

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Withdrawn



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2005 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch

Tel.: +41 22 919 02 11

Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: csc@iec.ch

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

PRICE CODE
CODE PRIX

XD

ICS 13.110; 25.040.99; 29.020

ISBN 2-8318-7818-7

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope and object.....	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	23
4.1 Objective	23
4.2 Requirements	23
5 Requirements for the specification of Safety-Related Control Functions (SRCFs)	24
5.1 Objective	24
5.2 Specification of requirements for SRCFs	24
6 Design and integration of the safety-related electrical control system (SRECS)	27
6.1 Objective	27
6.2 General requirements	27
6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS	28
6.4 Requirements for systematic safety integrity of the SRECS	29
6.5 Selection of safety-related electrical control system	31
6.6 Safety-related electrical control system (SRECS) design and development	31
6.7 Realisation of subsystems	36
6.8 Realisation of diagnostic functions	52
6.9 Hardware implementation of the SRECS	53
6.10 Software safety requirements specification	53
6.11 Software design and development	54
6.12 Safety-related electrical control system integration and testing	62
6.13 SRECS installation	63
7 Information for use of the SRECS	63
7.1 Objective	63
7.2 Documentation for installation, use and maintenance	63
8 Validation of the safety-related electrical control system	64
8.1 General requirements	65
8.2 Validation of SRECS systematic safety integrity	65
9 Modification	66
9.1 Objective	66
9.2 Modification procedure	66
9.3 Configuration management procedures	67
10 Documentation	69

Annex A (informative) SIL assignment	71
Annex B (informative) Example of safety-related electrical control system (SRECS) design using concepts and requirements of Clauses 5 and 6	79
Annex C (informative) Guide to embedded software design and development.....	86
Annex D (informative) Failure modes of electrical/electronic components	95
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	100
Annex F (informative) Methodology for the estimation of susceptibility to common cause failures (CCF).....	102
Figure 1 – Relationship of IEC 62061 to other relevant standards	8
Figure 2 – Workflow of the SRECS design and development process	33
Figure 3 – Allocation of safety requirements of the function blocks to subsystems (see 6.6.2.1.1)	34
Figure 4 – Workflow for subsystem design and development (see box 6B of Figure 2).....	39
Figure 5 – Decomposition of a function block into redundant function block elements and their associated subsystem elements	40
Figure 6 – Subsystem A logical representation	46
Figure 7 – Subsystem B logical representation	47
Figure 8 – Subsystem C logical representation	47
Figure 9 – Subsystem D logical representation	49
Figure A.1 – Workflow of SIL assignment process.....	72
Figure A.2 – Parameters used in risk estimation	73
Figure A.3 – Example proforma for SIL assignment process	78
Figure B.1 – Terminology used in functional decomposition	79
Figure B.2 – Example machine	80
Figure B.3 – Specification of requirements for an SRCF	80
Figure B.4 – Decomposition to a structure of function blocks	81
Figure B.5 – Initial concept of an architecture for a SRECS	82
Figure B.6 – SRECS architecture with diagnostic functions embedded within each subsystem (SS1 to SS4).....	83
Figure B.7 – SRECS architecture with diagnostic functions embedded within subsystem SS3.....	84
Figure B.8 – Estimation of PFH_D for a SRECS.....	85
Table 1 – Recommended application of IEC 62061 and ISO 13849-1(under revision)	9
Table 2 – Overview and objectives of IEC 62061	11
Table 3 – Safety integrity levels: target failure values for SRCFs	26
Table 4 – Characteristics of subsystems 1 and 2 used in this example.....	36
Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem	42
Table 6 – Architectural constraints: SILCL relating to categories.....	43
Table 7 – Probability of dangerous failure	45
Table 8 – Information and documentation of a SRECS	69

Table A.1 – Severity (Se) classification.....	74
Table A.2– Frequency and duration of exposure (Fr) classification	74
Table A.3– Probability (Pr) classification.....	75
Table A.4– Probability of avoiding or limiting harm (Av) classification	76
Table A.5– Parameters used to determine class of probability of harm (CI).....	76
Table A.6 – SIL assignment matrix.....	76
Table D.1 – Examples of the failure mode ratios for electrical/electronic components	95
Table E.1 – EM phenomenon and increased immunity levels for SRECS	100
Table E.2 – Selected frequencies for RF field tests.....	101
Table E.3 – Selected frequencies for conducted RF tests	101
Table F.1 – Criteria for estimation of CCF.....	102
Table F.2 – Estimation of CCF factor (β).....	103

Withdrawn

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

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

The text of this standard is based on the following documents:

FDIS	Report on voting
44/460/FDIS	44/470/RVD

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

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

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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 corrigenda of July 2005 and April 2008 have been included in this copy.

Withdrawn

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.

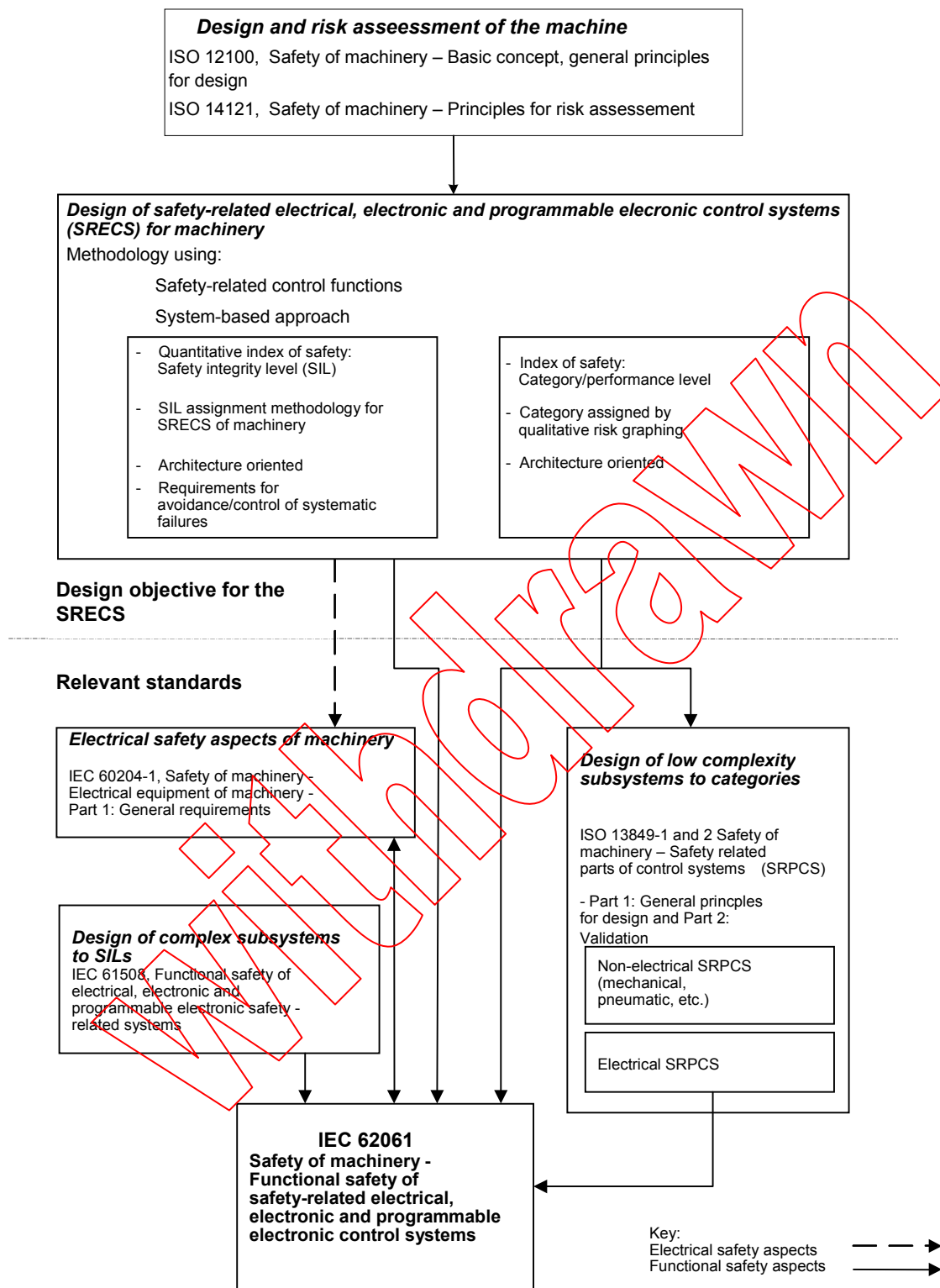


Figure 1 – Relationship of IEC 62061 to other relevant standards

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).

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

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

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

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.

[ISO 12100-1:2003, 3.1]

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

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

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 definition is a limitation of the general definition of IEC 61508-4: “set of elements which interact according to a design, where an element of a system can be another system, called a subsystem, which may include hardware, software and human interaction.”

