

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+A2:2015, incorporating corrigendum February 2010. It is identical to IEC 62061:2005, incorporating amendments 1:2012 and 2:2015, and corrigenda July 2005 and April 2008. It supersedes BS EN 62061:2005+A1:2013, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment 1 is indicated by A1 tags **A1** **A1**.

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** **AC1**, and text altered by IEC corrigendum April 2008 is indicated in the text by **AC2** **AC2**.

The UK participation in its preparation was entrusted to Technical Committee MCE/3, Safeguarding of machinery.

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.

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
	30 June 2013	Implementation of IEC amendment 1:2012 with CENELEC endorsement A1:2013; Annex ZA and ZZ updated
	31 October 2015	Implementation of IEC amendment 2:2015 with CENELEC endorsement A2:2015; Annex ZA updated

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

© The British Standards Institution 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 88106 0

EUROPEAN STANDARD

EN 62061:2005+A2

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2015

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

© 2005 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

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 2006/42/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.

Foreword to amendment A1

The text of document 44/655/CDV, future edition 1 of IEC 62061:2005/A1, prepared by IEC TC 44 "Safety of machinery - Electrotechnical aspects" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62061:2005/A1:2013.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2013-09-18
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2015-12-18

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62061:2005/A1:2012 was approved by CENELEC as a European Standard without any modification.

Foreword to amendment A2

The text of document 44/718/CDV, future edition 1 of IEC 62061:2005/A2, prepared by IEC TC 44 "Safety of machinery - Electrotechnical aspects" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62061:2005/A2:2015.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2016-05-01
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2018-07-31

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of EN 62061:2005.

Endorsement notice

The text of the International Standard IEC 62061:2005/A2:2015 was approved by CENELEC as a European Standard without any modification.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60204-1	- ¹⁾	Safety of machinery - Electrical equipment of machines Part 1: General requirements	EN 60204-1 + corr. September	1997 ²⁾ 1998
IEC 61000-6-2, mod.	- ¹⁾	Electromagnetic compatibility (EMC) Part 6-2: Generic standards - Immunity for industrial environments	EN 61000-6-2	2001 ²⁾
IEC 61310	Series	Safety of machinery - Indication, marking and actuation	EN 61310	Series
IEC 61508-2	- ¹⁾	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001 ²⁾
IEC 61508-3	- ¹⁾	Part 3: Software requirements	EN 61508-3	2001 ²⁾
ISO 12100	2010	Safety of machinery – General principles for design – Risk assessment and risk reduction	EN ISO 12100	2010
ISO 13849-1	2006	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design	EN ISO 13849-1	2008
ISO 13849-2	-	Safety of machinery – Safety-related parts of control systems – Part 2: Validation	EN ISO 13849-2	-

¹⁾ Undated reference.

²⁾ Valid edition at date of issue.

Annex ZZ (informative)

Coverage of Essential Requirements of EC Directives

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and within its scope the standard covers the following essential requirements out of those given in Annex I of the EC Directive 2006/42/EC

– 1.2.1

Compliance with this standard provides one means of conformity with the specified essential requirements of the Directive concerned.

WARNING: Other requirements and other EC Directives may be applicable to the products falling within the scope of this standard.

CONTENTS

INTRODUCTION.....	9
1 Scope and object.....	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	23
4 Management of functional safety	24
4.1 Objective	24
4.2 Requirements	24
5 Requirements for the specification of Safety-Related Control Functions (SRCFs)	25
5.1 Objective	25
5.2 Specification of requirements for SRCFs	25
6 Design and integration of the safety-related electrical control system (SRECS)	28
6.1 Objective	28
6.2 General requirements	28
6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS	29
6.4 Requirements for systematic safety integrity of the SRECS	30
6.5 Selection of safety-related electrical control system	32
6.6 Safety-related electrical control system (SRECS) design and development	32
6.7 Realisation of subsystems	37
6.8 Realisation of diagnostic functions	53
6.9 Hardware implementation of the SRECS	54
6.10 Software safety requirements specification	54
6.11 Software design and development	55
6.12 Safety-related electrical control system integration and testing	63
6.13 SRECS installation	64
7 Information for use of the SRECS	64
7.1 Objective	64
7.2 Documentation for installation, use and maintenance	64
8 Validation of the safety-related electrical control system	65
8.1 General requirements	65
8.2 Validation of SRECS systematic safety integrity	66
9 Modification	67
9.1 Objective	67
9.2 Modification procedure	67
9.3 Configuration management procedures	68
10 Documentation	70

