

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

ICS 13.110; 25.040.99; 29.020

National foreword

This British Standard is the UK implementation of EN 62061:2005, incorporating corrigendum February 2010. It is identical with IEC 62061:2005, incorporating corrigenda July 2005 and April 2008.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by IEC corrigendum July 2005 is indicated in the text by AC1, and text altered by IEC corrigendum April 2008 is indicated in the text by AC2.

The UK participation in its preparation was entrusted to Technical Committee MCE/3, Safety of machinery — Electrotechnical aspects.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 26 April 2005

© BSI 2010

Amendments/corrigenda issued since publication

Amd. No.	Date	Comments
15929 Corrigendum No. 1	July 2006	Implementation of IEC corrigendum July 2005
	28 February 2009	Implementation of IEC corrigendum April 2008
	31 May 2010	Implementation of CENELEC corrigendum February 2010. Replacement of EC Directive 98/37/EC with 2006/42/EC and deletion of the second dashed item in Annex ZZ

EUROPEAN STANDARD

EN 62061

NORME EUROPÉENNE

EUROPÄISCHE NORM

April 2005

ICS 13.110; 25.040.99; 29.020

Incorporates corrigendum February 2010

English version

**Safety of machinery –
Functional safety of safety-related electrical,
electronic and programmable electronic control systems
(IEC 62061:2005)**

Sécurité des machines –
Sécurité fonctionnelle des systèmes
de commande électriques, électroniques
et électroniques programmables relatifs
à la sécurité
(CEI 62061:2005)

Sicherheit von Maschinen –
Funktionale Sicherheit
sicherheitsbezogener elektrischer,
elektronischer und programmierbarer
elektronischer Steuerungssysteme
(IEC 62061:2005)

This European Standard was approved by CENELEC on 2004-12-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of document 44/460/FDIS, future edition 1 of IEC 62061, prepared by IEC TC 44, Safety of machinery - Electrotechnical aspects, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62061 on 2004-12-01.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2005-11-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2007-12-01

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EC Directive 98/37/EC. See Annex ZZ.

PROOF TEST INTERVAL AND LIFETIME

The following important information should be noted in relation to the requirements of this standard:

Where the probability of dangerous failure per hour (PFH_D) is highly dependent upon proof testing (i.e. tests intended to reveal faults not detected by diagnostic functions) then the proof test interval needs to be shown as realistic and practicable in the context of the expected use of the safety-related electrical control system (SRECS) (e.g. proof test intervals of less than 10 years can be unreasonably short for many machinery applications).

CEN/TC114/WG6 have used a proof test interval (mission time) of 20 years to support the estimation of mean time to dangerous failure ($MTTF_D$) for the realization of designated architectures in Annex B of prEN ISO 13849-1. Therefore, it is recommended that SRECS designers endeavour to use a 20 year proof test interval.

It is acknowledged that some subsystems and/or subsystem elements (e.g. electro-mechanical components with high duty cycles) will require replacement within the SRECS proof test interval.

Proof testing involves detailed and comprehensive checks that can, in practice, only be performed when the SRECS and/or its subsystems has been designed to facilitate proof testing (e.g. dedicated test ports) and provided with necessary information (e.g. proof test instructions).

To ensure the validity of the proof test interval specified by the designer it is important that any other necessary designated tests (e.g. functional tests) are also successfully performed at the SRECS.

Annexes ZA and ZZ have been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 62061:2005 was approved by CENELEC as a European Standard without any modification.

The contents of the corrigendum of February 2010 have been included in this copy.

CONTENTS

INTRODUCTION.....	6
1 Scope and object.....	9
2 Normative references	10
3 Terms, definitions and abbreviations	11
3.1 Alphabetical list of definitions	11
3.2 Terms and definitions	13
3.3 Abbreviations	21
4 Management of functional safety	22
4.1 Objective	22
4.2 Requirements	22
5 Requirements for the specification of Safety-Related Control Functions (SRCFs)	23
5.1 Objective	23
5.2 Specification of requirements for SRCFs	23
6 Design and integration of the safety-related electrical control system (SRECS)	26
6.1 Objective	26
6.2 General requirements	26
6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS	27
6.4 Requirements for systematic safety integrity of the SRECS	28
6.5 Selection of safety-related electrical control system	30
6.6 Safety-related electrical control system (SRECS) design and development	30
6.7 Realisation of subsystems	35
6.8 Realisation of diagnostic functions	51
6.9 Hardware implementation 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	61
6.13 SRECS installation	62
7 Information for use of the SRECS	62
7.1 Objective	62
7.2 Documentation for installation, use and maintenance	62
8 Validation of the safety-related electrical control system	63
8.1 General requirements	64
8.2 Validation of SRECS systematic safety integrity	64
9 Modification	65
9.1 Objective	65
9.2 Modification procedure	65
9.3 Configuration management procedures	66
10 Documentation	68

Annex A (informative) SIL assignment	70
Annex B (informative) Example of safety-related electrical control system (SRECS) design using concepts and requirements of Clauses 5 and 6	78
Annex C (informative) Guide to embedded software design and development.....	85
Annex D (informative) Failure modes of electrical/electronic components	94
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	99
Annex F (informative) Methodology for the estimation of susceptibility to common cause failures (CCF).....	101
Annex ZA (normative) Normative references to international publications with their corresponding European publications	103
Annex ZZ (informative) Coverage of Essential Requirements of EC Directives.....	104
Figure 1 – Relationship of IEC 62061 to other relevant standards	7
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 function blocks to 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.....	71
Figure A.2 – Parameters used in risk estimation	72
Figure A.3 – Example proforma for SIL assignment process	77
Figure B.1 – Terminology used in functional decomposition	78
Figure B.2 – Example machine	79
Figure B.3 – Specification of requirements for an SRCF	79
Figure B.4 – Decomposition to a structure of function blocks	80
Figure B.5 – Initial concept of an architecture for a SRECS	81
Figure B.6 – SRECS architecture with diagnostic functions embedded within each subsystem (SS1 to SS4)	82
Figure B.7 – SRECS architecture with diagnostic functions embedded within subsystem SS3.....	83
Figure B.8 – Estimation of PFH_D for a SRECS.....	84