NOTE 3 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”.

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, 3.4.4 modified]

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, 3.1.9 modified]

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 12100-1: 2003, 3.6 modified]

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 12100-1:2003, 3.9 modified]

3.2.12**protective measure**

measure intended to achieve risk reduction

[ISO 12100-1:2003, 3.18 modified]

3.2.13

risk

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

ISO 12100-1:2003, 3.11]

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)

[ISO 12100-1:2003, 3.28]

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

[IEC 61508-4, 3.5.2 modified]

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

[IEC 61508-4, 3.5.5 modified]

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

[IEC 61508-4, 3.5.3 modified]

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.

[IEC 61508-4, 3.5.4 modified]

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

[IEC 61508-4, 3.5.6 modified]

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**

mode of operation in which the frequency of demands on a SRECS is no greater than one per year and no greater than twice the proof-test frequency

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**

mode of operation in which the frequency of demands on a SRECS is greater than one per year or greater than twice the proof-test frequency

[IEC 61508-4, 3.5.12 modified]

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

average probability of dangerous failure within 1 h

NOTE PFH_D should not be confused with probability of failure on demand (PFD).

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.

[IEC 61508-4, 3.5.13 modified]

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

[IEC 61508-4, 3.6.1 modified]

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

[IEC 61508-4, 3.6.3 modified]

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

[IEC 61508-4, 3.3.5 modified]

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**

test that can detect faults 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

[IEC 61508-4, 3.8.5 modified]

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**

decrease in the probability of dangerous hardware failures resulting from the operation of the automatic diagnostic tests

[IEC 61508-4, 3.8.6 modified]

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

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

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

3.2.39**failure**

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

[IEC 61508-4, 3.6.4 modified and ISO 12100-1:2003, 3.32]

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

[IEC 61508-4, 3.6.7 modified]

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

[IEC 61508-4, 3.6.8 modified]

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 coincident failures of two or more separate channels in a multiple channel (redundant architecture) subsystem, leading to failure of a SRCF

[IEC 61508-4, 3.6.10 modified]

NOTE This definition differs from that given in ISO 12100-1 and IEC 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

[IEC 61508-4, 3.6.5]

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

[IEC 61508-4, 3.6.6]

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, 3.2.81.1.3 modified]

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, 3.2.81.1.2 modified]

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, 3.8.1 modified and IEC 61511-1, 3.2.92 modified]

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, 3.8.2 modified]

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 12100-1, ISO 12100-2, and ISO 14121, 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 IEC 61508-7.

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

5.2.3.1 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);
- 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.

5.2.3.2 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 Annex E. 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 1 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 2 EM immunity performance criterion for functional safety of a SRECS is given in 6.4.3.

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 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).

6.4 Requirements for systematic safety integrity of the SRECS

NOTE These requirements are applicable at the 'system level' where subsystems are interconnected to realise a SRECS. For requirements relevant to subsystem realisation, see 6.7.8.

6.4.1 Requirements for the avoidance of systematic hardware failures

6.4.1.1 The following measures shall be applied:

- a) the SRECS shall be designed and implemented in accordance with the functional safety plan (see 4.2);
- b) proper selection, combination, arrangements, assembly and installation of subsystems, including cabling, wiring and any interconnections;
- c) use of the SRECS within the manufacturer's specification;
- d) use of manufacturer's application notes, for example catalogue sheets, installation instructions, and use of good engineering practice (see also ISO 13849-2, Clause D.1);
- e) use of subsystems that have compatible operating characteristics (see also ISO 13849-2, Clause D.1);
- f) the SRECS shall be protected in accordance with IEC 60204-1;
- g) prevention of the loss of functional earth connection(s) in accordance with IEC 60204-1;
- h) undocumented modes of component operation shall not be used (e.g. 'reserved' registers of programmable equipment); and
- i) consideration of foreseeable misuse, environmental changes or modification(s).

6.4.1.2 In addition, at least one of the following techniques and/or measures shall be applied taking into account the complexity of the SRECS and the SIL(s) for those functions to be implemented by the SRECS:

- a) SRECS hardware design review (e.g. by inspection or walk-through): to establish by reviews and/or analysis any discrepancies between the specification and implementation;

NOTE 1 In order to reveal discrepancies between the specification and implementation, any points of doubt or potential weak points concerning the realisation, the implementation and the use of the product are documented so they can be resolved; taking into account that on an inspection procedure the author is passive and the inspector is active whilst on a walk-through procedure the author is active and the inspector is passive.

- b) advisory tools such as computer-aided design packages capable of simulation or analysis, and/or the use of computer-aided design tools to perform the design procedures systematically with the use of pre-designed elements that are already available and tested;

NOTE 2 The integrity of these tools can be demonstrated by specific testing, or by an extensive history of satisfactory use, or by independent verification of their output for the particular SRECS that is being designed. See 6.11.3.4.

- c) simulation: perform a systematic and complete assimilation of a SRECS design in terms of both functional performance and the correct dimensioning and interaction of its subsystems.

EXAMPLE The function of the SRECS can be simulated on a computer via a software behavioural model (see 6.11.3.4) where individual subsystems or subsystem elements each have their own simulated behaviour, and the response of the circuit in which they are connected is examined by looking at the marginal data of each subsystem or subsystem element.

6.4.2 Requirements for the control of systematic faults

The following measures shall be applied:

- a) use of de-energization: the SRECS shall be designed so that with loss of its electrical supply a safe state of the machine is achieved or maintained;
- b) measures to control the effect of temporary subsystem failures: the SRECS shall be designed so that, for example:
 - voltage variation (e.g. interruptions, dips) to an individual subsystem or a part of a subsystem does not lead to a hazard (e.g. a voltage interruption that affects a motor circuit shall not cause an unexpected start-up when the supply is restored), and

NOTE 1 See also relevant requirements of IEC 60204-1. In particular:

overvoltage or undervoltage should be detected early enough so that all outputs can be switched to a safe condition by the power-down routine or a switch-over to a second power unit; and/or

where necessary, overvoltage or undervoltage should be detected early enough so that the internal state can be saved in non-volatile memory, so that all outputs can be set to a safe condition by the power-down routine, or all outputs can be switched to a safe condition by the power-down routine or a switch-over to a second power unit.

- the effects of electromagnetic interference from the physical environment or a subsystem(s) do not lead to a hazard;
- c) measures to control the effects of errors and other effects arising from any data communication process, including transmission errors, repetitions, deletion, insertion, re-sequencing, corruption, delay and masquerade;

NOTE 2 Further information can be found in IEC 60870-5-1, EN 50159-1, EN 50159-2 and IEC 61508-2.

NOTE 3 The term 'masquerade' means that the true contents of a message are not correctly identified. For example, a message from a non-safety component is incorrectly identified as a message from a safety component.

- d) when a dangerous fault occurs at an interface, the fault reaction function shall be performed before the hazard due to this fault can occur. When a fault that reduces the hardware fault tolerance to zero occurs, this fault reaction shall take place before the estimated MTTR (see 6.7.4.4.2 g) is exceeded.

The requirements of item d) apply to interfaces that are inputs and outputs of subsystems and all other parts of subsystems that include or require cabling during integration (for example output signal switching devices of a light curtain, output of a guard position sensor).

NOTE 4 This does not require that a subsystem or subsystem element on its own has to detect a fault on its outputs(s). The fault reaction function may also be initiated by any subsequent subsystem after a diagnostic test is performed.

6.4.3 Electromagnetic (EM) immunity

In addition to the requirements of IEC 61000-6-2 and the EM phenomena given in Annex E, the following performance criterion for functional safety shall be satisfied by a SRECS:

- unsafe conditions or hazards shall not be introduced; and
- no loss of the SRCF(s); or

- the SRCF(s) implemented by the SRECS may be disturbed temporarily or permanently provided that a safe state of the machine is maintained or achieved before a hazard can occur. Where the EM phenomena can result in the destruction of components, it shall be ensured (e.g. by analysis) that functional safety is not affected, including by lower value(s) of EM phenomena that can cause partial destruction.

NOTE Consideration should be given to the behaviour of the SRECS in response to EM phenomena at all value(s) up to those given in Annex E.

6.5 Selection of safety-related electrical control system

Where a supplier provides a SRECS for a specific function referenced in the safety requirements specification, a pre-designed SRECS may be selected instead of a custom design providing that it meets the requirements of the safety requirements specification and 6.3, 6.4 and 6.6.1.

NOTE Selection of a pre-designed SRECS is an alternative to the design and development of a specific SRECS in accordance with 6.6.

6.6 Safety-related electrical control system (SRECS) design and development

6.6.1 General requirements

6.6.1.1 The SRECS shall be designed and developed in accordance with the SRECS safety requirements specification (see 5.2).