Annex A (informative) SIL assignment	72
Annex B (informative) Example of safety-related electrical control system (SRECS) design using concepts and requirements of Clauses 5 and 6	80
Annex C (informative) Guide to embedded software design and development.....	87
Annex F (informative) Methodology for the estimation of susceptibility to common cause failures (CCF).....	97
Figure 1 – Relationship of IEC 62061 to other relevant standards	10
Figure 2 – Workflow of the SRECS design and development process	34
Figure 3 – Allocation of safety requirements of the function blocks to subsystems (see 6.6.2.1.1)	35
Figure 4 – Workflow for subsystem design and development (see box 6B of Figure 2).....	40
Figure 5 – Decomposition of function blocks to function block elements and their associated subsystem elements.....	41
Figure 6 – Subsystem A logical representation	47
Figure 7 – Subsystem B logical representation	48
Figure 8 – Subsystem C logical representation	48
Figure 9 – Subsystem D logical representation	50
Figure A.1 – Workflow of SIL assignment process.....	73
Figure A.2 – Parameters used in risk estimation	74
Figure A.3 – Example proforma for SIL assignment process	79
Figure B.1 – Terminology used in functional decomposition	80
Figure B.2 – Example machine	81
Figure B.3 – Specification of requirements for an SRCF	81
Figure B.4 – Decomposition to a structure of function blocks	82
Figure B.5 – Initial concept of an architecture for a SRECS	83
Figure B.6 – SRECS architecture with diagnostic functions embedded within each subsystem (SS1 to SS4)	84
Figure B.7 – SRECS architecture with diagnostic functions embedded within subsystem SS3.....	85
Figure B.8 – Estimation of PFH_D for a SRECS.....	86

Table 2 – Overview and objectives of IEC 62061 12

Table 3 – Safety integrity levels: target failure values for SRCFs 27

Table 4 – Characteristics of subsystems 1 and 2 used in this example..... 37

Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed
for a SRCF using this subsystem 43

Table 8 – Information and documentation of a SRECS..... 70

Table A.1 – Severity (Se) classification 75

Table A.2– Frequency and duration of exposure (Fr) classification 75

Table A.3– Probability (Pr) classification..... 76

Table A.4– Probability of avoiding or limiting harm (Av) classification 77

Table A.5– Parameters used to determine class of probability of harm (CI)..... 77

Table A.6 – SIL assignment matrix..... 78

Table F.1 – Criteria for estimation of CCF 96

Table F.2 – Estimation of CCF factor (β)..... 97

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 [A2](#) ISO 12100:2010 [A2](#)) 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 [A2](#) ISO 12100 [A2](#) and in conjunction with risk assessment according to the principles described in [A2](#) ISO 12100 [A2](#). 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.

[A1](#) Text deleted [A1](#)

