



BSI Standards Publication

Safety of machinery — Functional safety of safety-related control systems

National foreword

This British Standard is the UK implementation of EN IEC 62061:2021+A1:2024. It is identical to IEC 62061:2021, incorporating amendment 1:2024. It supersedes BS EN IEC 62061:2021, which is withdrawn.

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

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

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication has been prepared under a mandate given to the European Standards Organizations by the European Commission and the European Free Trade Association. It is intended to support requirements of the EU legislation detailed in the European Foreword. A European Annex, usually Annex ZA or ZZ, describes how this publication relates to that EU legislation.

For the Great Britain market (England, Scotland and Wales), if UK Government has designated this publication for conformity with UKCA marking (or similar) legislation, it may contain an additional National Annex. Where such a National Annex exists, it shows the correlation between this publication and the relevant UK legislation. If there is no National Annex of this kind, the relevant Annex ZA or ZZ in the body of the European text will indicate the relationship to UK regulation applicable in Great Britain. References to EU legislation may need to be read in accordance with the UK designation and the applicable UK law. Further information on designated standards can be found at www.bsigroup.com/standardsandregulation.

For the Northern Ireland market, UK law will continue to implement relevant EU law subject to periodic confirmation. Therefore Annex ZA/ZZ in the European text, and references to EU legislation, are still valid for this market.

UK Government is responsible for legislation. For information on legislation and policies relating to that legislation, consult the relevant pages of www.gov.uk.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 19419 7

ICS 13.110; 25.040.99; 29.020

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2021.

Amendments/corrigenda issued since publication

Date	Text affected
30 June 2024	Implementation of IEC amendment 1:2024 with CENELEC endorsement A1:2024

English Version

Safety of machinery - Functional safety of safety-related control
systems
(IEC 62061:2021)

Sécurité des machines - Sécurité fonctionnelle des
systèmes de commande relatifs à la sécurité
(IEC 62061:2021)

Sicherheit von Maschinen - Funktionale Sicherheit
sicherheitsbezogener Steuerungssysteme
(IEC 62061:2021)

This European Standard was approved by CENELEC on 2021-04-26. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 44/885/FDIS, future edition 2 of IEC 62061, prepared by IEC/TC 44 "Safety of machinery - Electrotechnical aspects" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62061:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2022-01-26 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2024-04-26 document have to be withdrawn

This document supersedes EN 62061:2005 and all of its amendments and corrigenda (if any).

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

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 62061:2021 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60068 (series)	NOTE	Harmonized as EN 60068 (series)
IEC 60364-4-41:2005	NOTE	Harmonized as HD 60364-4-41:2017
IEC 60529	NOTE	Harmonized as EN 60529
IEC 60721 (series)	NOTE	Harmonized as EN 60721-3-9:1993/A1 (series)
IEC 60812	NOTE	Harmonized as EN IEC 60812
IEC 60947-4-1:2018	NOTE	Harmonized as EN IEC 60947-4-1:2019 (not modified)
IEC 60947-5-1	NOTE	Harmonized as EN 60947-5-1
IEC 60947-5-3	NOTE	Harmonized as EN 60947-5-3
IEC 60947-5-5	NOTE	Harmonized as EN 60947-5-5
IEC 60947-5-8	NOTE	Harmonized as EN IEC 60947-5-8
IEC 61000-6-7	NOTE	Harmonized as EN 61000-6-7
IEC 61025:2006	NOTE	Harmonized as EN 61025:2007 (not modified)
IEC 61131-2:2017	NOTE	Harmonized as EN 61131-2:2017 (not modified) to be published
IEC 61131-6:2012	NOTE	Harmonized as EN 61131-6:2012 (not modified)

IEC 61140:2016	NOTE	Harmonized as EN 61140:2016 (not modified)
IEC 61165	NOTE	Harmonized as EN 61165
IEC 61204-7:2016	NOTE	Harmonized as EN IEC 61204-7:2018 (not modified)
IEC 61310 (series)	NOTE	Harmonized as EN 61310 (series)
IEC 61326-3-1	NOTE	Harmonized as EN 61326-3-1
IEC 61496 (series)	NOTE	Harmonized as EN IEC 61496 (series)
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified)
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified)
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified)
IEC 61508-7:2010	NOTE	Harmonized as EN 61508-7:2010 (not modified)
IEC 61511 (series)	NOTE	Harmonized as EN 61511 (series)
IEC 61511-1:2016	NOTE	Harmonized as EN 61511-1:2017 (not modified)
IEC 61511-1:2016/A1:2017	NOTE	Harmonized as EN 61511-1:2017/A1:2017 (not modified)
IEC 61511-3:2016	NOTE	Harmonized as EN 61511-3:2017 (not modified)
IEC 61649	NOTE	Harmonized as EN 61649
IEC 61709:2017	NOTE	Harmonized as EN 61709:2017 (not modified)
IEC 61784-3 (series)	NOTE	Harmonized as EN 61784-3 (series)
IEC 61784-3:2016	NOTE	Harmonized as EN 61784-3:2016 (not modified)
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2
IEC 61810 (series)	NOTE	Harmonized as EN 61810 (series)
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)
IEC 62477 (series)	NOTE	Harmonized as EN IEC 62477 (series)
IEC 62502	NOTE	Harmonized as EN 62502
ISO/IEC 27001:2013	NOTE	Harmonized as EN ISO/IEC 27001:2017 (not modified)
ISO 4413:2010	NOTE	Harmonized as EN ISO 4413:2010 (not modified)
ISO 4414:2010	NOTE	Harmonized as EN ISO 4414:2010 (not modified)
ISO 11161:2007	NOTE	Harmonized as EN ISO 11161:2007 (not modified)
ISO 13850:2015	NOTE	Harmonized as EN ISO 13850:2015 (not modified)
ISO 13851:2019	NOTE	Harmonized as EN ISO 13851:2019 (not modified)
ISO 13855:2010	NOTE	Harmonized as EN ISO 13855:2010 (not modified)
ISO 14118:2017	NOTE	Harmonized as EN ISO 14118:2018 (not modified)
ISO 14119:2013	NOTE	Harmonized as EN ISO 14119:2013 (not modified)
ISO/TR 22100-4:2018	NOTE	Harmonized as CEN ISO/TR 22100-4:2020 (not modified)

European foreword to amendment A1

The text of document 44/1020/FDIS, future Amendment 1 of IEC 62061, prepared by IEC/TC 44 "Safety of machinery - Electrotechnical aspects" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62061:2021/A1:2024.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2024-12-28 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2027-06-28 document have to be withdrawn

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

This document has been prepared under a standardization request addressed to CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN and CENELEC websites.