6.6.1.2 A clearly structured design process shall be followed and documented (see 6.6.2).

6.6.1.3 Where the use of diagnostics is necessary to achieve the required safety integrity when a fault is detected, the SRECS shall perform the specified fault reaction function (see 5.2 and 6.3).

6.6.1.4 Where a SRECS or part of a SRECS (i.e. its subsystem(s)) is to implement both SRCFs and other functions, then all its hardware and software shall be treated as safety-related unless it can be shown that the implementation of the SRCFs and other functions is sufficiently independent (i.e. that the normal operation or failure of any other functions do not affect the SRCFs).

NOTE Sufficient independence of implementation can be established by showing that the probability of a dependent failure between the non-safety and safety-related parts is equivalent to that of the safety integrity level of the SRECS.

6.6.1.5 For a SRECS or its subsystems that implements safety-related control functions of different safety integrity levels, its hardware and software shall be treated as requiring the highest safety integrity level unless it can be shown that the implementation of the safety-related control functions of the different safety integrity levels is sufficiently independent.

NOTE Sufficient independence of implementation can be established by showing that the probability of a dependent failure between the parts implementing SRCFs of different integrity levels is equivalent to that of the safety integrity level achieved by the SRECS.

6.6.1.6 Interconnections (e.g. wiring, cabling) other than digital data communication shall be considered to be part of one of the subsystems to which they are connected (see also item d) of 6.4.2).

6.6.1.7 Where digital data communication is used as a part of a SRECS implementation it shall satisfy the relevant requirements of IEC 61508-2 in accordance with the SIL target(s) of the SRCF(s).

6.6.1.8 The information for use of the SRECS shall specify those techniques and measures necessary during the design life of the SRECS to maintain the safety integrity level.

6.6.2 Design and development process

The design and development shall follow a clearly defined process that shall take into account all aspects covered by the process shown in Figure 2.

NOTE The approach of this standard is to apply a structured design process to the SRECS beginning from the requirements that are specified in the Safety Requirements Specification. Figure 3 shows the workflow of the design process and the terminology that applies to the different levels.

6.6.2.1 System architecture design

6.6.2.1.1 Each SRCF as specified in the SRECS safety requirements specification shall be decomposed to a structure of function blocks, for example as shown in Figure 3. This structure shall be documented comprising:

- the description of the structure;
- the safety requirements (functional, integrity,) for each function block;
- definition of inputs and outputs of each function block.

NOTE 1 The decomposition process should lead to a structure of function blocks that fully describes the functional and integrity requirements of the SRCF. This process should be applied down to that level that permits the functional and integrity requirements determined for each function block to be allocated to subsystems, where the allocation to a subsystem of the complete functional requirements of a function block is possible. However, it is possible to allocate more than one function block to a single subsystem, but it is not possible to allocate one function block to several subsystems where it is intended that these subsystems have separate functional and integrity requirements. Where the intention is to allocate the functional requirements of one function block to redundant subsystem elements, refer to 6.7.4.

NOTE 2 The inputs and outputs of each function block are the information that is transferred, for example speed, position, mode of operation, etc.

NOTE 3 The function blocks are a representation of functions of the SRCF (see 3.2.16) and do not include SRECS diagnostic functions (see 3.2.17). For the purposes of this standard, the diagnostic functions are considered as separate functions that may have a different structure to the SRCF (see 6.8).

6.6.2.1.2 An initial concept for an architecture of the SRECS shall be created in accordance with the structure of the function blocks.

NOTE There should be ongoing collaboration between the developer of the safety-related control architecture, the organization responsible for configuration of the devices and the developer of the software. As the software safety requirements and the possible software architecture become more precise, there may be an impact on the SRECS hardware architecture, and for this reason close co-operation between the SRECS architecture designer, the subsystem supplier(s), software developer and, as necessary, the machinery designer or the user can help to reduce the potential for systematic failure(s).

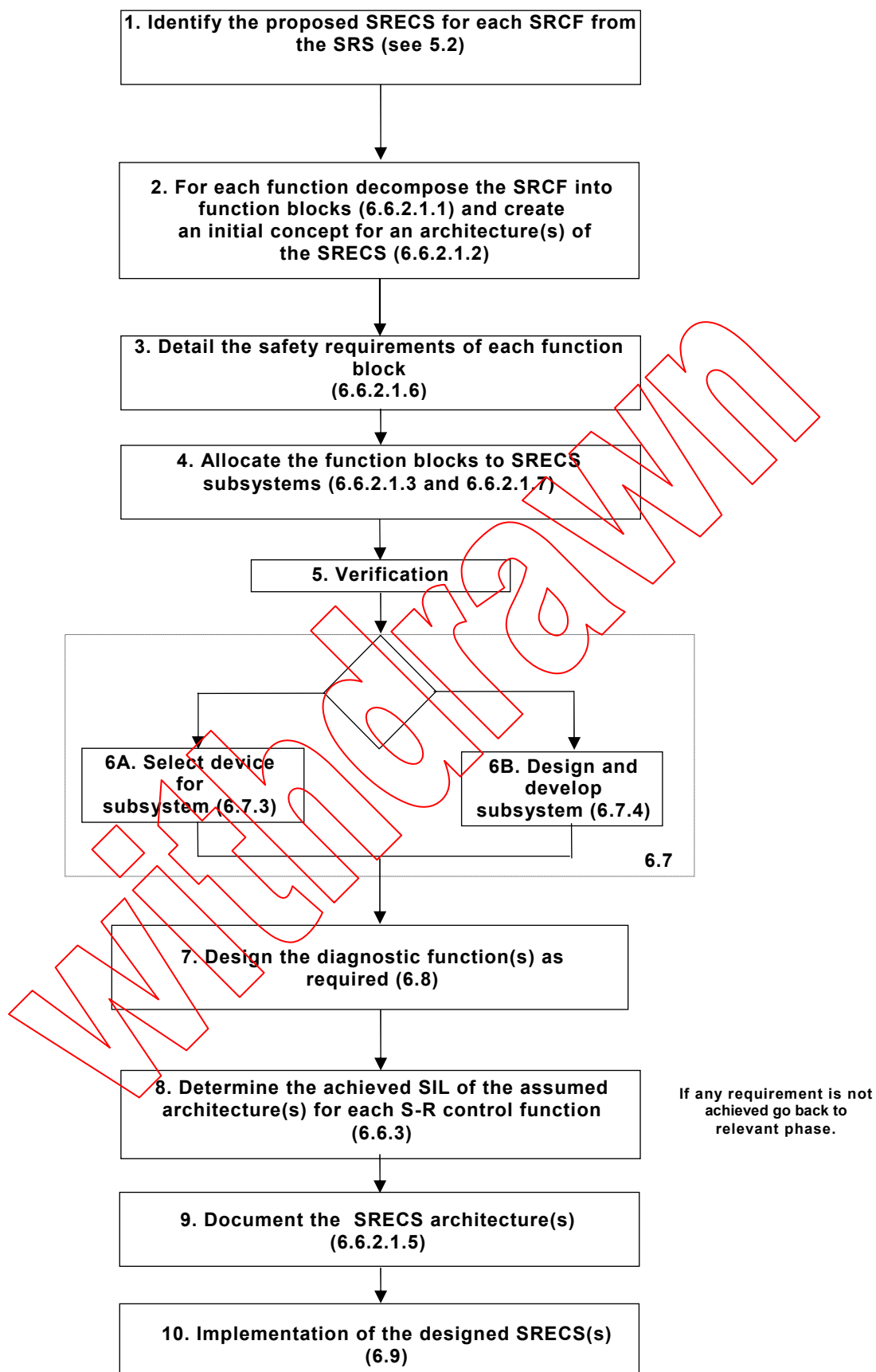


Figure 2 – Workflow of the SRECS design and development process

6.6.2.1.3 Each function block shall be allocated to a subsystem within the architecture of the SRECS. More than one function block may be allocated to one subsystem.