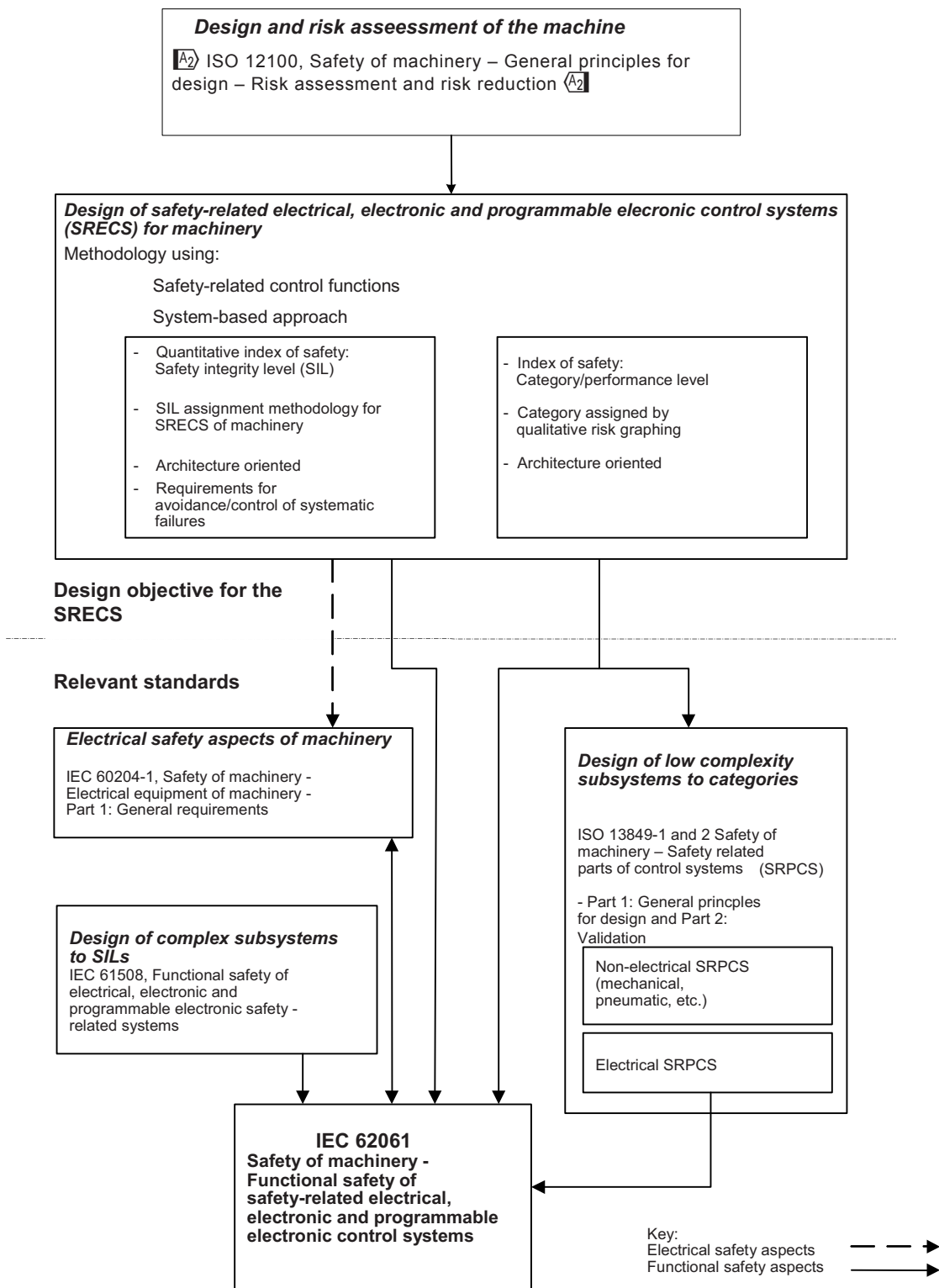


Figure 1 – Relationship of IEC 62061 to other relevant standards

[A1] Text deleted [A1]

[A1] 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. [A1]

[A1] Text deleted [A1]

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*

Text deleted

3 Terms, definitions and abbreviations

3.1 Alphabetical list of definitions

Term	Definition number
application software	3.2.46
architectural constraint	3.2.36
architecture	3.2.35
common cause failure	3.2.43
complex component	3.2.8
control function	3.2.14
dangerous failure	3.2.40
demand	3.2.25
diagnostic coverage	3.2.38
electrical control system	3.2.3
embedded software	3.2.47
failure	3.2.39
fault	3.2.30
fault tolerance	3.2.31
full variability language (FVL)	3.2.48
function block	3.2.32
function block element	3.2.33

functional safety	3.2.9
hardware safety integrity	3.2.20
hazard (from machinery)	3.2.10
hazardous situation	3.2.11
high demand or continuous mode	3.2.27
limited variability language (LVL)	3.2.49
low complexity component	3.2.7
low demand mode	3.2.26
machine control system	3.2.2
machinery (machine)	3.2.1
mean time to failure (MTTF)	3.2.34
probability of dangerous failure per hour (PFH _D)	3.2.28
proof test	3.2.37
protective measure	3.2.12
random hardware failure	3.2.44
risk	3.2.13
safe failure	3.2.41
safe failure fraction	3.2.42
safety function	3.2.15
safety integrity	3.2.19
safety integrity level (SIL)	3.2.23
safety-related control function (SRCF)	3.2.16
safety-related electrical control system (SRECS)	3.2.4
safety-related software	3.2.50
SIL claim limit	3.2.24
software safety integrity	3.2.21
SRECS diagnostic function	3.2.17
SRECS fault reaction function	3.2.18
subsystem	3.2.5
subsystem element	3.2.6
systematic failure	3.2.45
systematic safety integrity	3.2.22
target failure value	3.2.29
validation	3.2.52
verification	3.2.51

3.2 Terms and definitions

For the purposes of this standard, the following terms and definitions apply.

3.2.1

machinery

assembly of linked parts or components, at least one of which moves, with the appropriate machine actuators, control and power circuits, joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material.

The terms “machinery” and “machine” also cover an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

Ⓐ₂ [ISO 12100:2010, 3.1] Ⓐ₂

3.2.2

machine control system

system which responds to an input from, for example, the process, other machine elements, an operator, external control equipment, and generates an output(s) causing the machine to behave in the intended manner

3.2.3

electrical control system

all the electrical, electronic and programmable electronic parts of the machine control system used to provide, for example, operational control, monitoring, interlocking, communications, protection and safety-related control functions

NOTE Safety-related control functions can be performed by an electrical control system that is either integral to or independent of those parts of a machine's control system that perform non-safety-related functions.

3.2.4

Safety-Related Electrical Control System

SRECS

electrical control system of a machine whose failure can result in an immediate increase of the risk(s)

NOTE A SRECS includes all parts of an electrical control system whose failure may result in a reduction or loss of functional safety and this can comprise both electrical power circuits and control circuits.

3.2.5

subsystem

Ⓐ₁ entity of the top-level architectural design of the SRECS where a dangerous failure of any subsystem will result in a dangerous failure of a safety-related control function

Ⓐ₂ [IEC 61508-4:2010, 3.2.7] Ⓐ₂

NOTE 1 A complete subsystem can be made up from a number of identifiable and separate subsystem elements, which when put together implement the function blocks allocated to the subsystem.

NOTE 2 This differs from common language where “subsystem” may mean any sub-divided part of an entity, the term “subsystem” is used in this standard within a strongly defined hierarchy of terminology: “subsystem” is the first level subdivision of a system. The parts resulting from further subdivision of a subsystem are called “subsystem elements”. Ⓐ₁

3.2.6

subsystem element

part of a subsystem, comprising a single component or any group of components

3.2.7**low complexity component**

component in which

- the failure modes are well-defined; and
- the behaviour under fault conditions can be completely defined

Ⓐ [IEC 61508-4:2010, 3.4.3] Ⓐ

NOTE 1 Behaviour of the low complexity component under fault conditions may be determined by analytical and/or test methods.

NOTE 2 A subsystem or subsystem element comprising one or more limit switches, operating, possibly via interposing electro-mechanical relays, one or more contactors to de-energise an electric motor is an example of a low complexity component.