Endorsement notice

The text of the International Standard IEC 62061:2021/AMD1:2024 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

- EC 61784-3:2021 NOTE Approved as EN IEC 61784-3:2021 (not modified)
- IEC/TS 63074:2023 NOTE Approved as CLC IEC/TS 63074:2024 (not modified)
- IEC/TS 63394:2023 NOTE Approved as CLC IEC/TS 63394:2024 (not modified)

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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

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

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

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60204-1 (mod) + AMD1	2016 2021	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	EN 60204-1 -	2018 -
IEC 61000-1-2	2016	Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena	EN 61000-1-2	2016
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements	IEC 61508-1	2010
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010
IEC 61508-5	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels	EN 61508-5	2010
IEC 61508-6	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	EN 61508-6	2010

EN IEC 62061:2021+A1:2024 (E)

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61508-7	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures	EN 61508-7	2010
ISO 12100	2010	Safety of machinery - General principles for design - Risk assessment and risk reduction	EN ISO 12100	2010
ISO 13849-1	2023	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	2023
ISO 13849-2	2012	Safety of machinery - Safety-related parts of control systems - Part 2: Validation	EN ISO 13849-2	2012

Annex ZZ (informative)

Relationship between this European standard and the essential requirements of Directive 2006/42/EC [2006 OJ L 157] aimed to be covered

This European standard has been prepared under a Commission's standardisation request "M/396" to provide one voluntary means of conforming to *essential* requirements of Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) [2006 OJ L 157].

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZZ.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Directive, and associated EFTA regulations.

Table ZZ.1 — Correspondence between this European standard and Annex 1 of Directive] 2006/42/EC [2006 OJ L 157]

The relevant Essential Requirements of Directive 2006/42/EC	Clause(s) / sub-clause(s) of this EN	Remarks / Notes
1.2.1	Clauses 4, 5, 6, 7, 8, 9.	
1.7.4.2 (e, g, i, r, s)	10.3	This subclause only deals with the instruction for safety functions

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	11
2 Normative references	12
3 Terms, definitions and abbreviations	13
3.1 Alphabetical list of definitions.....	13
3.2 Terms and definitions.....	15
3.3 Abbreviations.....	28
4 Design process of an SCS and management of functional safety.....	28
4.1 Objective	28
4.2 Design process	29
4.3 Management of functional safety using a functional safety plan	31
4.4 Configuration management	33
4.5 Modification	33
5 Specification of a safety function	34
5.1 Objective	34
5.2 Safety requirements specification (SRS).....	34
5.2.1 General	34
5.2.2 Information to be available.....	34
5.2.3 Functional requirements specification	35
5.2.4 Estimation of demand mode of operation	35
5.2.5 Safety integrity requirements specification.....	36
6 Design of an SCS	37
6.1 General.....	37
6.2 Subsystem architecture based on top down decomposition	37
6.3 Basic methodology – Use of subsystem	37
6.3.1 General	37
6.3.2 SCS decomposition	38
6.3.3 Sub-function allocation	39
6.3.4 Use of a pre-designed subsystem.....	39
6.4 Determination of safety integrity of the SCS.....	40
6.4.1 General	40
6.4.2 PFH.....	40
6.5 Requirements for systematic safety integrity of the SCS	41
6.5.1 Requirements for the avoidance of systematic hardware failures	41
6.5.2 Requirements for the control of systematic faults.....	42
6.6 Electromagnetic immunity	43
6.7 Software based manual parameterization.....	43
6.7.1 General	43
6.7.2 Influences on safety-related parameters	43
6.7.3 Requirements for software based manual parameterization	44
6.7.4 Verification of the parameterization tool.....	45
6.7.5 Performance of software based manual parameterization	45
6.8 Security aspects	45
6.9 Aspects of periodic testing	46
7 Design and development of a subsystem.....	46

7.1	General.....	46
7.2	Subsystem architecture design	47
7.3	Requirements for the selection and design of subsystem and subsystem elements	48
7.3.1	General	48
7.3.2	Systematic integrity	48
7.3.3	Fault consideration and fault exclusion	51
7.3.4	Failure rate of subsystem element	52
7.4	Architectural constraints of a subsystem	55
7.4.1	General	55
7.4.2	Estimation of safe failure fraction (<i>SFF</i>)	56
7.4.3	Behaviour (of the SCS) on detection of a fault in a subsystem	58
7.4.4	Realization of diagnostic functions	59
7.5	Subsystem design architectures.....	59
7.5.1	General	59
7.5.2	Basic subsystem architectures.....	60
7.5.3	Basic requirements	61
7.6	<i>PFH</i> of subsystems	62
7.6.1	General	62
7.6.2	Methods to estimate the <i>PFH</i> of a subsystem	62
7.6.3	Simplified approach to estimation of contribution of common cause failure (CCF).....	62
8	Software	62
8.1	General.....	62
8.2	Definition of software levels	63
8.3	Software – Level 1	64
8.3.1	Software safety lifecycle – SW level 1	64
8.3.2	Software design – SW level 1	65
8.3.3	Module design – SW level 1.....	67
8.3.4	Coding – SW level 1	67
8.3.5	Module test – SW level 1	68
8.3.6	Software testing – SW level 1	68
8.3.7	Documentation – SW level 1	69
8.3.8	Configuration and modification management process – SW level 1	69
8.4	Software level 2	70
8.4.1	Software safety lifecycle – SW level 2	70
8.4.2	Software design – SW level 2	71
8.4.3	Software system design – SW level 2	73
8.4.4	Module design – SW level 2.....	73
8.4.5	Coding – SW level 2	74
8.4.6	Module test – SW level 2	75
8.4.7	Software integration testing SW level 2.....	75
8.4.8	Software testing SW level 2	75
8.4.9	Documentation – SW level 2	76
8.4.10	Configuration and modification management process – SW level 2	77
9	Validation	77
9.1	Validation principles.....	77
9.1.1	Validation plan.....	80
9.1.2	Use of generic fault lists	80