Table 1 – Recommended application of IEC 62061 and ISO 13849-1(under revision)	8
Table 2 – Overview and objectives of IEC 62061	10
Table 3 – Safety integrity levels: target failure values for SRCFs	25
Table 4 – Characteristics of subsystems 1 and 2 used in this example.....	35
Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem	41
Table 6 – Architectural constraints: SILCL relating to categories.....	41
Table 7 – Probability of dangerous failure	44
Table 8 – Information and documentation of a SRECS.....	68
Table A.1 – Severity (Se) classification.....	73
Table A.2– Frequency and duration of exposure (Fr) classification	73
Table A.3– Probability (Pr) classification.....	74
Table A.4– Probability of avoiding or limiting harm (Av) classification	75
Table A.5– Parameters used to determine class of probability of harm (Cl).....	75
Table A.6 – SIL assignment matrix.....	76
Table D.1 – Examples of the failure mode ratios for electrical/electronic components	94
Table E.1 – EM phenomenon and increased immunity levels for SRECS	99
Table E.2 – Selected frequencies for RF field tests.....	100
Table E.3 – Selected frequencies for conducted RF tests	100
Table F.1 – Criteria for estimation of CCF.....	101
Table F.2 – Estimation of CCF factor (β).....	102

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

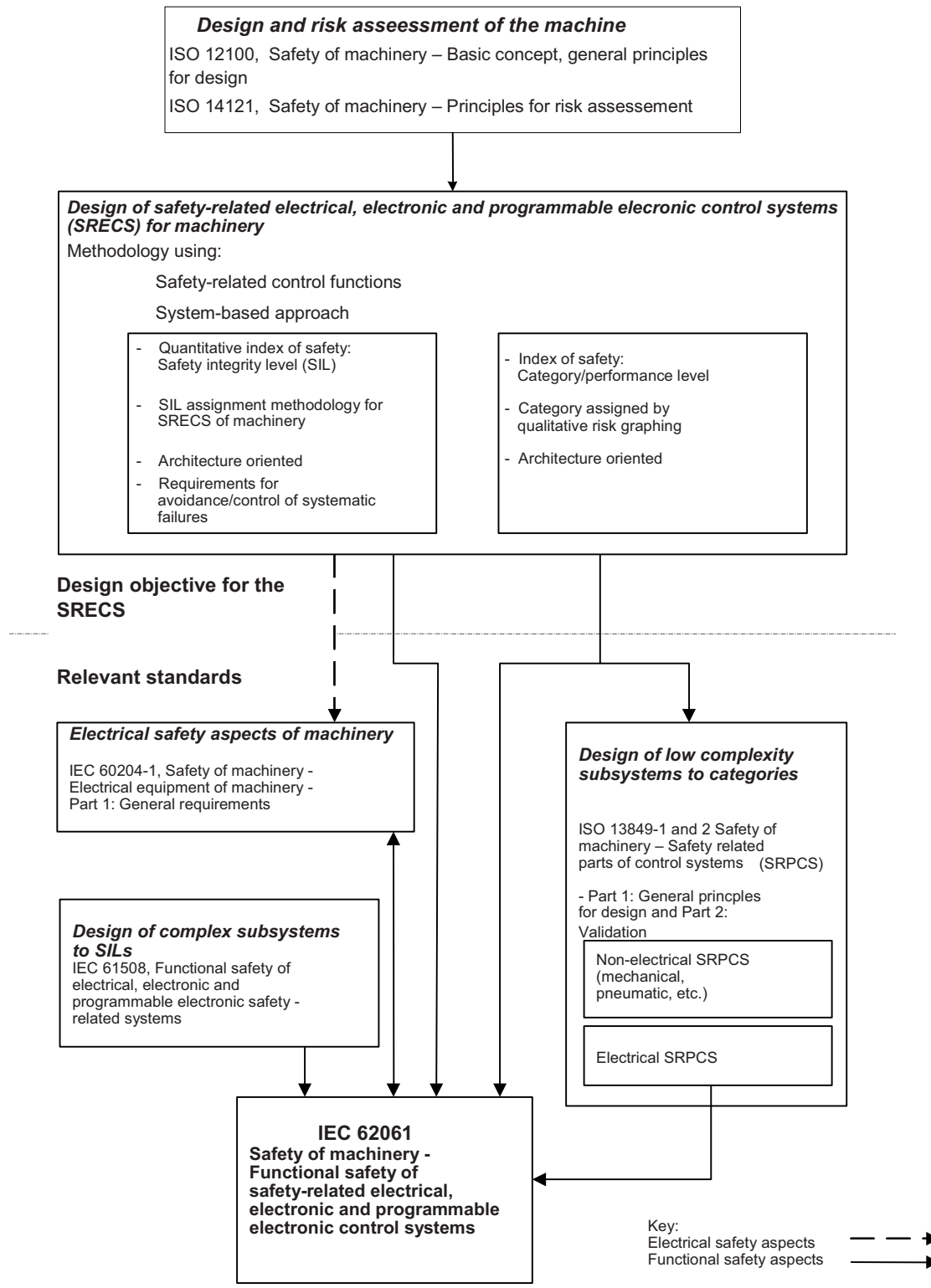


Figure 1 – Relationship of IEC 62061 to other relevant standards

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

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

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. 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).