3.2.8**complex component**

component in which

- the failure modes are not well-defined; or
- the behaviour under fault conditions cannot be completely defined

3.2.9**functional safety**

part of the safety of the machine and the machine control system which depends on the correct functioning of the SRECS, other technology safety-related systems and external risk reduction facilities

Ⓐ [IEC 61508-4:2010, 3.1.12] Ⓐ

NOTE 1 This standard only considers the functional safety that depends on the correct functioning of the SRECS in machinery applications.

NOTE 2 ISO/IEC Guide 51 defines safety as freedom from unacceptable risk.

3.2.10**hazard (from machinery)**

potential source of physical injury or damage to health

Ⓐ [ISO 12100:2010, 3.6] Ⓐ

NOTE The term hazard can be qualified in order to define its origin or the nature of the expected harm (e.g. electric shock hazard, crushing hazard, cutting hazard, toxic hazard, fire hazard).

3.2.11**hazardous situation**

circumstance in which a person is exposed to a hazard(s)

Ⓐ [ISO 12100:2010, 3.10] Ⓐ

3.2.12**protective measure**

measure intended to achieve risk reduction

Ⓐ [ISO 12100:2010, 3.19] Ⓐ

3.2.13

risk

combination of the probability of occurrence of harm and the severity of that harm

Ⓐ₂ [ISO 12100:2010, 3.12] Ⓐ₂

3.2.14

control function

function that evaluates input information or signals and produces output information or activities

3.2.15

safety function

function of a machine whose failure can result in an immediate increase of the risk(s)

Ⓐ₂ [ISO 12100:2010, 3.30] Ⓐ₂

NOTE This definition differs from the definitions in IEC 61508-4 and ISO 13849-1.

3.2.16

Safety-Related Control Function

SRCF

control function implemented by a SRECS with a specified integrity level that is intended to maintain the safe condition of the machine or prevent an immediate increase of the risk(s)

3.2.17

SRECS diagnostic function

function intended to detect faults in the SRECS and produce a specified output information or activity when a fault is detected

NOTE This function is intended to detect faults that could lead to a dangerous failure of a SRCF and initiate a specified fault reaction function.

3.2.18

SRECS fault reaction function

function that is initiated when a fault within a SRECS is detected by the SRECS diagnostic function

3.2.19

safety integrity

probability of a SRECS or its subsystem satisfactorily performing the required safety-related control functions under all stated conditions

Ⓐ₂ [IEC 61508-4:2010, 3.5.4] Ⓐ₂

NOTE 1 The higher the level of safety integrity of the item, the lower the probability that the item will fail to carry out the required safety-related control function.

NOTE 2 Safety integrity comprises hardware safety integrity (see 3.2.20) and systematic safety integrity (see 3.2.22).

3.2.20

hardware safety integrity

part of the safety integrity of a SRECS or its subsystems comprising requirements for both the probability of dangerous random hardware failures and architectural constraints

Ⓐ₂ [IEC 61508-4:2010, 3.5.7] Ⓐ₂

3.2.21

software safety integrity

part of the systematic safety integrity of a SRECS or its subsystems related to the capability of software in a programmable electronic system performing its safety-related control functions under all stated conditions during a stated period of time

Ⓐ₂ [IEC 61508-4:2010, 3.5.5] Ⓐ₂

NOTE Software safety integrity cannot usually be quantified precisely.

3.2.22

systematic safety integrity

part of the safety integrity of a SRECS or its subsystems relating to its resistance to systematic failures (see 3.2.45) in a dangerous mode.

Ⓐ₂ [IEC 61508-4:2010, 3.5.6] Ⓐ₂

NOTE 1 Systematic safety integrity cannot usually be quantified precisely.

NOTE 2 Requirements for systematic safety integrity apply to both hardware and software aspects of a SRECS or its subsystems.

3.2.23

Safety Integrity Level

SIL

discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest

Ⓐ₂ [IEC 61508-4:2010, 3.5.8] Ⓐ₂

NOTE SIL 4 is not considered in this standard, as it is not relevant to the risk reduction requirements normally associated with machinery. For requirements applicable to SIL 4, see IEC 61508-1 and IEC 61508-2.

3.2.24

SIL Claim Limit (for a subsystem)

SILCL

maximum SIL that can be claimed for a SRECS subsystem in relation to architectural constraints and systematic safety integrity

3.2.25

demand

event that causes the SRECS to perform its SRCF

3.2.26

low demand mode

Ⓐ₁ mode of operation in which the frequency of demands on a SRECS is no greater than one per year Ⓐ₁

NOTE Equipment that is only designed in accordance with requirements for the low demand mode of operation described in IEC 61508-1 and IEC 61508-2 can be unsuitable for use as part of a SRECS in this standard. Low demand mode of operation is not considered to be relevant for SRECS applications at machinery.

3.2.27

high demand or continuous mode

Ⓐ₁ mode of operation in which the frequency of demands on a SRECS is greater than one per year or the SRCF retains the machine in a safe state as part of normal operation Ⓐ₁

Ⓐ₂ [IEC 61508-4:2010, 3.5.16] Ⓐ₂

NOTE 1 Low demand mode of operation is not considered to be relevant for SRECS applications at machinery. Therefore, in this standard SRECS are only considered to operate in the high demand or continuous mode.