9.1.3	Specific fault lists	80
9.1.4	Information for validation	81
9.1.5	Validation record	81
9.2	Analysis as part of validation	82
9.2.1	General	82
9.2.2	Analysis techniques	82
9.2.3	Verification of safety requirements specification (SRS)	82
9.3	Testing as part of validation	83
9.3.1	General	83
9.3.2	Measurement accuracy	83
9.3.3	More stringent requirements	84
9.3.4	Test samples	84
9.4	Validation of the safety function	84
9.4.1	General	84
9.4.2	Analysis and testing	85
9.5	Validation of the safety integrity of the SCS	85
9.5.1	General	85
9.5.2	Validation of subsystem(s)	85
9.5.3	Validation of measures against systematic failures	86
9.5.4	Validation of safety-related software	86
9.5.5	Validation of combination of subsystems	87
10	Documentation	87
10.1	General	87
10.2	Technical documentation	87
10.3	Information for use of the SCS	89
10.3.1	General	89
10.3.2	Information for use given by the manufacturer of subsystems	89
10.3.3	Information for use given by the SCS integrator	90
Annex A (informative)	Determination of required safety integrity	92
A.1	General	92
A.2	Matrix assignment for the required SIL	92
A.2.1	Hazard identification/indication	92
A.2.2	Risk estimation	92
A.2.3	Severity (Se)	93
A.2.4	Probability of occurrence of harm	93
A.2.5	Class of probability of harm (CI)	96
A.2.6	SIL assignment	96
A.3	Overlapping hazards	98
Annex B (informative)	Example of SCS design methodology	99
B.1	General	99
B.2	Safety requirements specification	99
B.3	Decomposition of the safety function	99
B.4	Design of the SCS by using subsystems	100
B.4.1	General	100
B.4.2	Subsystem 1 design – “guard door monitoring”	100
B.4.3	Subsystem 2 design – “evaluation logic”	102
B.4.4	Subsystem 3 design – “motor control”	103
B.4.5	Evaluation of the SCS	103
B.4.6	PFH	104

B.5	Verification.....	104
B.5.1	General	104
B.5.2	Analysis.....	104
B.5.3	Tests	105
Annex C (informative)	Examples of $MTTF_D$ values for single components	106
C.1	General.....	106
C.2	Good engineering practices method	106
C.3	Hydraulic components.....	106
C.4	$MTTF_D$ of pneumatic, mechanical and electromechanical components	107
Annex D (informative)	Examples for diagnostic coverage (DC).....	109
Annex E (informative)	Methodology for the estimation of susceptibility to common cause failures (CCF).....	111
E.1	General.....	111
E.2	Methodology	111
E.2.1	Requirements for CCF	111
E.2.2	Estimation of effect of CCF	111
Annex F (informative)	Guideline for software level 1	114
F.1	Software safety requirements.....	114
F.2	Coding guidelines	115
F.3	Specification of safety functions	116
F.4	Specification of hardware design	117
F.5	Software system design specification.....	119
F.6	Protocols	121
Annex G (informative)	Examples of safety functions.....	124
Annex H (informative)	Simplified approaches to evaluate the PFH value of a subsystem	125
H.1	Table allocation approach	125
H.2	Simplified formulas for the estimation of PFH	127
H.2.1	General	127
H.2.2	Basic subsystem architecture A: single channel without a diagnostic function	127
H.2.3	Basic subsystem architecture B: dual channel without a diagnostic function	128
H.2.4	Basic subsystem architecture C: single channel with a diagnostic function	128
H.2.5	Basic subsystem architecture D: dual channel with a diagnostic function(s)	133
H.3	Parts count method.....	134
Annex I (informative)	The functional safety plan and design activities	135
I.1	General.....	135
I.2	Example of a machine design plan including a safety plan	135
I.3	Example of activities, documents and roles	135
Annex J (informative)	Independence for reviews and testing/verification/validation activities	138
J.1	Software design	138
J.2	Validation.....	138
Bibliography		140

Figure 1 – Scope of this document.....

Figure 2 – Integration within the risk reduction process of ISO 12100 (extract)	29
Figure 3 – Iterative process for design of the safety-related control system	30
Figure 4 – Example of a combination of subsystems as one SCS.....	31
Figure 5 – By activating a low demand safety function at least once per year it can be assumed to be high demand	36
Figure 6 – Examples of typical decomposition of a safety function into sub-functions and its allocation to subsystems	39
Figure 7 – Example of safety integrity of a safety function based on allocated subsystems as one SCS	40
 Figure 8 – Basic subsystem architecture A logical representation	60 
 Figure 9 – Basic subsystem architecture B logical representation	60 
 Figure 10 – Basic subsystem architecture C logical representation	60 
 Figure 11 – Basic subsystem architecture D logical representation	61 
Figure 12 – V-model for SW level 1.....	64
Figure 13 – V-model for software modules customized by the designer for SW level 1	64
Figure 14 – V-model of software safety lifecycle for SW level 2.....	70
Figure 15 – Overview of the validation process	79
Figure A.1 – Parameters used in risk estimation	92
Figure A.2 – Example proforma for SIL assignment process	98
Figure B.1 – Decomposition of the safety function.....	100
Figure B.2 – Overview of design of the subsystems of the SCS	100
Figure F.1 – Plant sketch	116
Figure F.2 – Principal module architecture design.....	119
Figure F.3 – Principal design approach of logical evaluation	120
Figure F.4 – Example of logical representation (program sketch)	121
 Figure H.1 – Basic subsystem architecture A logical representation	127 
 Figure H.2 – Basic subsystem architecture B logical representation	128 
 Figure H.3 – Basic subsystem architecture C logical representation.....	128 
 Figure H.4 – Correlation of basic subsystem architecture C and the pertinent fault handling function	129 
 Figure H.5 – Basic subsystem architecture C with external fault handling function	130 
 Figure H.6 – Basic subsystem architecture C with external fault diagnostics	131 
 Figure H.7 – Basic subsystem architecture C with external fault reaction	131 
 Figure H.8 – Basic subsystem architecture C with internal fault diagnostics and internal fault reaction.....	131 
 Figure H.9 – Basic subsystem architecture D logical representation.....	133 
Figure I.1 – Example of a machine design plan including a safety plan	135
Figure I.2 – Example of activities, documents and roles (1 of 2).....	136
Table 1 – Terms used in IEC 62061	13
Table 2 – Abbreviations used in IEC 62061.....	28
Table 3 – SIL and limits of <i>PFH</i> values.....	36
Table 4 – Required SIL and <i>PFH</i> of pre-designed subsystem	40
Table 5 – Relevant information for each subsystem	47

