de la modification des SRECS. Ceci comprend vérifier que: les modifications de tout SRECS sont correctement planifiées, vérifiées avant de procéder à la modification; la spécification des exigences de sécurité des SRECS est satisfaite après mise en œuvre de la modification.

2 Références normatives

Les documents référencés suivants sont indispensables pour l'application de ce document. Pour des références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition du document référencé (y compris tous les amendements) qui s'applique.

IEC 60204–1, *Sécurité des machines – Equipement électrique des machines – Partie 1: Règles générales*

IEC 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

IEC 61310 (toutes les parties), *Sécurité des machines – Indication, marquage et manoeuvre*

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

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

~~ISO 12100-1:2003, Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 1: Terminologie de base, méthodologie~~

~~ISO 12100-2:2003, Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 2: Principes techniques~~

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

ISO 13849-1:1999 2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2:2003 2012, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*

~~ISO 14121, Sécurité des machines – Principes pour l'appréciation du risque~~



FINAL VERSION

VERSION FINALE

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

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	8
2 Normative references	9
3 Terms, definitions and abbreviations	10
3.1 Alphabetical list of definitions	10
3.2 Terms and definitions	11
3.3 Abbreviations	19
4 Management of functional safety	20
4.1 Objective.....	20
4.2 Requirements.....	20
5 Requirements for the specification of Safety-Related Control Functions (SRCFs).....	21
5.1 Objective.....	21
5.2 Specification of requirements for SRCFs	21
6 Design and integration of the safety-related electrical control system (SRECS).....	23
6.1 Objective.....	23
6.2 General requirements.....	23
6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS.....	24
6.4 Requirements for systematic safety integrity of the SRECS	25
6.5 Selection of safety-related electrical control system	26
6.6 Safety-related electrical control system (SRECS) design and development	27
6.7 Realisation of subsystems.....	32
6.8 Realisation of diagnostic functions	46
6.9 Hardware implementation of the SRECS	47
6.10 Software safety requirements specification.....	48
6.11 Software design and development.....	49
6.12 Safety-related electrical control system integration and testing.....	55
6.13 SRECS installation	56
7 Information for use of the SRECS.....	57
7.1 Objective.....	57
7.2 Documentation for installation, use and maintenance	57
8 Validation of the safety-related electrical control system.....	58
8.1 Objective.....	58
8.2 General requirements.....	58
8.3 Validation of SRECS systematic safety integrity	58
9 Modification.....	59
9.1 Objective.....	59
9.2 Modification procedure	59
9.3 Configuration management procedures	60
10 Documentation	62
Annex A (informative) SIL assignment	64
Annex B (informative) Example of safety-related electrical control system (SRECS) design using concepts and requirements of Clauses 5 and 6	72

Annex C (informative) Guide to embedded software design and development.....	79
Annex F (informative) Methodology for the estimation of susceptibility to common cause failures (CCF).....	87
Figure 1 – Relationship of IEC 62061 to other relevant standards	7
Figure 2 – Workflow of the SRECS design and development process	29
Figure 3 – Allocation of safety requirements of the function blocks to subsystems (see 6.6.2.1.1)	30
Figure 4 – Workflow for subsystem design and development (see box 6B of Figure 2).....	35
Figure 5 – Decomposition of a function block into redundant function block elements and their associated subsystem elements	36
Figure 6 – Subsystem A logical representation	41
Figure 7 – Subsystem B logical representation	42
Figure 8 – Subsystem C logical representation	42
Figure 9 – Subsystem D logical representation	44
Figure A.1 – Workflow of SIL assignment process.....	65
Figure A.2 – Parameters used in risk estimation	66
Figure A.3 – Example proforma for SIL assignment process.....	71
Figure B.1 – Terminology used in functional decomposition.....	72
Figure B.2 – Example machine	73
Figure B.3 – Specification of requirements for an SRCF	73
Figure B.4 – Decomposition to a structure of function blocks	74
Figure B.5 – Initial concept of an architecture for a SRECS	75
Figure B.6 – SRECS architecture with diagnostic functions embedded within each subsystem (SS1 to SS4).....	76
Figure B.7 – SRECS architecture with diagnostic functions embedded within subsystem SS3.....	77
Figure B.8 – Estimation of PFH_D for a SRECS.....	78
Table 2 – Overview and objectives of IEC 62061	9
Table 3 – Safety integrity levels: target failure values for SRCFs	23
Table 4 – Characteristics of subsystems 1 and 2 used in this example (see Note above)	32
Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem	38
Table 8 – Information and documentation of a SRECS.....	63
Table A.1 – Severity (Se) classification.....	66
Table A.2– Frequency and duration of exposure (Fr) classification	67
Table A.3– Probability (Pr) classification.....	68
Table A.4– Probability of avoiding or limiting harm (Av) classification	69
Table A.5– Parameters used to determine class of probability of harm (CI)	69
Table A.6 – SIL assignment matrix.....	70
Table F.1 – Criteria for estimation of CCF.....	88
Table F.2 – Estimation of CCF factor (β).....	89

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, 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.