6.6.2.1.4 Each subsystem and the function blocks allocated to it shall be clearly identified.

6.6.2.1.5 The architecture shall be documented describing its subsystems and their interrelationship.

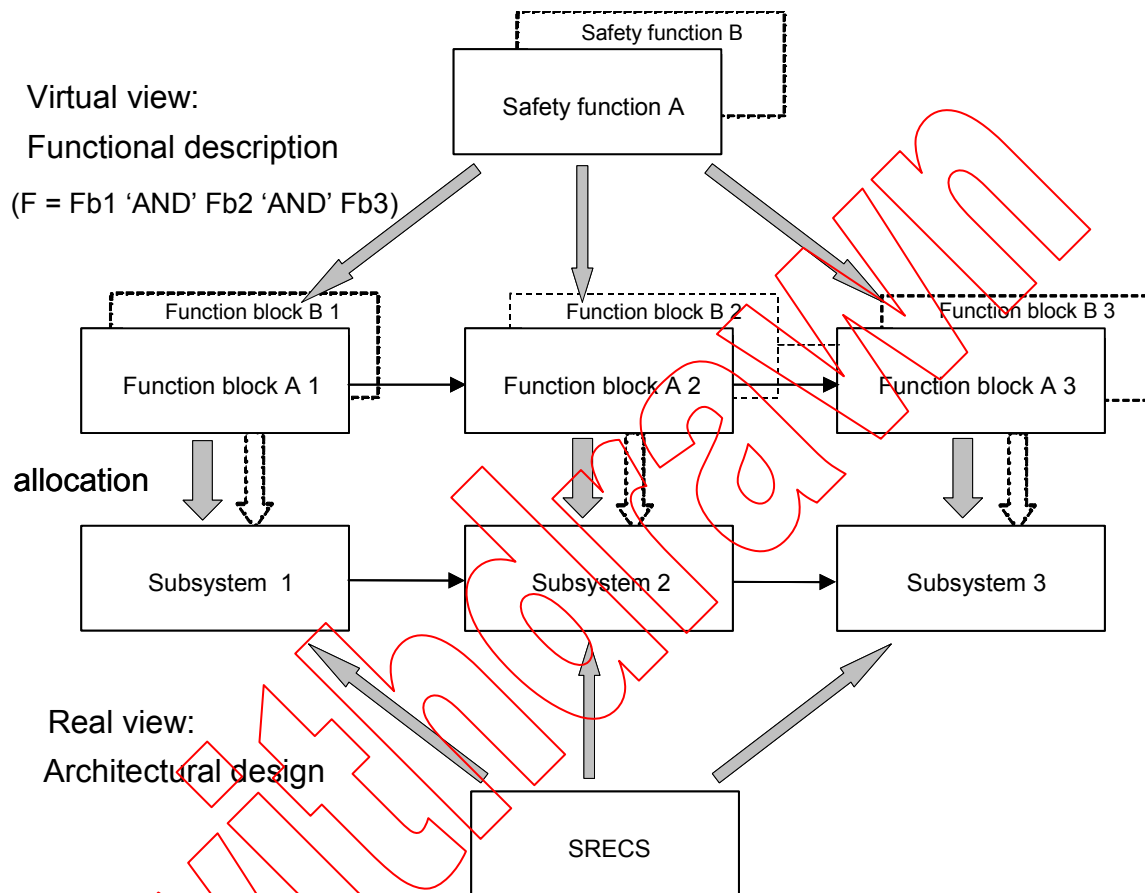


Figure 3 – Allocation of safety requirements of the function blocks to subsystems (see 6.6.2.1.1)

6.6.2.1.6 The safety requirements for each function block shall be as specified in the safety requirements specification of the corresponding SRCF in terms of

- functional requirements (e.g. input information, internal operation (logic) and output of the function block);
- safety integrity requirements.

6.6.2.1.7 The safety requirements for a subsystem shall be those of the function block(s) allocated to it. If more than one function block is allocated to a subsystem, then the highest integrity requirement applies (see 6.6.3). These requirements shall be documented as the subsystem safety requirements specification.

6.6.3 Requirements for the estimation of the safety integrity achieved by a SRECS

6.6.3.1 General

The SIL that can be achieved by the SRECS shall be considered separately for each SRCF to be performed by the SRECS.

The SIL that can be achieved by the SRECS shall be determined from the probability of dangerous random hardware failure, architectural constraints, and systematic safety integrity of the subsystems that comprise the SRECS. The SIL that is achieved is less than or equal to the lowest value of the SILCLs of any of the subsystems for systematic safety integrity and architectural constraints.

6.6.3.2 Hardware safety integrity

6.6.3.2.1 The probability of dangerous failure of each SRCF due to dangerous random hardware failures shall be equal to or less than the target failure value as specified in the safety requirements specification.

NOTE The target values associated with SILs are given in Table 3.

6.6.3.2.2 The probability of dangerous failure of each SRCF due to dangerous random hardware failures shall be estimated taking into account:

- a) the architecture of the SRECS as it relates to each SRCF under consideration;

NOTE This involves deciding which failure modes of the subsystems are in a series configuration (i.e. any failure causes failure of the relevant SRCF to be carried out) and which are in a parallel (redundant) configuration (i.e. co-incident failures are necessary for the relevant SRCF to fail).

- b) the estimated rate of failure of each subsystem to perform its allocated function block(s) in any modes which would cause a dangerous failure of the SRECS.

6.6.3.2.3 The estimation of the probability of dangerous failure shall be based on the probability of dangerous random hardware failure of each relevant subsystem as derived using the information required in 6.7.2.2 including, where appropriate 6.7.2.2 (k), for digital data communication processes between subsystems. The probability of dangerous random hardware failure of the SRECS is the sum of the probabilities of dangerous random hardware failure of all subsystems involved in the performance of the SRCF and shall include, where appropriate, the probability of dangerous transmission errors for digital data communication processes:

$$PFH_D = PFH_{D1} + \dots + PFH_{Dn} + P_{TE}$$

NOTE 1 This approach is based on the definition of a function block which states that a failure of any function block will result in a failure of the SRCF (see 3.2.16).

NOTE 2 Interconnections other than digital data communication are considered to be a part of the subsystems.

6.6.3.3 Architectural constraints

The SIL achieved by the SRECS according to the architectural constraints is less than or equal to the lowest SILCL of any subsystem (see 6.7.6) involved in the performance of the SRCF.

NOTE For example, a SRECS comprises two series connected subsystems (subsystem 1 and subsystem 2) where the SFF and fault tolerance of each subsystem are assumed to be as shown in Table 4. The estimated PFH_D for the SRECS is 8×10^{-8} , which corresponds to SIL 3. However, according to Table 5 the architectural constraint of subsystem 2 limits the SIL that can be achieved by the SRECS to SIL 2.

Table 4 – Characteristics of subsystems 1 and 2 used in this example (see Note above)

Subsystem	Hardware fault tolerance	SFF	SIL claim limit according to architectural constraints (see Table 5)
1	1	95 %	SIL 3
2	1	80 %	SIL 2

6.6.3.4 Systematic safety integrity

The SIL achieved by the SRECS is less than or equal to the lowest SILCL of any subsystem involved in the performance of the SRCF.

NOTE The measures described in 6.7.9 give a SILCL of up to SIL 3 for systematic safety integrity of a subsystem realised according to 6.7.4.

6.7 Realisation of subsystems

6.7.1 Objective

The objective is to realise a subsystem that fulfils all safety requirements of the allocated function blocks (see Figure 3). Two approaches are considered.

- selection of a device that is sufficient to fulfil the requirements for that subsystem, i.e. it shall fulfil the safety requirements specification of each of its allocated function blocks and the requirements of this standard; or
- design and development of a subsystem by combining function block elements and specifying how they are arranged and how they interact.

6.7.2 General requirements for subsystem realisation

6.7.2.1 The subsystem shall be realised by either selection (see 6.7.3) or design (see 6.7.4) in accordance with its safety requirements specification (see 6.6.2.1.7), taking into account all the requirements of 6.2. Subsystem(s) incorporating complex components shall comply with IEC 61508-2 and IEC 61508-3 as appropriate for the required SIL.

EXCEPTION: Where a subsystem design includes a complex component as a subsystem element, 6.7.4.2.3 is applicable.

6.7.2.2 The following information shall be available for each subsystem:

- a) a functional specification of those functions and interfaces of the subsystem which can be used by SRCFs;
- b) the estimated rates of failure (due to random hardware failures) declared in any modes which could cause a dangerous failure of the SRECS;

NOTE 1 For electromechanical subsystems, the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer and the duty cycle (see 5.2.3). This information should be based upon a B10 value (i.e. the expected time at which 10% of the population will fail). See also IEC 61810-2¹.

c) constraints on the subsystem for

- the environment and operating conditions which should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures; and

¹ To be published.

- the lifetime of the subsystem which should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures;
- d) any test and/or maintenance requirements;
- e) the diagnostic coverage and the diagnostic test interval (when required, see Note 2);

NOTE 2 Item e) relates to diagnostic functions that are external to the subsystem. This information is only required when credit is claimed in the reliability model of the SRECS for the action of the diagnostic functions performed in the subsystem.

- f) any additional information (e.g. repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics.

NOTE 3 Items b) to f) are needed to allow the probability of failure per hour of the SRCF to be estimated.

- g) the SILCL due to architectural constraints (see 6.7.6) or:
 - all information which is necessary to enable the derivation of the safe failure fraction (SFF) of the subsystem as applied in the SRECS; and

NOTE 4 The required information is the possible failure modes of the subsystem. Based on the failure modes of the subsystem, it can be decided whether the subsystem failure causes a safe or a dangerous failure of the SRECS.