Table 6 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem	56
Table 7 – Overview of basic requirements and interrelation to basic subsystem architectures	61
Table 8 – Different levels of application software	63
Table 9 – Documentation of an SCS	88
Table A.1 – Severity (Se) classification	93
Table A.2 – Frequency and duration of exposure (Fr) classification	94
Table A.3 – Probability (Pr) classification	95
Table A.4 – Probability of avoiding or limiting harm (Av) classification	96
Table A.5 – Parameters used to determine class of probability of harm (CI)	96
Table A.6 – Matrix assignment for determining the required SIL (or PL _r) for a safety function	97
Table B.1 – Safety requirements specification – example of overview	99
Table B.2 – Systematic integrity – example of overview	104
Table B.3 – Verification by tests	105
Table C.1 – Standards references and $MTTF_D$ or B_{10D} values for components	107
Table D.1 – Estimates for diagnostic coverage (DC) (1 of 2)	109
Table E.1 – Estimation of CCF factor (β)	112
Table E.2 – Criteria for estimation of CCF	113
Table F.1 – Example of relevant documents related to the simplified V-model	114
Table F.2 – Examples of coding guidelines	115
Table F.3 – Specified safety functions	117
Table F.4 – Relevant list of input and output signals	118
Table F.5 – Example of simplified cause and effect matrix	121
Table F.6 – Verification of software system design specification	122
Table F.7 – Software code review	122
Table F.8 – Software validation	123
Table G.1 – Examples of typical safety functions	124
Table H.1 – Allocation of PFH value of a subsystem	126
Table H.2 – Relationship between B_{10D} , operations and $MTTF_D$	127
A1 Table H.3 – Minimum value of $1/\lambda_D F_H$ for the applicability of PFH equation (H.3)	132 A1
Table J.1 – Minimum levels of independence for review, testing and verification activities	138
Table J.2 – Minimum levels of independence for validation activities	138

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SAFETY OF MACHINERY –
FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

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

This second constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- structure has been changed and contents have been updated to reflect the design process of the safety function,
- standard extended to non-electrical technologies,
- definitions updated to be aligned with IEC 61508-4,
- functional safety plan introduced and configuration management updated (Clause 4),
- requirements on parametrization expanded (Clause 6),
- reference to requirements on security added (Subclause 6.8),
- requirements on periodic testing added (Subclause 6.9),
- various improvements and clarification on architectures and reliability calculations (Clause 6 and Clause 7),
- shift from "SILCL" to "maximum SIL" of a subsystem (Clause 7),
- use cases for software described including requirements (Clause 8),
- requirements on independence for software verification (Clause 8) and validation activities (Clause 9) added,
- new informative annex with examples (Annex G),
- new informative annexes on typical MTTF_D values, diagnostics and calculation methods for the architectures (Annex C, Annex D and Annex H).

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this document and its amendment will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

IEC 62061 specifies requirements for the design and implementation of safety-related control systems of machinery. This document is machine sector specific within the framework of IEC 61508.

NOTE While IEC 62061 and ISO 13849-1 are using different methodologies for the design of safety related control systems, they intend to achieve the same risk reduction.

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

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

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

- assign the required safety integrity for each safety function to be implemented by SCS;
- enable the design of the SCS appropriate to the assigned safety (control) function(s);
- integrate safety-related subsystems designed in accordance with other applicable functional safety-related standards (see 6.3.4);
- validate the SCS.

This document is intended to be used within the framework of systematic risk reduction, in conjunction with risk assessment described in ISO 12100. Suggested methodologies for a safety integrity assignment are given in informative Annex A.

SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

1 Scope

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

This document is a machinery sector specific standard within the framework of IEC 61508 (all parts).

The design of complex programmable electronic subsystems or subsystem elements is not within the scope of this document. This is in the scope of IEC 61508 or standards linked to it; see Figure 1.

NOTE 1 Elements such as systems on chip or microcontroller boards are considered complex programmable electronic subsystems.

The main body of this sector standard specifies general requirements for the design, and verification of a safety-related control system intended to be used in high/continuous demand mode.

This document:

- is concerned only with functional safety requirements intended to reduce the risk of hazardous situations;
- is restricted to risks arising directly from the hazards of the machine itself or from a group of machines working together in a co-ordinated manner;

NOTE 2 Requirements to mitigate risks arising from other hazards are provided in relevant sector standards. For example, where a machine(s) is part of a process activity, additional information is available in IEC 61511.

This document does not cover

- electrical hazards arising from the electrical control equipment itself (e.g. electric shock – see IEC 60204-1);
- other safety requirements necessary at the machine level such as safeguarding;
- specific measures for security aspects – see [A1](#) IEC TS 63074. [A1](#)

This document is not intended to limit or inhibit technological advancement.

Figure 1 illustrates the scope of this document.