NOTE 2 Demand mode means that a safety-related control function is only performed on request (demand) in order to transfer the machine into a specified state. The SRECS does not influence the machine until there is a demand on the safety-related control function.

NOTE 3 Continuous mode means that a safety-related control function is performed perpetually (continuously), i.e. the SRECS is continuously controlling the machine and a (dangerous) failure of its function can result in a hazard.

3.2.28

Probability of dangerous Failure per Hour

PFH_D

$\overline{A_1}$ average probability of a dangerous failure per hour of a safety related system/subsystem to perform the specified safety function over a given period of time

NOTE 1 PFH_D should not be confused with probability of dangerous failure on demand (PFD). $\overline{A_1}$

$\overline{A_2}$ NOTE 2 Within this standard λ is expressed as the constant failure rate with respect to 1 hour. $\overline{A_2}$

3.2.29

target failure value

intended PFH_D to be achieved to meet a specific safety integrity requirement(s)

NOTE Target failure value is specified in terms of the probability of dangerous failure per hour.

$\overline{A_2}$ [IEC 61508-4:2010, 3.5.17] $\overline{A_2}$

3.2.30

fault

abnormal condition that may cause a reduction in or loss of, the capability of a SRECS, a subsystem, or a subsystem element to perform a required function

$\overline{A_2}$ [IEC 61508-4:2010, 3.6.1] $\overline{A_2}$

3.2.31

fault tolerance

ability of a SRECS, a subsystem, or subsystem element to continue to perform a required function in the presence of faults or failures

$\overline{A_2}$ [IEC 61508-4:2010, 3.6.3] $\overline{A_2}$

3.2.32

function block

smallest element of a SRCF whose failure can result in a failure of the SRCF

NOTE 1 In this standard, a SRCF (F) may be seen as a logical AND of the function blocks (FB), i.e. $F = FB_1 \text{ AND } FB_2 \text{ AND } FB_n$.

NOTE 2 This definition of a function block differs from those used in IEC 61131-3 and other standards.

3.2.33

function block element

part of a function block

3.2.34

Mean Time To Failure

MTTF

expectation of the mean time to failure

[IEV 191-12-07, modified]

NOTE MTTF is normally expressed as an average value of expectation of the time to failure.

3.2.35**architecture**

specific configuration of hardware and software elements in a SRECS

Ⓐ₂ [IEC 61508-4:2010, 3.3.4] Ⓐ₂

3.2.36**architectural constraint**

set of architectural requirements that limit the SIL that can be claimed for a subsystem

NOTE Requirements for architectural constraints are given in 6.7.6.

3.2.37**proof test**

Ⓐ₁ periodic test performed to detect dangerous hidden failures and degradation in a SRECS and its subsystems so that, if necessary, the SRECS and its subsystems can be restored to an “as new” condition or as close as practical to this condition Ⓐ₁

Ⓐ₂ [IEC 61508-4:2010, 3.8.5] Ⓐ₂

NOTE A proof test is intended to confirm that the SRECS is in a condition that assures the specified safety integrity.

3.2.38**diagnostic coverage**

Ⓐ₁ fraction of dangerous failures detected by automatic on-line diagnostic test Ⓐ₁

Ⓐ₂ [IEC 61508-4:2010, 3.8.6] Ⓐ₂

Ⓐ₁ NOTE 1 Ⓐ₁ Diagnostic coverage (DC) can be calculated using the following equation:

$$DC = \Sigma \lambda_{DD} / \lambda_{Dtotal}$$

where λ_{DD} is the rate of detected dangerous hardware failures and λ_{Dtotal} is the rate of total dangerous hardware failures.

Ⓐ₁ NOTE 2 The fraction of detected dangerous failures is computed to be the rate of dangerous failures that are detected by automatic on-line diagnostic tests divided by the rate of total dangerous failures. Ⓐ₁

3.2.39**failure**

termination of the ability of a SRECS, a subsystem, or a subsystem element to perform a required function

Ⓐ₂ [IEC 61508-4:2010, 3.6.4 modified and ISO 12100:2010, 3.34] Ⓐ₂

NOTE Failures are either random (in hardware) or systematic (in hardware or software).

3.2.40**dangerous failure**

failure of a SRECS, a subsystem, or a subsystem element that has the potential to cause a hazard or non-functional state

Ⓐ₁ *Text deleted* Ⓐ₁

NOTE 1 Whether or not the potential is realised can depend on the channel architecture of the system; for example, in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to function state.

NOTE 2 In a subsystem with multiple channels, the probability of dangerous failure of the subsystem can be smaller than the dangerous failure rate of a channel that constitutes the subsystem. The probability of dangerous failure of a SRECS cannot be smaller than that of any subsystem constituting the SRECS. (This comes from the particular definition of “subsystem” in this standard.)

NOTE 3 A dangerous failure normally results in a failure or potential failure to perform the SRCF.

3.2.41

safe failure

failure of a SRECS, a subsystem of a SRECS, or a subsystem element of a SRECS that does not have the potential to cause a hazard

A1 Text deleted **A1**

AC2 Note deleted **AC2**

3.2.42

Safe Failure Fraction

SFF

fraction of the overall failure rate of a subsystem that does not result in a dangerous failure

NOTE Safe Failure Fraction (*SFF*) can be calculated using the following equation:

$$(\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

where

λ_S is the rate of safe failure,

$\Sigma\lambda_S + \Sigma\lambda_D$ is the overall failure rate,

λ_{DD} is the rate of dangerous failure which is detected by the diagnostic functions, and

λ_D is the rate of dangerous failure.