NOTE 5 For details on estimation of the SFF see 6.7.7.

- the hardware fault tolerance of the subsystem;
- h) any limits on the application of the subsystem which should be observed in order to avoid systematic failures;
- i) the highest safety integrity level that can be claimed for a SRCF which uses the subsystem on the basis of:
 - measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software of the subsystem;
 - the design features that make the subsystem tolerant against systematic faults.

NOTE 6 Items h) and i) are needed to determine the highest safety integrity level that can be claimed for a SRCF according to the architectural constraints. Also, these items can be used to provide a link (see Tables 4 and 5) to the category requirements of ISO 13849-1 in terms of both fault detection and hardware fault tolerance.

- j) any information which is required to identify the hardware and software configuration of the subsystem in order to enable the configuration management of a SRECS in accordance with 6.11.3.2;
- k) the probability of dangerous transmission errors for digital data communication processes, where applicable.

6.7.3 Requirements for selection of existing (pre-designed) subsystems

6.7.3.1 Where a supplier provides a subsystem for a specific SRCF referenced in the safety requirements specification, such a pre-designed subsystem may be selected instead of a custom design providing that it satisfies the safety requirements specification for the subsystem, 6.4.3 and 6.7.3.2 or 6.7.3.3.

6.7.3.2 Subsystems incorporating complex components shall comply with IEC 61508-2 and IEC 61508-3 as appropriate for the required SIL.

EXCEPTION: Where a subsystem design includes a complex component as a subsystem element, 6.7.4.2.3 is applicable.

6.7.3.3 Subsystems comprising low complexity components only shall comply with 6.7.4.4.1, 6.7.6.2, 6.7.6.3, 6.7.7, 6.7.8 and 6.8 of this standard.

6.7.4 Design and development of subsystems

6.7.4.1 Objectives

6.7.4.1.1 The first objective is to design a subsystem that fulfils the safety requirements of the allocated function block(s).

6.7.4.1.2 The second objective is to create an architecture in terms of subsystem elements that work together in combination to fulfil the functional and safety integrity requirements of all function blocks allocated to the subsystem.

6.7.4.2 General requirements

6.7.4.2.1 The subsystem shall be designed in accordance with its safety requirements specification.

6.7.4.2.2 The subsystem shall be such as to meet all of the requirements a) to c) as follows:

- a) the requirements for hardware safety integrity comprising:
 - the architectural constraints on hardware safety integrity (see 6.7.6), and
 - the requirements for the probability of dangerous random hardware failures (see 6.7.8);
- b) the requirements for systematic safety integrity comprising:
 - the requirements for the avoidance of failures (see 6.7.9.1), and the requirements for the control of systematic faults (see 6.7.9.2), or
 - evidence that the equipment is 'proven-in-use'. In this case, the subsystem shall fulfil the relevant requirements of IEC 61508-2 (see IEC 61508-2, 7.4.7.5 to 7.4.7.12).
- c) the requirements for subsystem behaviour on detection of a fault (fault reaction)(see 6.3).

6.7.4.2.3 Where the design of a subsystem incorporates a complex component (as a subsystem element) which satisfies all relevant requirements of IEC 61508-2 and IEC 61508-3 in relation to the SILCL, it can be considered as a low complexity component in the context of a subsystem design since its relevant failure modes, behaviour on detection of a fault, rate of failure, and other safety-related information are known. Such components shall only be used in accordance with its specification and the relevant information for use provided by its supplier.

6.7.4.3 Subsystem design and development process

The subsystem design and development shall follow a clearly defined process that shall take into account all aspects covered by the process shown in Figure 4.

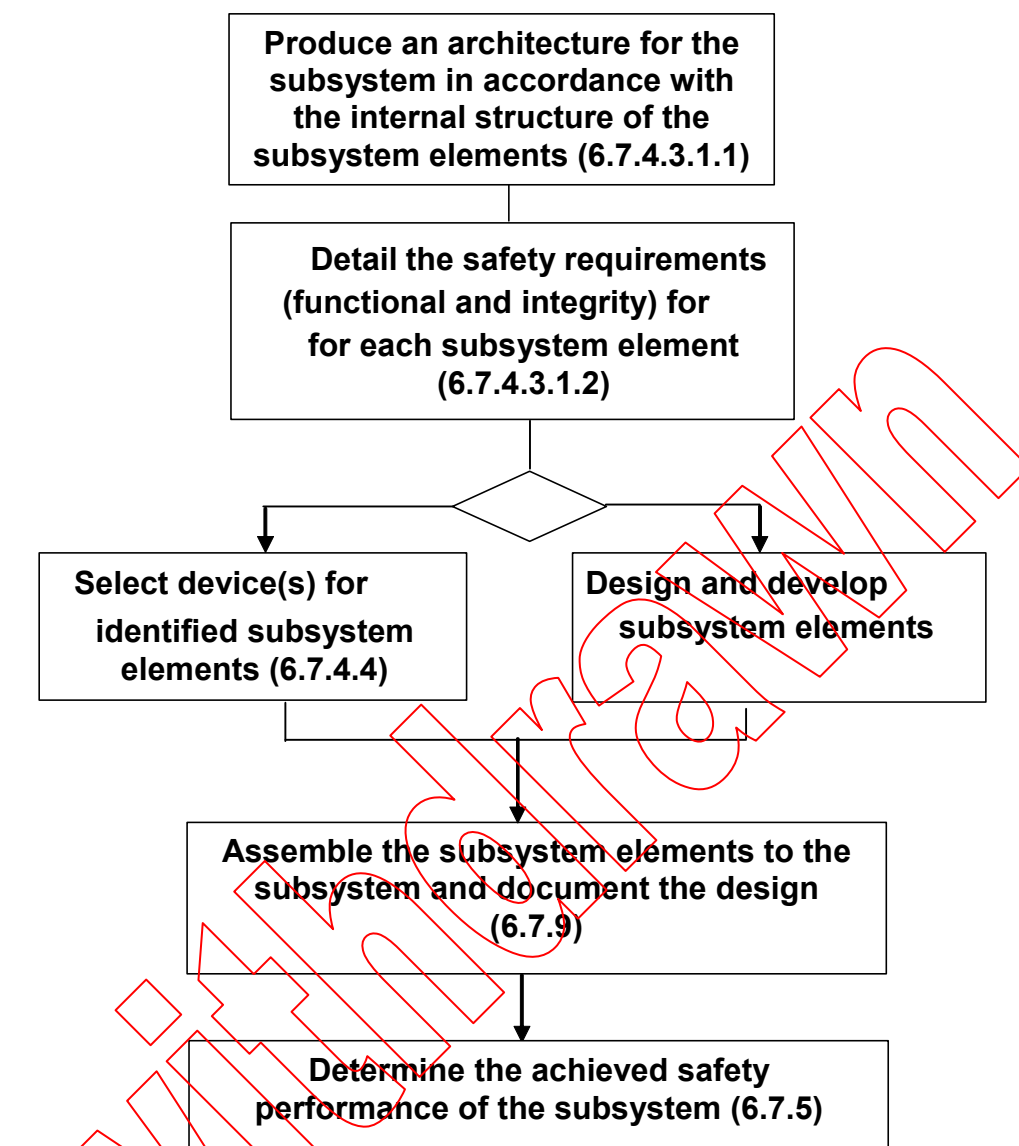


Figure 4 – Workflow for subsystem design and development (see box 6B of Figure 2)

6.7.4.3.1 Subsystem architecture design

6.7.4.3.1.1 During subsystem architecture design, the decomposition process should lead to a structure of function block elements that fully represent the functional requirements of the function block. This process should be applied down to that level which permits the functional requirements determined for each function block element to be allocated to subsystem elements (see example in Figure 5).

NOTE The workflow of the design process is shown in Figure 4.