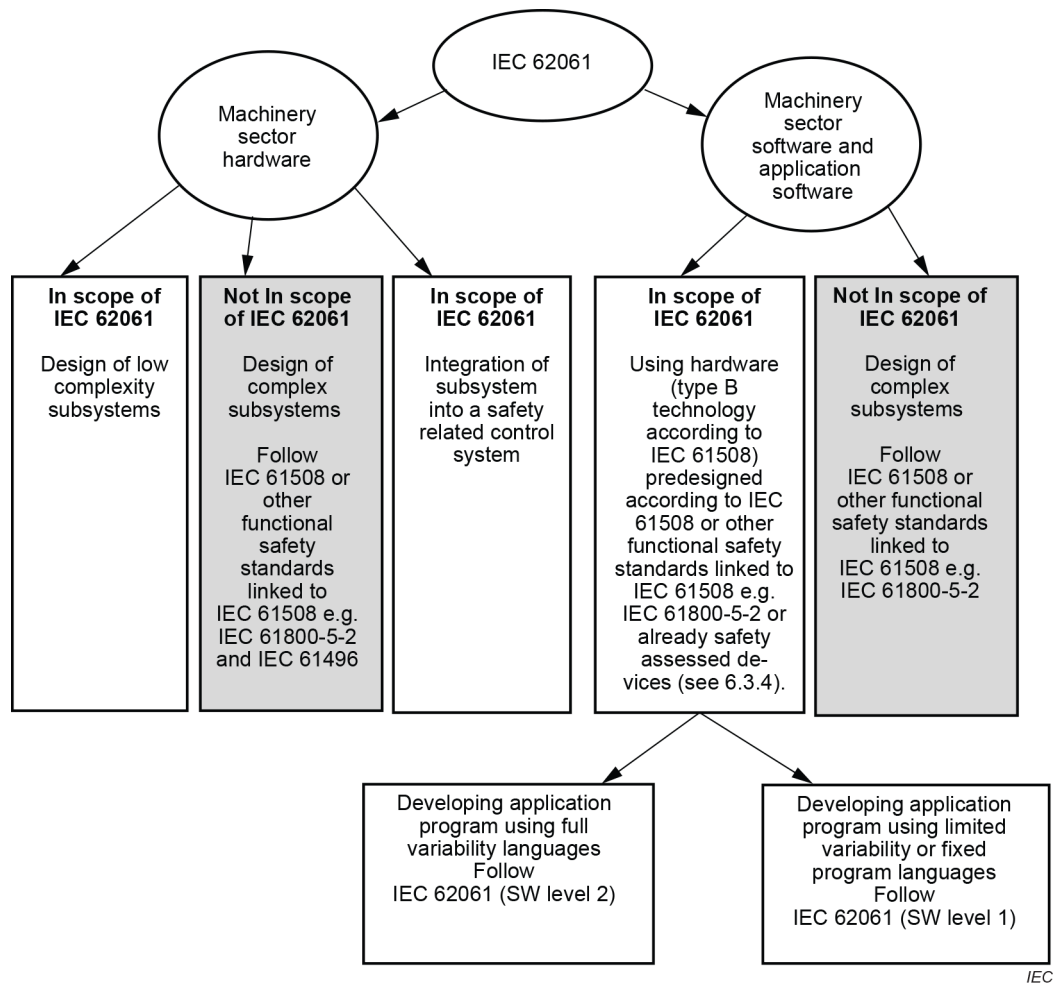


Figure 1 – Scope of this document

2 Normative references

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

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

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

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

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

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

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

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

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

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

3 Terms, definitions and abbreviations

3.1 Alphabetical list of definitions

Terms used throughout IEC 62061 are given in Table 1. Also included are some common abbreviations related to machinery safety.

Table 1 – Terms used in IEC 62061

Term	Definition number
application software	3.2.59
architectural constraint	3.2.46
architecture	3.2.45
average frequency of dangerous failure per hour (PFH)	3.2.29
average probability of dangerous failure on demand (PFD_{avg})	3.2.31
baseline (configuration)	3.2.67
bypass	3.2.17
common cause failure (CCF)	3.2.56
complex component	3.2.8
configuration management	3.2.66
continuous mode	3.2.28
dangerous failure	3.2.52
demand	3.2.25
diagnostic coverage (DC)	3.2.49
diagnostic test interval	3.2.50
embedded software	3.2.60
failure	3.2.51
fault	3.2.33
fault tolerance	3.2.34
full variability language (FVL)	3.2.61
functional safety	3.2.10
hardware fault tolerance (HFT)	3.2.35
hardware safety integrity	3.2.22
harm	3.2.12
hazard	3.2.11
high demand mode	3.2.27
integrator	3.2.13

Term	Definition number
limited variability language (LVL)	3.2.62
low complexity component	3.2.7
low demand mode	3.2.26
machine control system	3.2.2
machinery (machine)	3.2.1
mean repair time (MRT)	3.2.40
mean time to failure ($MTTF$)	3.2.37
mean time to dangerous failure ($MTTF_D$)	3.2.38
mean time to restoration (MTTR)	3.2.39
muting	3.2.16
pre-designed (SCS or subsystem)	3.2.5
probability of dangerous failure on demand (PFD)	3.2.30
process safety time	3.2.41
proof test coverage	3.2.48
proof test	3.2.47
protective measure	3.2.14
random hardware failure	3.2.57
ratio of dangerous failure (RDF)	3.2.55
risk	3.2.15
safe failure	3.2.53
safe failure fraction (SFF)	3.2.54
safe state	3.2.68
safety	3.2.9
safety function	3.2.18
safety integrity	3.2.21
safety integrity level (SIL)	3.2.24
safety-related control system (SCS)	3.2.3
safety-related software	3.2.63
security	3.2.69
(SCS) diagnostic function	3.2.19
(SCS) fault reaction function	3.2.20
subsystem	3.2.4
subsystem element	3.2.6
sub-function	3.2.36
systematic failure	3.2.58
systematic safety integrity	3.2.23
target failure measure	3.2.32
useful lifetime	3.2.42
validation (of the safety function)	3.2.65
verification	3.2.64
well-tried component	3.2.43
well-tried safety principles	3.2.44

3.2 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.2.1

machinery

machine

assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application

Note 1 to entry: The term “machinery” also covers an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

[SOURCE: ISO 12100:2010, 3.1]

3.2.2

machine control system

system that responds to input signals from the machinery and/or from an operator and generates output signals causing the machinery to operate in the desired manner

Note 1 to entry: The machine control system includes input devices and final elements.