DISCLAIMER

This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 62061 bears the edition number 1.2. It consists of the first edition (2005-01) [documents 44/460/FDIS and 44/470/RVD], its amendment 1 (2012-11) [documents 44/655/CDV and 44/663/RVC] and its amendment 2 (2015-06) [documents 44/718/CDV and 44/725/RVC], the corrigenda 1 (July 2005) and 2 (April 2008). The technical content is identical to the base edition and its amendments.

This Final version does not show where the technical content is modified by amendments 1 and 2. A separate Redline version with all changes highlighted is available in this publication.

IEC 62061:2005

– 5 –

+AMD1:2012+AMD2:2015 CSV © IEC 2015

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

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

The committee has decided that the contents of the base publication and its amendments will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The contents of the corrigendum of August 2015 have been included in this copy.

IECNORM.COM : Click to view the full PDF of IEC 62061 Amd 1 & 2 CSV ed 1.2:2015

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 12100:2010) 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 and in conjunction with risk assessment according to the principles described in ISO 12100. 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.

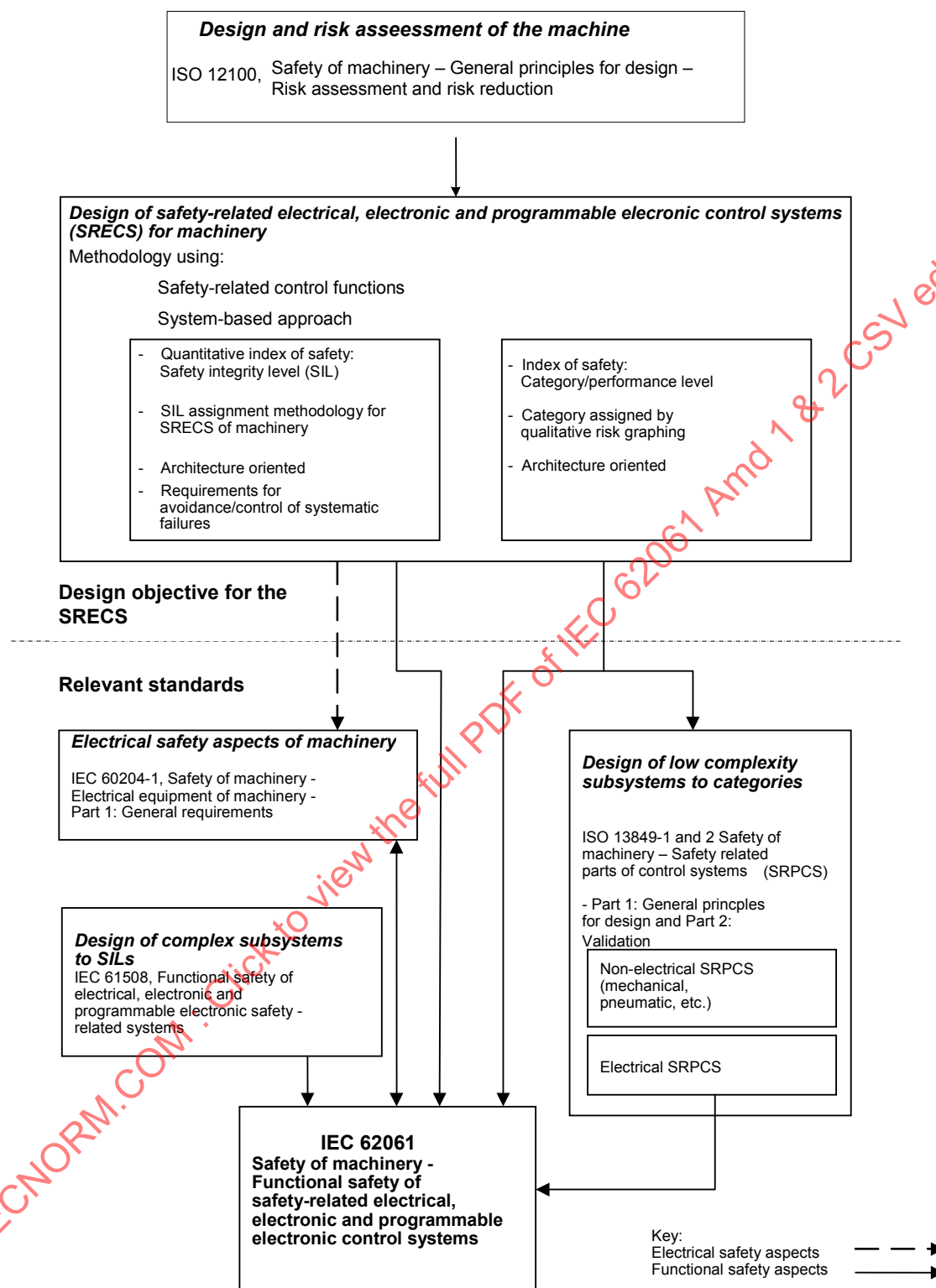


Figure 1 – Relationship of IEC 62061 to other relevant standards

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

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

1 Scope

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

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

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

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

This standard:

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

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

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

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

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

The objectives of specific Clauses in IEC 62061 are as given in Table 2.

Table 2 – Overview and objectives of IEC 62061

Clause	Objective
4: Management of functional safety	To specify the management and technical activities which are necessary for the achievement of the required functional safety of the SRECS.
5: Requirements for the specification of safety-related control functions	To set out the procedures to specify the requirements for safety-related control functions. These requirements are expressed in terms of functional requirements specification, and safety integrity requirements specification.
6: Design and integration of the safety-related electrical control system	To specify the selection criteria and/or the design and implementation methods of the SRECS to meet the functional safety requirements. This includes: selection of the system architecture, selection of the safety-related hardware and software, design of hardware and software, verification that the designed hardware and software meets the functional safety requirements.