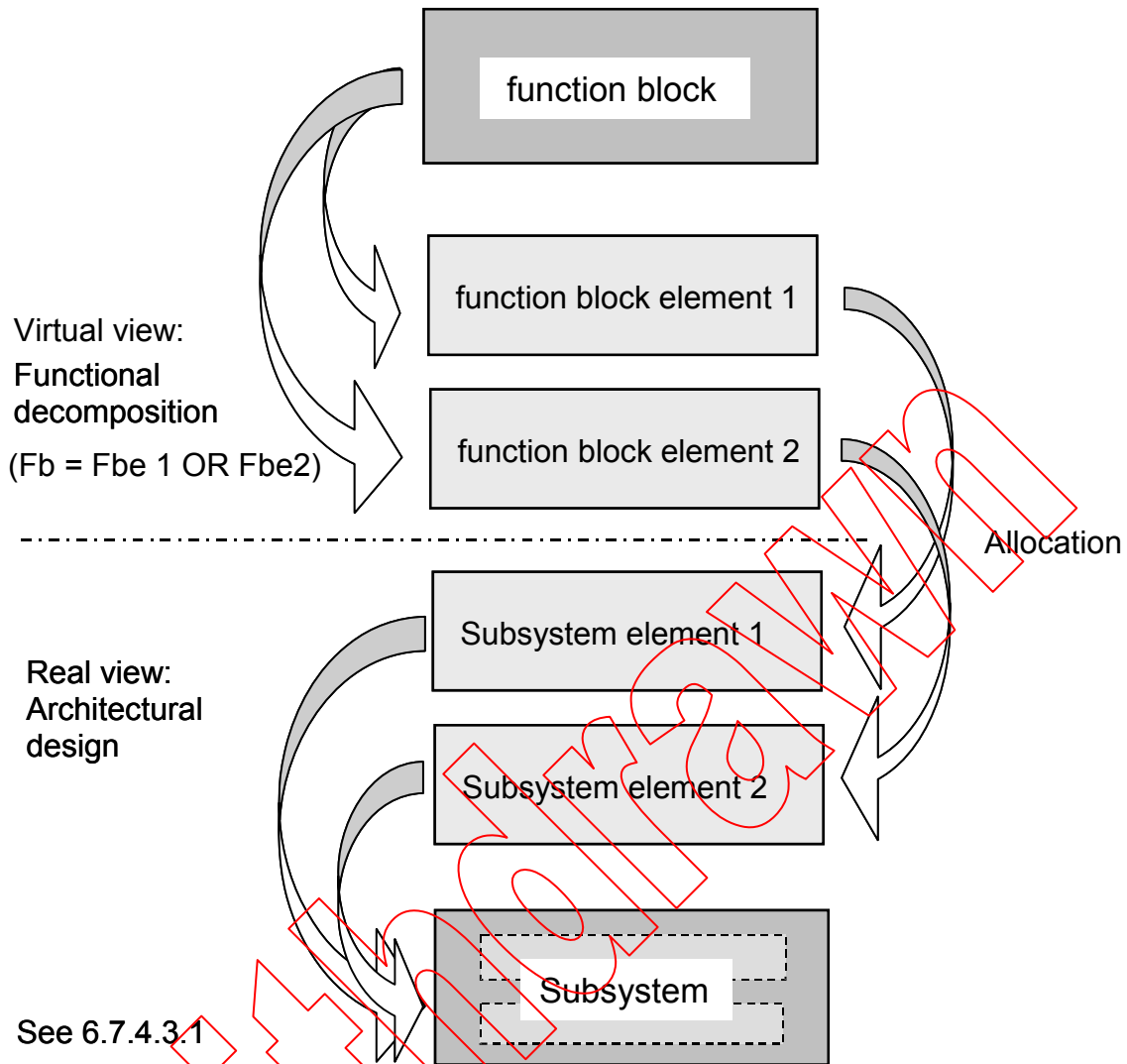


Figure 5 – Decomposition of a function block into redundant function block elements and their associated subsystem elements

6.7.4.3.1.2 The subsystem architecture shall be documented in terms of its elements and their interrelationships. Where necessary this shall also include information relating to function block elements that are allocated to subsystem elements.

6.7.4.4 Requirements for the selection and design of subsystem elements

6.7.4.4.1 Subsystem elements shall be suitable for their intended use and shall conform to relevant international standards where such exist.

6.7.4.4.2 The following information shall be available for each subsystem element:

- a) a functional specification of the subsystem element;
- b) specification of the interfaces of the subsystem element (e.g. electrical characteristics);

- c) each failure mode and its probability of occurrence, and, where relevant (e.g. complex components used in accordance with 6.7.4.2.3), the diagnostic coverage and probability of dangerous failure.

NOTE For electromechanical subsystems, the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer and the duty cycle of the application (see 5.2.3). This information should be based upon a B10 value (i.e. the expected time at which 10 % of the population will fail). See also IEC 61810-2².

- d) constraints on the subsystem element for
- the environment and operating conditions which should be observed in order to maintain the validity of the information given in item c); and
 - the lifetime of the subsystem element which should not be exceeded in order to maintain the validity of the information given in item (c);
- e) any periodic proof test and/or maintenance requirements;
- f) features that can contribute to diagnostics (e.g. mechanically linked contacts);
- g) any additional information (e.g. repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics;
- h) any limits on the application of the subsystem element which should be observed in order to avoid systematic failures;
- i) hardware fault tolerance.

6.7.5 Determination of the safety performance of the subsystem

The safety performance of a subsystem is characterized by the SILCL determined by its architectural constraints (6.7.6), its SILCL due to systematic integrity (6.7.9) and its probability of dangerous random hardware failure (6.7.8).

NOTE 1 The SILCL of a subsystem sets a limit for the maximum safety integrity level that can be claimed for a safety-related control function using this subsystem.

NOTE 2 Information about all three aspects is necessary to determine the SIL achieved by the safety-related control system implementing the allocated SRCF.

6.7.6 Architectural constraints on hardware safety integrity of subsystems

6.7.6.1 In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a SRCF is limited by the hardware fault tolerances and safe failure fractions of the subsystems that carry out that SRCF. Table 5 specifies the highest safety integrity level that can be claimed for a SRCF that uses a subsystem taking into account the hardware fault tolerance and safe failure fraction of that subsystem. The architectural constraints given in Table 5 shall be applied to each subsystem. With respect to these architectural constraints:

- a) a hardware fault tolerance of N means that $N+1$ faults could cause a loss of the SRCF. In determining the hardware fault tolerance, no account is taken of other measures that can control the effects of faults such as diagnostics; and
- b) where one fault directly leads to the occurrence of one or more subsequent faults, these shall be considered as a single fault;
- c) in determining hardware fault tolerance, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented (see also 6.7.7).

² To be published.

6.7.6.2 The architectural constraints of Table 5 shall apply to each subsystem implementing a function block of an SRCF.

6.7.6.3 A subsystem that comprises only a single subsystem element shall satisfy the requirements of Table 5. In particular, for such a subsystem that has a hardware fault tolerance of zero (i.e. $N = 0$) then a SFF of greater than 99 % shall be achieved by a SRECS diagnostic function(s).

NOTE This requirement is necessary to ensure an appropriate form of the architectural constraints is applied to subsystems that comprise only a single subsystem element in order to justify a SILCL of SIL 3.

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

Safe failure fraction	Hardware fault tolerance (see Note 1)		
	0	1	2
< 60 %	Not allowed (for exceptions see Note 3)	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3 (see Note 2)
≥ 99 %	SIL3	SIL3 (see Note 2)	SIL3 (see Note 2)

NOTE 1 A hardware fault tolerance of N means that $N+1$ faults could cause a loss of the safety-related control function.

NOTE 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1.

NOTE 3 See 6.7.6.4 or for subsystems where fault exclusions have been applied to faults that could lead to a dangerous failure, see 6.7.7.

6.7.6.4 Electromechanical subsystems, which have a safe failure fraction of less than 60 % and zero hardware fault tolerance, that use well-tried components (see Note) in accordance with ISO 13849-1:2006 Category 1 PLC shall be considered to achieve a SILCL of SIL1.

NOTE A well-tried component for a safety-related application is a component which has been:

- widely used in the past with successful results in similar applications, or
- made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

6.7.6.5 Where a subsystem is designed according to ISO 13849-1:1999 and validated according to ISO 13849-2:2003, the following relationship in the context of architectural constraints alone can be applied in accordance with Table 6. It is assumed that a subsystem with a particular category complying with ISO 13849-1:1999 has the associated hardware fault tolerance and safe failure fraction as indicated in Table 6.

NOTE To achieve a required SIL, it is also necessary to fulfil the requirements according to probability of dangerous failure and systematic safety integrity.

Table 6 – Architectural constraints: SILCL relating to categories

Category	Hardware fault tolerance	SFF	Maximum SIL claim limit according to architectural constraints
	It is assumed that subsystems with the stated category have the characteristics given below		
1	0	< 60 %	See Note 1
2	0	60 % – 90 %	SIL 1 (see Note 2)
3	1	< 60 %	SIL 1
	1	60 % – 90 %	SIL 2
4	>1	60 % – 90 %	SIL 3 (see Note 3)
	1	> 90 %	SIL 3 (see Note 4)

NOTE 1 Subsystems that have a SFF of <60% but are designed in accordance with Category 1 of ISO 13849-1:1999 and validated in accordance with ISO 13849-2:2003 are assumed to achieve a SILCL of SIL1.

NOTE 2 The case for Category 2 where SFF is > 90 % is assumed not to be achieved by the design requirements of ISO 13849-1:1999.

NOTE 3 The diagnostic coverage is assumed to be less than 90 % for Category 4 subsystems where greater than single hardware fault tolerance (i.e. accumulated faults) is considered.

NOTE 4 Category 4 requires a SFF of more than 90 % but less than 99 % when single hardware fault tolerance is considered.