The diagnostic coverage (if any) of each subsystem in SRECS is taken into account in the calculation of the probability of random hardware failures. The safe failure fraction is taken into account when determining the architectural constraints on hardware safety integrity (see 6.7.7).

3.2.43

Common Cause Failure

CCF

failure, which is the result of one or more events, causing **A1** concurrent **A1** failures of two or more separate channels in a multiple channel (redundant architecture) subsystem, leading to failure of a SRCF

A2 [IEC 61508-4:2010, 3.6.10] **A2**

NOTE This definition differs from that given in **A2** ISO 12100 **A2** and IECV 191-04-23.

3.2.44

random hardware failure

failure occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

A2 [IEC 61508-4:2010, 3.6.5] **A2**

3.2.45

systematic failure

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

A2 [IEC 61508-4:2010, 3.6.6] **A2**

NOTE 1 Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

NOTE 3 Examples of causes of systematic failures include human error in

- the safety requirements specification;
- the design, manufacture, installation and/or operation of the hardware;
- the design and/or implementation of the software.

3.2.46**application software**

software specific to the application, that is implemented by the designer of the SRECS, generally containing logic sequences, limits and expressions that control the appropriate input, output, calculations, and decisions necessary to meet the SRECS functional requirements

3.2.47**embedded software**

software, supplied by the manufacturer, that is part of the SRECS and that is not normally accessible for modification

NOTE Firmware and system software are examples of embedded software.

3.2.48**Full Variability Language****FVL**

type of language that provides the capability to implement a wide variety of functions and applications

 [IEC 61511-1:2003, 3.2.81.1.3] 

NOTE 1 Typical example of systems using FVL are general-purpose computers.

NOTE 2 FVL is normally found in embedded software and is rarely used in application software.

NOTE 3 FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

3.2.49**Limited Variability Language****LVL**

type of language that provides the capability to combine predefined, application specific, library functions to implement the safety requirements specifications

 [IEC 61511-1:2003, 3.2.81.1.2] 

NOTE 1 A LVL provides a close functional correspondence with the functions required to achieve the application.

NOTE 2 Typical examples of LVL are given in IEC 61131-3. They include ladder diagram, function block diagram and sequential function chart. Instruction lists and structured text are not considered to be LVL.

NOTE 3 Typical example of systems using LVL: Programmable Logic Controller (PLC) configured for machine control.

3.2.50**safety-related software**

software that is used to implement safety-related control functions in a safety-related system

3.2.51**verification**

confirmation by examination (e.g. tests, analysis) that the SRECS, its subsystems or subsystem elements meet the requirements set by the relevant specification

 [IEC 61508-4:2010, 3.8.1 and IEC 61511-1:2003, 3.2.92] 

NOTE The verification results should provide documented objective evidence.

EXAMPLE: Verification activities include:

- reviews on outputs (documents from all phases) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;
- design reviews;
- tests performed on the designed products to ensure that they perform according to their specification;
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

3.2.52 validation

confirmation by examination (e.g. tests, analysis) that the SRECS meets the functional safety requirements of the specific application

 [IEC 61508-4:2010, 3.8.2] 

3.3 Abbreviations

The following abbreviations are used in this standard.

CCF	Common Cause Failure(s)
DC	Diagnostic Coverage
EMC	Electromagnetic Compatibility
FB	Function Block
FVL	Full Variability Language
I/O	Input/Output
LVL	Limited Variability Language
PFH_D	Probability of dangerous Failure per Hour
MTTF	Mean Time To Failure
MTTR	Mean Time To Restoration
P_{TE}	Probability of dangerous Transmission Error
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SILCL	Safety Integrity Level (SIL) Claim Limit (for subsystems)
S-R	Safety Related
SRECS	Safety-Related Electrical Control System
SRCF	Safety-Related Control Function
SRS	Safety Requirements Specification
SYS	System

4 Management of functional safety

4.1 Objective

This Clause specifies management and technical activities that are necessary for the achievement of the required functional safety of the SRECS.

4.2 Requirements

4.2.1 A functional safety plan shall be drawn up and documented for each SRECS design project, and shall be updated as necessary. The plan shall include procedures for control of the activities specified in Clauses 5 to 9.

NOTE 1 The content of the functional safety plan should depend upon the specific circumstances, which can include:

- size of project;
- degree of complexity;
- degree of novelty of design and technology;
- degree of standardization of design features;
- possible consequence(s) in the event of failure.

In particular the plan shall:

- a) identify the relevant activities specified in Clauses 5 to 9.
- b) describe the policy and strategy to fulfil the specified functional safety requirements.
- c) describe the strategy to achieve functional safety for the application software, development, integration, verification and validation.
- d) identify persons, departments or other units and resources that are responsible for carrying out and reviewing each of the activities specified in Clauses 5 to 9.
- e) identify or establish the procedures and resources to record and maintain information relevant to the functional safety of a SRECS.