[SOURCE: IEC 61508-4:2010, 3.3.3, modified – the term defined has been changed, “process” has been changed to “machinery”]

3.2.3

safety-related control system

SCS

part of the control system of a machine which implements a safety function by one or more subsystems

Note 1 to entry: SCS is similar to SRECS of the previous edition of this document.

3.2.4

subsystem

entity of the top-level architectural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function

Note 1 to entry: This differs from common language where “subsystem” may mean any sub-divided part of an entity, the term “subsystem” is used in this document 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”.

Note 2 to entry: A complete subsystem can be made up from a number of identifiable and separate subsystem elements.

Note 3 to entry: The subsystem specification includes its role in the safety function and its interface with the other subsystems of the SCS.

Note 4 to entry: One subsystem can be part of several safety functions, e.g. the same combination of contactors can be used to de-energise a motor either in the event of detection of a person in a danger zone or also in the event of opening an interlock guard.

[SOURCE: IEC 61508-4:2010, 3.4.4, modified – cross references removed and notes added]

3.2.5**pre-designed SCS or subsystem**

SCS or subsystem which meets the relevant requirements of a functional safety standard

3.2.6**subsystem element**

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

Note 1 to entry: A subsystem element may comprise hardware and software.

Note 2 to entry: Elements that are not directly necessary for the safety function are not included, but may support it (for example, filters elements, protection against over-voltage).

Note 3 to entry: A subsystem element is the lowest level of detail to consider when ensuring that the requirements of a sub-function are met.

3.2.7**low complexity component/subsystem**

component/subsystem in which

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

Note 1 to entry: Behaviour of the low complexity component / subsystem under fault conditions may be determined by analytical and/or test methods.

Note 2 to entry: Examples of low complexity components / subsystem are limit switches, electro-mechanical relays or contactors.

[SOURCE: IEC 61508-4:2010, 3.4.3, modified – the term defined has been changed, leading to reformulation of text. Example converted into note 2]

3.2.8**complex component / subsystem**

component / subsystem in which

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

3.2.9**safety**

freedom from unacceptable risk

[SOURCE: IEC 61508-4:2010, 3.1.11]

3.2.10**functional safety**

part of the overall safety of the machine and the machine control system that depends on the correct functioning of the SCS and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – using terms machine, machine control system and SCS]

3.2.11**hazard**

potential source of harm

Note 1 to entry: 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).

[SOURCE: ISO 12100:2010, 3.6, modified – note 1 has been modified and notes 2 and 3 deleted]

3.2.12

harm

injury or damage to the health of people

[SOURCE: ISO/IEC Guide 51:2014, 3.1, modified – without damage to property or the environment]

3.2.13

integrator

entity who designs, manufactures or assembles an integrated manufacturing system and is responsible for the safety strategy, including the protective measures, control interfaces and interconnections of the control system

Note 1 to entry: The integrator may be for example a manufacturer, assembler, engineering company, or entity with the overall responsibility for the machine.

[SOURCE: ISO 11161:2007, 3.10, modified – "provides" has been deleted, last entry in note reformulated]

3.2.14

protective measure

measure intended to achieve risk reduction

[SOURCE: ISO 12100:2010, 3.19, modified – bullet list removed]

3.2.15

risk

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

[SOURCE: ISO/IEC Guide 51:2014, 3.9 modified – note to entry removed]

3.2.16

muting

temporary automatic suspension of a safety function(s)

Note 1 to entry: Other means are used to maintain the safety level.

[SOURCE: ISO 13849-1:2015, 3.1.8, modified – "by the SRP/CS" has been deleted, note added]

3.2.17

bypass

action or facility to prevent all or parts of the SCS functionality from being executed

Note 1 to entry: Examples of bypassing include:

- the input signal is blocked from the trip logic while still presenting the input parameters and alarm to the operator;
- the output signal from the trip logic to a final element is held in the normal state preventing final element operation;
- a physical bypass line is provided around the final element;
- preselected input state (e.g., on/off input) or set is forced by means of an engineering tool (e.g., in the application program).

Note 2 to entry: Other terms are also used to refer to bypassing, such as override, defeat, disable, force, or inhibit or muting.

[SOURCE: IEC 61511-1:2016, 3.2.4, modified – SIS replaced by SCS]

3.2.18

safety function

function implemented by an SCS 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) in respect of a specific hazardous event

Note 1 to entry: This term is used instead of "safety-related control function (SRCF)" of IEC 62061:2015. This definition differs from ISO 12100 because this document addresses risk reduction performed by SCS.

Note 2 to entry: A safety function is typically starting with a detection and evaluation of an 'initiation event' and ending with an output causing a reaction of a 'machine actuator'.

Note 3 to entry: Parts of machine operating function(s), e.g. the reaction of a machine actuator, can also be part of safety function(s).

[SOURCE: IEC 61508-4:2010, 3.5.1, modified – terminology adapted to machinery, other risk reduction measures deleted, example deleted, notes added]

3.2.19

(SCS) diagnostic function

function intended to detect faults in the SCS and initiate a specified fault reaction function when a fault is detected

Note 1 to entry: This function is intended to detect faults that could lead to a dangerous failure of a safety function and initiate a specified fault reaction function.

3.2.20

(SCS) fault reaction function

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

3.2.21

safety integrity

probability of an SCS or its subsystem satisfactorily performing the required safety function under all stated conditions within a stated period of time

Note 1 to entry: 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 function.

Note 2 to entry: Safety integrity comprises hardware safety integrity and systematic safety integrity.

[SOURCE: IEC 61508-4:2010, 3.5.4, modified – terminology adapted to machinery, notes 2, 3, 5 deleted]

3.2.22

hardware safety integrity

part of the safety integrity of an SCS or its subsystems relating to random hardware failures in a dangerous mode of failure

Note 1 to entry: The term relates to failures in a dangerous mode, that is, those failures of a safety-related system that would impair its safety integrity.

Note 2 to entry: Hardware safety integrity includes architectural constraints.

[SOURCE: IEC 61508-4:2010, 3.5.7 – terminology adapted to machinery, note 1 shortened, note 2 added]

3.2.23

systematic safety integrity

part of the safety integrity of an SCS or its subsystems relating to its resistance to systematic failures in a dangerous mode

Note 1 to entry: Systematic safety integrity cannot usually be quantified precisely.