NOTE 5 Category B in accordance with ISO 13849-1:1999 is not considered sufficient to achieve SIL 1.

6.7.7 Estimation of safe failure fraction (SFF)

6.7.7.1 The SFF shall be estimated where it is required to determine the SILCL due to architectural constraints.

6.7.7.2 To estimate the SFF, an analysis (e.g. fault tree analysis, failure mode and effects analysis) of each subsystem shall be performed to determine all relevant faults and their corresponding failure modes. Whether a failure is a safe or a dangerous failure depends on the SRECS and the intended safety-related control functions, including fault reaction function. The probability of each failure mode shall be determined based on the probability of the associated fault(s) taking into account the intended use and may be derived from sources such as:

- dependable failure rate data collected from field experience by the manufacturer and relevant to the intended use;
- component failure data from a recognised industry source (see references in Annex D) and relevant to the intended use;
- failure mode data given in Annex D;
- failure rate data derived from the results of testing and analysis.

EXCEPTION: For a subsystem with a hardware fault tolerance of zero and where fault exclusions have been applied to faults that could lead to a dangerous failure, then the SILCL due to architectural constraints of that subsystem is constrained to a maximum of SIL 2.

6.7.7.3 The use of fault exclusions shall be justified (e.g. by analysis) and documented.

NOTE It is permissible to exclude faults in accordance with 3.3 and D.5 of ISO 13849-2:2003.

6.7.8 Requirements for the probability of dangerous random hardware failures of subsystems

6.7.8.1 General requirements

6.7.8.1.1 The probability of dangerous random hardware failure shall be equal to or less than the target failure value as specified in the subsystem safety requirements specification (see 6.6.2.1.7).

6.7.8.1.2 The probability of dangerous failure of each subsystem due to random hardware failures to perform the allocated function blocks shall be estimated taking into account:

- a) the architecture of the subsystem as it relates to the allocated function blocks under consideration;

NOTE 1 This involves deciding whether there is hardware fault tolerance or not.

- b) the rate of failure of each subsystem element in any modes which would cause a dangerous failure of the subsystem but which are detected by diagnostic tests (see 6.3);
- c) the rate of failure of each subsystem element in any modes which would cause a dangerous failure of the subsystem which are undetected by the diagnostic tests (see 6.3);
- d) the susceptibility of the subsystem to common cause failures which would cause a dangerous failure of the subsystem (see Notes 2 and 3);

NOTE 2 Where comparison of redundant components is used for fault detection, failure of the fault detection means can occur when the redundant components fail at the same time in the same mode. This can occur due to a common cause referred to as a common cause failure (CCF) that is expressed as a beta (β) factor.

A simplified approach to estimate the susceptibility to common cause failures is given in 6.7.8.3. For further guidance on quantifying the effect of hardware-related common cause failures, see also IEC 61508-6, Annex D.

- e) the diagnostic coverage of the diagnostic tests (see 3.2.38) and the associated diagnostic test interval;
- f) the intervals at which proof tests are undertaken to reveal dangerous faults which are undetected by diagnostic tests and/or the mission time of the subsystem element(s) which should not be exceeded in order to maintain the validity of the information given in items b) and c);
- g) the repair times for detected faults where the subsystem is designed for online repair.

NOTE 3 The maximum repair time will constitute one part of the time to restoration (see IEC 191-10-05), including also the time taken to detect a fault and any time period during which repair is not possible (see IEC 61508-6, Annex B for an example of how the mean time to restoration can be used to calculate the probability of failure). For situations where the repair can only be carried out during a specific period of time, while the machine is shut down and in a safe state, it is particularly important that full account is taken of the time period when no repair can be carried out, especially when this is relatively large.

NOTE 4 A simplified approach for the estimation of the probability of dangerous random hardware failure of subsystems is given in 6.7.8.2. Other methods are available and the most appropriate method will depend on the circumstances. Available methods include:

- a) fault tree analysis (see B.6.6.5 of IEC 61508-7 and IEC 61025);
- b) Markov models (see C.6.4 of IEC 61508-7 and IEC 61165-13);
- c) reliability block diagrams (see C.6.5 of IEC 61508-7).

NOTE 5 Failures due to common cause effects and data communication processes can result from effects other than actual failures of hardware components (e.g. electromagnetic interference, software errors, etc.). See 6.7.9.

6.7.8.1.3 For subsystems or subsystem elements where the probability of failure is given in relation to a number of operating cycles, these values shall be transformed into time-related values by using the specified duty cycle for the relevant SRCFs (see 5.2.3).

6.7.8.1.4 The diagnostic test interval of any subsystem having a hardware fault tolerance of more than zero shall be such as to enable the subsystem to meet the requirement for the probability of random hardware failure (see 6.3.1).

NOTE This diagnostic test interval should be such that a fault is detected before the occurrence of a subsequent fault that may lead to dangerous failure of the subsystem and exceeds the target failure measure.

6.7.8.1.5 The diagnostic test interval of any subsystem having a hardware fault tolerance of zero shall be such that the requirements of 6.3.2 are fulfilled.

6.7.8.1.6 Where a low complexity subsystem is designed according to ISO 13849-1:1999 and validated according to ISO 13849-2:2003 and also meets the requirements for architectural constraints (see 6.7.6) and systematic safety integrity (see 6.7.9), the threshold values of probability of dangerous failure (PFH_D) given in Table 7 can be used to estimate the hardware safety integrity (see 6.6.3.2).

Table 7 – Probability of dangerous failure

Category	Hardware fault tolerance	DC	PFH_D threshold values (per hour) that can be claimed for the subsystem
	It is assumed that subsystems with the stated category have the characteristics given below		PFH_D (MTTF _{subsystem} , T _{test} , DC) (See Note 1)
1	0	0 %	To be provided by supplier or use generic data (see Annex D)
2	0	60 % – 90 %	$\geq 10^{-6}$
3	1	60 % – 90 %	$\geq 2 \times 10^{-7}$
4	>1	60 % – 90 %	$\geq 3 \times 10^{-8}$
	1	> 90 %	$\geq 3 \times 10^{-8}$

NOTE 1 The PFH_D threshold value is a function of the subsystem MTTF (to be derived by the subsystem manufacturer or from relevant component data handbooks), test/check cycle time as specified in the safety requirements specification (this information is also required for subsystem validation in accordance with ISO 13849-2:2003, 3.5) and the diagnostic coverage as shown in this table (these values are based on the requirements of the categories described in ISO 13849-1:1999).

NOTE 2 Category B in accordance with ISO 13849-1:1999 cannot be considered sufficient to achieve SIL 1.

6.7.8.2 Simplified approach for the estimation of probability of dangerous random hardware failures of subsystems

6.7.8.2.1 General

This subclause describes a simplified approach to the estimation of probability of dangerous random hardware failures for a number of basic subsystem architectures and gives formulae that can be used for subsystems assembled from either low complexity subsystem elements or complex subsystem elements. The formulae are in themselves a simplification of reliability analysis theory and are intended to provide estimates that are biased towards the safe direction. The precondition for the validity for all formulae given in this subclause is that $1 \gg \lambda \times T_1$, where T_1 is the smaller of the proof test interval or the lifetime, and the subsystem is operating in the “high demand or continuous mode” (see 3.2.27). See also 6.8.6.

NOTE 1 The results that are obtained represent a limitation upon probability of dangerous random hardware failures of subsystems and where this is unacceptable, it is possible to apply more accurate modelling techniques (see 6.7.8.1.1).

NOTE 2 For equations (A) to (D) given in 6.7.8.2 constant and sufficiently low ($1 \gg \lambda \times T$) failure rates (λ) of the subsystem elements are assumed (this means that the mean time to dangerous failure has to be much greater than the proof test interval or the lifetime of the subsystem). Therefore, the following basic equations can be used:

- $\lambda = 1/\text{MTTF}$, where MTTF is expressed in hours.

For electromechanical devices the failure rate is determined using the B_{10} value and the number of operating cycles C (expressed as the number of operating cycles per hour) of the application as specified (see 5.2.3).

- $\lambda = 0,1 \times C/B_{10}$.

NOTE 3 Terms used are as follows:

- $\lambda = \lambda_S + \lambda_D$; where λ_S is the rate of safe failure and λ_D is the rate of dangerous failure.
- $PFH_D = \lambda_D \times 1h$; average probability of dangerous failure within one hour.
- T_2 : diagnostic test interval.
- T_1 : proof test interval or lifetime whichever is the smaller.