NOTE 2 The following should be considered:

- the results of the hazard identification and risk assessment;
 - the equipment used for safety-related functions together with its safety requirements;
 - the organization responsible for maintaining functional safety;
 - the procedures necessary to achieve and maintain functional safety (including SRECS modifications).
- f) describe the strategy for configuration management (see 9.3) taking into account relevant organizational issues, such as authorized persons and internal structures of the organization.
 - g) establish a verification plan that shall include:
 - details of when the verification shall take place;
 - details of the persons, departments or units who shall carry out the verification;
 - the selection of verification strategies and techniques;
 - the selection and utilization of test equipment;
 - the selection of verification activities;
 - acceptance criteria; and
 - the means to be used for the evaluation of verification results.

h) establish a validation plan comprising:

- details of when the validation shall take place;
- identification of the relevant modes of operation of the machine (e.g. normal operation, setting);
- requirements against which the SRECS is to be validated;
- the technical strategy for validation, for example analytical methods or statistical tests;
- acceptance criteria; and
- actions to be taken in the event of failure to meet the acceptance criteria.

NOTE 3 The validation plan should indicate whether the SRECS and its subsystems are to be subject to routine testing, type testing and/or sample testing.

4.2.2 The functional safety plan shall be implemented to ensure prompt follow-up and satisfactory resolution of issues relevant to a SRECS arising from:

- activities specified in Clauses 5 to 9;
- verification activities; and
- validation activities.

5 Requirements for the specification of Safety-Related Control Functions (SRCFs)

5.1 Objective

This Clause sets out the procedures to specify the requirements of SRCF(s) to be implemented by the SRECS.

5.2 Specification of requirements for SRCFs

5.2.1 General

5.2.1.1 From the risk reduction strategy, as outlined in  ISO 12100 , any need for safety functions will be determined.

5.2.1.2 Where safety functions are selected to be implemented (in whole or in part) by SRECS, then the associated SRCF(s) (see 3.2.16) shall be specified.

5.2.1.3 Specifications of each SRCF shall comprise:

- functional requirements specification (see 5.2.3);
- safety integrity requirements specification (see 5.2.4).

and these shall be documented in the safety requirements specification (SRS).

NOTE 1 Where non-electrical equipment contributes towards the performance of a safety function in combination with electrical means, the target failure value(s) applicable to the non-electrical equipment is not considered within this standard. Electrical means covers any and all devices or systems operating on electrical principles, including:

- electro-mechanical devices;
- non-programmable electronic devices;
- programmable electronic devices.

NOTE 2 The SRS needs to be subject to version control as part of the configuration management procedures (see 9.3).

5.2.1.4 The safety requirements specification shall be verified to ensure consistency and completeness for its intended use.

NOTE For example this may be achieved by inspection, analysis, check-lists. See also B.2.6 of [A2](#) IEC 61508-7:2010 [A2](#).

5.2.2 Information to be available

The following information shall be used to produce both the functional requirements specification and safety integrity requirements specification of each SRCF:

- results of the risk assessment for the machine including all safety functions determined to be necessary for the risk reduction process for each specific hazard;
- machine operating characteristics, including:
 - modes of operation,
 - cycle time,
 - response time performance,
 - environmental conditions,
 - interaction of person(s) with the machine (e.g. repairing, setting, cleaning);
- all information relevant to the SRCFs which can have an influence on the SRECS design including, for example:
 - a description of the behaviour of the machine that a SRCF is intended to achieve or to prevent;
 - all interfaces between the SRCFs, and between SRCFs and any other function (either within or outside the machine);
 - required fault reaction functions of the SRCF.

NOTE Some of the information might not be available or sufficiently defined before starting the iterative design process of SRECS, so the SRECS safety requirements specifications can be required to be updated during the design process.

5.2.3 Functional requirements specification for SRCFs

[A1](#) The functional requirements specification for SRCFs shall describe details of each SRCF to be performed including, as applicable:

- the condition(s) (e.g. operating mode) of the machine in which the SRCF shall be active or disabled;
- the priority of those functions that can be simultaneously active and that can cause conflicting action;
- the frequency of operation of each SRCF;
- the required response time of each SRCF;
- the interface(s) of the SRCFs to other machine functions;
- the required response times (e.g. input and output devices);
- a description of each SRCF;
- a description of fault reaction function(s) and any constraints on, for example, re-starting or continued operation of the machine in cases where the initial fault reaction is to stop the machine;
- a description of the operating environment (e.g. temperature, humidity, dust, chemical substances, mechanical vibration and shock); [A1](#)

- A1** – tests and any associated facilities (e.g. test equipment, test access ports);
- rate of operating cycles, duty cycle, and/or utilisation category, for electromechanical devices intended for use in the SRCF.

NOTE 1 In addition to the requirements of IEC 61000-6-2, when a SRECS is intended for use in an industrial environment, electromagnetic (EM) immunity levels are given in IEC 61326-3-1. SRECS intended for use in another EM environment (e.g. residential) should have immunity levels based on those specified in different EMC standards (e.g., for a residential environment, IEC 61000-6-1).

NOTE 2 When specifying EM immunity levels it is necessary to consider whether the levels used in different EMC standards cover cases which can occur in a SRECS application even with a low probability of occurrence.