Note 2 to entry: Requirements for systematic safety integrity apply to both hardware and software aspects of an SCS or its subsystems.

[SOURCE: IEC 61508-4:2010, 3.5.6, modified – terminology adapted to machinery, note 1 shortened, note 2 added]

3.2.24

safety integrity level

SIL

discrete level (one out of a possible three) for describing the capability to perform a safety function where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest

3.2.25

demand

event that causes the SCS to perform a safety function

Note 1 to entry: Demand mode means that a safety function is only performed on request (demand) in order to transfer the machine into a specified state. The SCS does not influence the machine until there is a demand on the safety function.

Note 2 to entry: Demand rate (DR) or the frequency of demands is one of the main factor that is considered for assessing the demand mode, low or high. For this particular purpose, the demand rate (DR) can be identified with the rate of events, where harm would occur without intervention of the safety function. This rate may be lower than an actual rate of triggering the safety function during operation.

Note 3 to entry: For an emergency stop function, the demand mode is not defined. To determine the achieved SIL, the principle for evaluation of the selected demand mode of the other functions is usually applicable.

3.2.26

low demand mode

mode of operation in which the frequency of demands of a safety function is no greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – low demand extracted from definition of "mode of operation"]

3.2.27

high demand mode

mode of operation in which the frequency of demands of a safety function is greater than one per year

Note 1 to entry: Continuous mode means that a safety function is performed continuously, i.e. the SCS is continuously controlling the machine and a (dangerous) failure of its function can result in a hazard.

Note 2 to entry: The distinction between high demand and continuous mode is relevant for the qualification of diagnostic measures (refer to 7.4.3 and 7.4.4). It is not relevant for target failure measure and SIL assignment.

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – high demand extracted from definition of "mode of operation", notes added]

3.2.28

continuous mode

mode of operation where the safety function retains the machinery in a safe state as a part of normal operation

Note 1 to entry: Continuous mode means that a safety function is performed continuously, i.e. the SCS is continuously controlling the machine and a (dangerous) failure of its function can result in a hazard.

Note 2 to entry: The distinction between high demand and continuous mode is relevant for the qualification of diagnostic measures (refer to 7.4.3 and 7.4.4). It is not relevant for target failure measure and SIL assignment"

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – high demand extracted from definition of "mode of operation", notes added]

3.2.29

average frequency of a dangerous failure per hour

PFH or *PFH_D*

average frequency of dangerous failure of an SCS to perform a specified safety function over a given period of time

Note 1 to entry: Both terms *PFH* and *PFH_D* correspond to the probability of dangerous failures per hour (IEC 62061:2005+AMD1:2012+AMD2:2015).

Note 2 to entry: The term "average probability of dangerous failure per hour" is not used in this edition anymore but the acronym *PFH* has been retained but when it is used it means "average frequency of dangerous failure [h]".

[SOURCE: IEC 61508-4:2010, 3.6.19, modified – terminology adapted to machinery, existing notes deleted, new notes added]

3.2.30

probability of dangerous failure on demand

PFD

safety unavailability (see IEC 60050-192) of an SCS to perform the specified safety function when a demand occurs from the machinery or machinery control system

Note 1 to entry: The [instantaneous] unavailability (as per IEC 60050-192) is the probability that an item is not in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided. It is generally noted by $U(t)$.

Note 2 to entry: The [instantaneous] availability does not depend on the states (running or failed) experienced by the item before it. It characterizes an item which only has to be able to work when it is required to do so, for example, an SCS working in low demand mode.

Note 3 to entry: If periodically tested, the *PFD* of an SCS is, in respect of the specified safety function, represented by a saw tooth curve with a large range of probabilities ranging from low, just after a test, to a maximum just before a test.

[SOURCE: IEC 61508-4:2010, 3.6.17, modified – terminology adapted to machinery]

3.2.31

average probability of dangerous failure on demand

PFD_{avg}

mean unavailability (see IEC 60050-192) of an SCS to perform the specified safety function when a demand occurs from the machinery or machinery control system as an average over time

Note 1 to entry: The mean unavailability over a given time interval $[t_1, t_2]$ is generally noted by $U(t_1, t_2)$.

Note 2 to entry: Two kind of failures contribute to *PFD* and *PFD_{avg}*: the dangerous undetected failures occurred since the last proof test and genuine on demand failures caused by the demands (proof tests and safety demands) themselves. The first one is time dependent and characterized by their dangerous failure rate $\lambda_{DU}(t)$ whilst the second one is dependent only on the number of demands and is characterized by a probability of failure per demand (denoted by γ).

Note 3 to entry: As genuine on demand failures cannot be detected by tests, it is necessary to identify them and take them into consideration when calculating the target failure measures.

[SOURCE: IEC 61508-4:2010, 3.6.18, modified – terminology adapted to machinery]

3.2.32

target failure measure

intended *PFH* or *PFD_{avg}* to be achieved to meet a specific safety integrity requirement(s)

Note 1 to entry: Target failure measure is specified in terms of:

- the average probability of a dangerous failure of the safety function on demand, (for a low demand mode of operation);
- the average frequency of a dangerous failure [h^{-1}] (for a high demand mode of operation or a continuous mode of operation).

[SOURCE: IEC 61508-4:2010, 3.5.17, modified – "target probability of dangerous mode failures" changed to "intended PFH or PFD_{avg} ", bullet list moved to note 1, existing note deleted]

3.2.33

fault

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

Note 1 to entry: In IEC 60050-192, 192-04-01 a fault of an item is described as inability to perform as required, due to an internal state.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – terminology adapted to machinery, note shortened]

3.2.34

fault tolerance

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

[SOURCE: IEC 61508-4:2010, 3.6.3, modified – terminology adapted to machinery]

3.2.35

hardware fault tolerance

HFT

property of a subsystem to potentially lose the safety function upon at least $N+1$ faults

Note 1 to entry: A hardware fault tolerance of N means that $N+1$ faults of a subsystem could cause a loss of the safety function.