6.7.8.2.2 Basic subsystem architecture A: zero fault tolerance without a diagnostic function

In this architecture, any dangerous failure of a subsystem element causes a failure of the SRCF. For architecture A, the probability of dangerous failure of the subsystem is the sum of the probabilities of dangerous failure of all subsystems elements:

$$\lambda_{DssA} = \lambda_{De1} + \dots + \lambda_{Den} \quad (A)$$

$$PFH_{DssA} = \lambda_{DssA} \times 1h$$

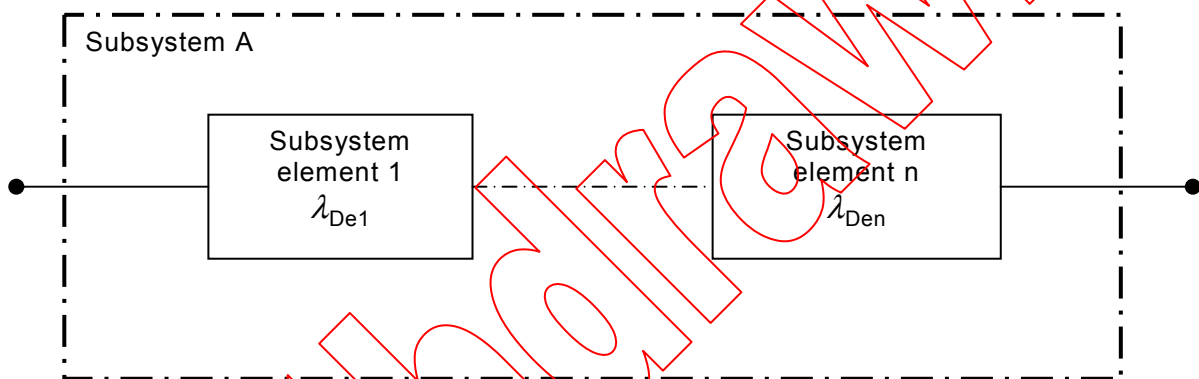


Figure 6 – Subsystem A logical representation

NOTE Figure 6 is a logical representation of the subsystem A architecture and should not be interpreted as its physical implementation.

6.7.8.2.3 Basic subsystem architecture B: single fault tolerance without a diagnostic function

This architecture is such that a single failure of any subsystem element does not cause a loss of the SRCF. Thus, there would have to be a dangerous failure in more than one element before failure of the SRCF can occur. For architecture B, the probability of dangerous failure of the subsystem is:

$$\lambda_{DssB} = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2 \quad (B)$$

$$PFH_{DssB} = \lambda_{DssB} \times 1h$$

where

T_1 is the proof test interval or lifetime whichever is the smaller.

β is the susceptibility to common cause failures.

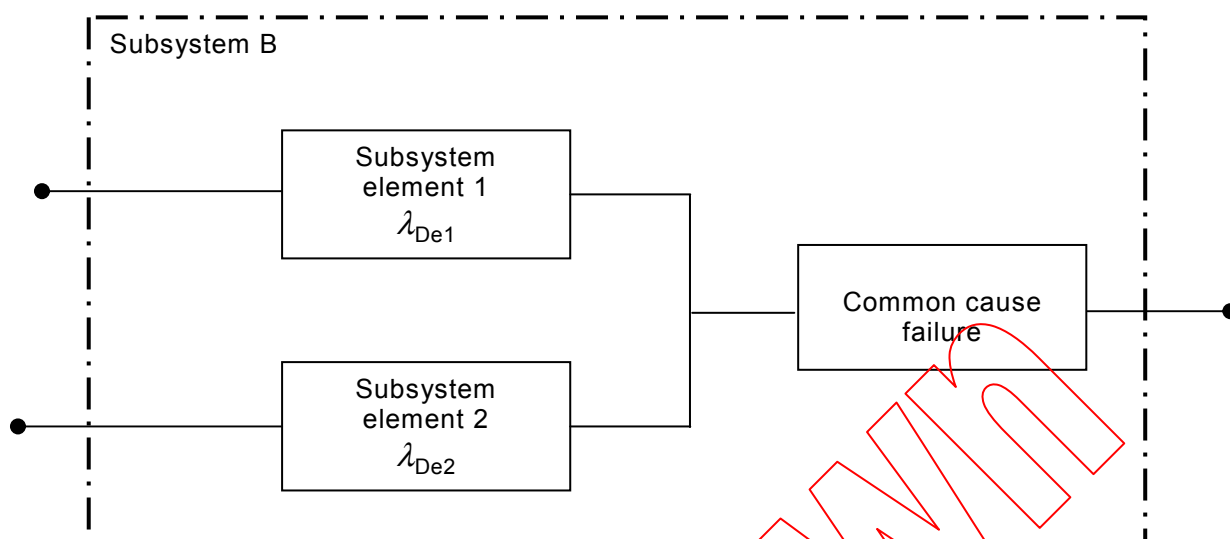


Figure 7 – Subsystem B logical representation

NOTE Figure 7 is a logical representation of the subsystem B architecture and should not be interpreted as its physical implementation.

6.7.8.2.4 Basic subsystem architecture C: zero fault tolerance with a diagnostic function

Any undetected dangerous fault of the subsystem element leads to a dangerous failure of the SRCF. Where a fault of a subsystem element is detected, the diagnostic function(s) initiates a fault reaction function (see 6.3.2). For architecture C, the probability of dangerous failure of the subsystem is:

$$\lambda_{DssC} = \lambda_{De1}(1 - DC_1) + \dots + \lambda_{Den}(1 - DC_n) \quad (C)$$

$$PFH_{DssC} = \lambda_{DssC} \times Ih$$

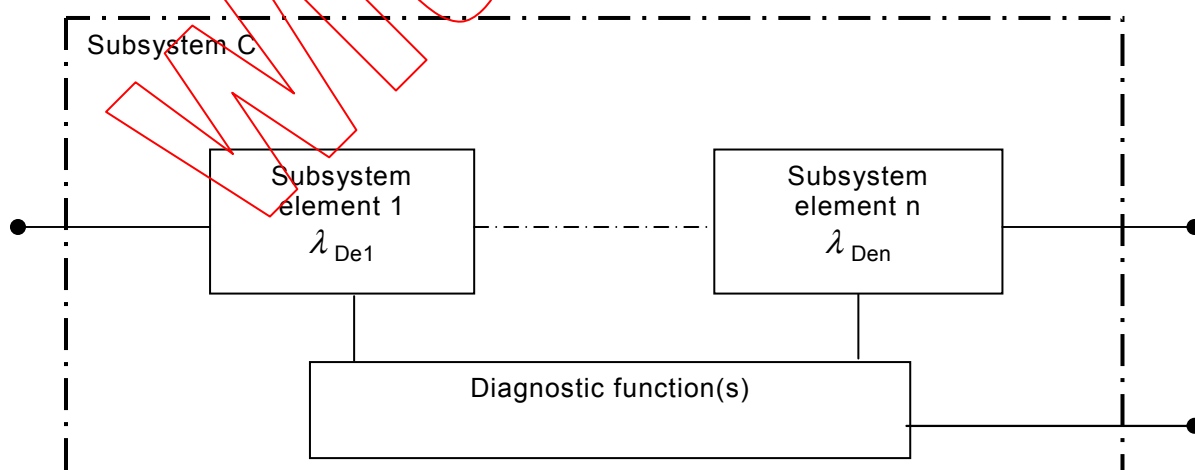


Figure 8 – Subsystem C logical representation

NOTE Figure 8 is a logical representation of the subsystem C architecture and should not be interpreted as its physical implementation. The diagnostic function shown may be carried out by

- the subsystem which requires diagnostics; or
- other subsystems of the SRECS; or
- subsystems not involved in the performance of the safety-related control function.

6.7.8.2.5 Basic subsystem architecture D: single fault tolerance with a diagnostic function(s)

This architecture is such that a single failure of any subsystem element does not cause a loss of the SRCF, where

T_2 is the diagnostic test interval;

T_1 is the proof test interval or lifetime whichever is the smaller.

β is the susceptibility to common cause failures; $\lambda_D = \lambda_{DD} + \lambda_{DU}$; where λ_{DD} is the rate of detectable dangerous failures and λ_{DU} is the rate of undetectable dangerous failure.

$$\lambda_{DD} = \lambda_D \times DC$$

$$\lambda_{DU} = \lambda_D \times (1 - DC)$$

For subsystem elements of different design:

λ_{De1} is the dangerous failure rate of subsystem element 1;

DC_1 is the diagnostic coverage of subsystem element 1;

λ_{De2} is the dangerous failure rate of subsystem element 2;

DC_2 is the diagnostic coverage of subsystem element 2.

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)] \times T_2/2 + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)] \times T_1/2 \} + \beta \times (\lambda_{De1} + \lambda_{De2})/2 \quad (D.1)$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

For subsystem elements of the same design:

λ_{De} is the dangerous failure rate of subsystem element 1 or 2;

DC is the diagnostic coverage of subsystem element 1 or 2.

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1 - DC)] \times T_1 \} + \beta \times \lambda_{De} \quad (D.2)$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$