NOTE 3 EM immunity performance criterion for functional safety of a SRECS is given in 6.4.3. **A1**

5.2.4 Safety integrity requirements specification for SRCFs

5.2.4.1 The safety integrity requirements for each SRCF shall be derived from the risk assessment to ensure the necessary risk reduction can be achieved. In this standard, a safety integrity requirement is expressed as a target failure value for the probability of dangerous failure per hour of each SRCF.

5.2.4.2 The safety integrity requirements for each SRCF shall be specified in terms of a SIL in accordance with Table 3 and documented. An example of a methodology is given in Annex A.

Table 3 – Safety integrity levels: target failure values for SRCFs

Safety integrity level	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE Where the required safety integrity of a SRCF is less than SIL 1, as a minimum the requirements of category B of ISO 13849-1 should be met.

5.2.4.3 Where a product standard specifies a SIL for a SRCF then this shall take precedence over Annex A.

6 Design and integration of the safety-related electrical control system (SRECS)

6.1 Objective

This Clause specifies requirements for the selection or design of a SRECS to meet the functional and safety integrity requirements specified in the safety requirements specification (see 5.2).

6.2 General requirements

6.2.1 The SRECS shall be selected or designed to meet the safety requirements specification (see 5.2) and where relevant the software safety requirements specification (see 6.10) taking into account the appropriate requirements of this standard.

6.2.2 The selection or design of the SRECS (including the overall hardware and software architecture, sensors, actuators, programmable electronics, embedded software, application software, etc.) shall comply with either 6.5 or 6.6. Whichever method is used, the SRECS shall meet the following requirements:

- a) the requirements for hardware safety integrity comprising:
 - the architectural constraints on hardware safety integrity (see 6.6.3.3); and
 - the requirements for the probability of dangerous random hardware failures (see 6.6.3.2);
- b) the requirements for systematic safety integrity (see 6.4) comprising:
 - the requirements for the avoidance of failures, and
 - the requirements for the control of systematic faults;
- c) the requirements for SRECS behaviour on detection of a fault (see 6.3);
- d) the requirements for the design and development of safety-related software (see 6.10 and 6.11).

6.2.3 The design of the SRECS shall take into account human capabilities and limitations (including reasonably foreseeable misuse) and be suitable for the actions assigned to operators, maintenance staff and others who might interact with the SRECS. The design of all operator interfaces shall follow good human-factor practice (see the IEC 61310 series) and shall accommodate the likely level of training or awareness of operators, in particular, for mass-produced subsystems where the operator can be a member of the public.

NOTE The design goal should be that reasonably foreseeable mistakes made by operators or maintenance staff are prevented or eliminated by design. Where this is not possible, other means should also be applied (e.g. manual action with secondary confirmation before completion) to minimize the possibility of operator errors and ensure that foreseeable mistakes do not lead to increased risk.

6.2.4 Maintainability and testability shall be considered during the design and integration to facilitate the implementation of these properties in the SRECS.

6.2.5 The SRECS design, including its diagnostic and fault reaction functions, shall be documented. This documentation shall:

- be accurate, complete and concise;
- be suitable for its intended purpose;
- be accessible and maintainable;
- be version controlled.

6.2.6 The outcome of the activities performed during SRECS design, development and implementation shall be verified at appropriate stages.

6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS

6.3.1 The detection of a dangerous fault in any subsystem that has a hardware fault tolerance of more than zero shall result in the performance of the specified fault reaction function.

The specification may allow isolation of the faulty part of the subsystem to continue safe operation of the machine while the faulty part is repaired. In this case, if the faulty part is not repaired within the estimated maximum time as assumed in the calculation of the probability of random hardware failure (see 6.7.8), then a second fault reaction shall be performed to maintain a safe condition.

Where the SRECS is designed for online repair, isolation of a faulty part shall only be applicable where this does not increase the probability of dangerous random hardware failure of the SRECS above that specified in the SRS.

After the occurrence of faults that reduce the hardware fault tolerance to zero, the requirements of 6.3.2 apply.

NOTE The mean time to restoration (see IEC 60050-191-13-08) that is considered in the reliability model will need to take into account the diagnostic test interval, the repair time and any other delays prior to restoration.

6.3.2 Where a diagnostic function(s) is necessary to achieve the required probability of dangerous random hardware failure and the subsystem has a hardware fault tolerance of zero, then the fault detection and specified fault reaction shall be performed before the hazardous situation addressed by the SRCF can occur.

EXCEPTION to 6.3.2: In the case of a subsystem implementing a particular SRCF where the hardware fault tolerance is zero and the ratio of the diagnostic test rate to the demand rate exceeds 100, then the diagnostic test interval of that subsystem shall be such as to enable the subsystem to meet the requirement for the probability of dangerous random hardware failure.

6.3.3 Where performance of a fault reaction function as part of a SRCF that is specified as SIL 3 has resulted in the machine being stopped, subsequent normal operation of the machine via the SRECS (e.g. enabling re-start of the machine) shall not be possible until the fault has been repaired or rectified. For SRCFs with a specified safety integrity of less than SIL 3, the behaviour of the machine after performance of a fault reaction function (e.g. re-starting normal operation) shall depend on the specification of relevant fault reaction functions (see 5.2.3).