7: Information for use of the machine	To specify requirements for the information for use of the SRECS, which has to be supplied with the machine. This includes: provision of the user manual and procedures, provision of the maintenance manual and procedures.
8: Validation of the safety-related electrical control system	To specify the requirements for the validation process to be applied to the SRECS. This includes inspection and testing of the SRECS to ensure that it achieves the requirements stated in the safety requirements specification.
9: Modification of the safety-related electrical control system	To specify the requirements for the modification procedure that has to be applied when modifying the SRECS. This includes: modifications to any SRECS are properly planned and verified prior to making the change; the safety requirements specification of the SRECS is satisfied after any modifications have taken place.

2 Normative references

The following referenced documents are indispensable for the application 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, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

IEC 61310 (all parts), *Safety of machinery – Indication, marking and actuation*

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

IEC 61508-3, *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 13849-1: 2006, *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*

IECNORM.COM : Click to view the full PDF of IEC 62061 Amd 1 & 2 CSV ed 1.2:2015

SOMMAIRE

AVANT-PROPOS	93
INTRODUCTION.....	95
1 Domaine d'application	97
2 Références normatives	98
3 Termes, définitions et abréviations	99
3.1 Liste alphabétique des définitions.....	99
3.2 Termes et définitions	101
3.3 Abréviations	109
4 Gestion de la sécurité fonctionnelle	109
4.1 Objectifs.....	109
4.2 Exigences	109
5 Exigences pour la spécification des fonctions de commande relatives à la sécurité (SRCF).....	111
5.1 Objectifs.....	111
5.2 Spécification des exigences pour les SRCF.....	111
6 Conception et intégration des systèmes de commande électrique relatifs à la sécurité (SRECS)	113
6.1 Objectifs.....	113
6.2 Exigences générales	113
6.3 Exigences comportementales (d'un SRECS) lors de la détection d'une anomalie dans le SRECS	114
6.4 Exigences pour l'intégrité de sécurité systématique des SRECS	115
6.5 Choix du système de commande électrique relatif à la sécurité	117
6.6 Conception et développement d'un système de commande électrique relatif à la sécurité (SRECS)	117
6.7 Réalisation des sous-systèmes	122
6.8 Réalisation des fonctions de diagnostic	137
6.9 Réalisation du matériel d'un SRECS.....	138
6.10 Spécification des exigences de sécurité du logiciel.....	138
6.11 Conception et développement du logiciel.....	139
6.12 Intégration et test du système de commande électrique relatif à la sécurité.....	147
6.13 Installation d'un SRECS	148
7 Informations pour l'utilisation du SRECS	148
7.1 Objectifs.....	148
7.2 Documentation pour l'installation, l'utilisation et l'entretien	148
8 Validation du système de commande électrique relatif à la sécurité.....	149
8.1 Objectifs.....	149
8.2 Exigences générales	150
8.3 Validation de l'intégrité de sécurité systématique d'un SRECS	150
9 Modification	151
9.1 Objectifs.....	151
9.2 Procédure de modification	151
9.3 Procédures de gestion de la configuration	152
10 Documentation	154