[SOURCE: IEC 61508-2:2010, derived from 7.4.4.1.1]

3.2.36

sub-function

part of a safety function whose failure can result in a failure of the safety function

Note 1 to entry: In this document, a safety function can be seen as a logical AND of the sub-functions.

3.2.37

mean time to failure

$MTTF$

expectation of the mean time to failure

Note 1 to entry: $MTTF$ is normally expressed as an average value of expectation of the time to failure.

[SOURCE: IEC 60050-192, 192-05-11, modified – note added and original notes removed]

3.2.38

mean time to dangerous failure

$MTTF_D$

expectation of the mean time to dangerous failure

[SOURCE: Definition derived from IEC 60050-192, 192-05-11, modified – restricted to dangerous failures]

3.2.39**mean time to restoration****MTTR**

expected time to achieve restoration after a fault has occurred in a safety function.

Note 1 to entry: MTTR encompasses:

- the time to detect the failure (a); and
- the time spent before starting the repair (b); and
- the effective time to repair (c); and
- the time before the component is put back into operation (d).

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

Note 2 to entry: During this time the machine can continue to operate

[SOURCE: IEC 61508-4:2010, 3.6.21, modified – terminology adapted to machinery and more details added to definition]

3.2.40**mean repair time****MRT**

mean repair time after a fault has been detected in a safety function and machine continues to operate

Note 1 to entry: MRT encompasses:

- the time spent before starting the repair (b); and
- the effective time to repair (c); and
- the time before the component is put back into operation (d).

Note 2 to entry: Depending on the type of detected fault and the fault reaction, the numerical values for MRT and MTTR can be different.

[SOURCE: IEC 61508-4:2010, 3.6.22, modified – terminology adapted to machinery and more details added to definition, note 1 made similar to 3.2.39, note 2 added]

3.2.41**process safety time**

period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the machinery or machinery control system and the time by which action has to be completed in the machinery to prevent the hazardous event occurring

Note 1 to entry: It is foreseen that the safety function detects the failure and completes its action soon enough to prevent the hazardous event taking into account any process lag (e.g. stopping times).

[SOURCE: IEC 61508-4:2010, 3.6.20 modified – terminology adapted to machinery, note 1 added]

3.2.42**useful lifetime**

minimum elapsed time between the installation of the SCS or subsystem or subsystem element and the point in time when component failure rates of the SCS or subsystem or subsystem element can no longer be predicted, with any accuracy

Note 1 to entry: Typically it will be 20 years or less unless the manufacturers of the SCS and its subsystems can justify a longer lifetime by providing evidence, based on calculations, showing that reliability data is valid for the longer lifetime.

[SOURCE: IEC 61131-6:2012, 3.57, modified – terminology adapted to machinery, note 1 added, example deleted]

3.2.43

well-tried component

for a safety-related application, component for a safety-related application which has been either

- a) widely used in the past with successful results in similar safety-related applications as given as well-tried components in the informative annexes of ISO 13849-2, or
- b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications

Note 1 to entry: ISO 13849-2 lists a variety of components and the conditions for specific technologies under which the component can be considered well-tried.

Note 2 to entry: Newly developed components may be considered as equivalent to “well-tried” if they fulfil the conditions of b).

Note 3 to entry: The decision to accept a particular component as being “well-tried” depends on the application, e.g. owing to the environmental influences and can be impacted by product or manufacturer changes.

Note 4 to entry: Complex electronic components (e.g. PLC, microprocessor, application-specific integrated circuit) cannot be considered as equivalent to “well tried”.

Note 5 to entry: A well-tried component is not a proven in use component.

3.2.44

well-tried safety principles

principles that have proved effective in the design or integration of safety-related control systems in the past, to avoid or control critical faults or failures which can influence the performance of a safety function

Note 1 to entry: Newly developed safety principles can be considered as equivalent to “well-tried” if they are verified using principles which demonstrate their suitability and reliability for safety-related applications.

Note 2 to entry: Well-tried safety principles are effective not only against random hardware failures, but also against systematic failures which may creep into the product at some point in the course of the product life cycle, e.g. faults arising during product design, integration, modification or deterioration.

Note 3 to entry: Tables A.2, B.2, C.2 and D.2 in the informative annexes of ISO 13849-2:2012 address well-tried safety principles for different technologies.

[SOURCE: Definition derived from ISO 13849-1:2015]

3.2.45

architecture

specific configuration of hardware and software elements in an SCS

[SOURCE: IEC 61508-4:2010, 3.3.4, modified – terminology adapted to machinery]

3.2.46

architectural constraint

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

3.2.47

proof test

periodic test that can detect dangerous undetected faults and degradation in an SCS and its subsystems so that, if necessary, the relevant parts of the SCS and its subsystems can be restored to an “as new” condition or as close as practical to this condition

Note 1 to entry: A proof test is intended to confirm that relevant parts of an SCS are in a condition that assures the specified safety integrity.

Note 2 to entry: The effectiveness of the proof test will be dependent both on failure coverage and repair effectiveness. In practice, detecting 100 % of the degradation that could lead to the hidden dangerous failures later on is not easily achieved. For complex elements or safety features that are difficult to verify, a proof test coverage of 100 % cannot be usually obtained.

[SOURCE: IEC 61508-4:2010, 3.8.5, modified – terminology adapted to machinery, notes 1, 3, 4 deleted, new note 1 added, note 2 shortened]

3.2.48

proof test coverage

term given to the percentage of dangerous undetected failures that are detected by a defined proof test procedure

Note 1 to entry: It measures the effectiveness of a proof test and ranges from 0 % to 100 % (perfect proof-test).

Note 2 to entry: For example, a PTC of 95 % states that 95 % of all possible undetected failures will be detected during the proof test. It doesn't include aging or degradation not directly related to the safety function failure.

Note 3 to entry: The PTC can be estimated by the means of Failure Mode and Effects Analysis (FMEA) in conjunction with engineering judgement based on sound evidence.

3.2.49

diagnostic coverage

DC

fraction of dangerous failures detected by automatic on-line diagnostic tests

Note 1 to entry: The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures.

Note 2 to entry: The dangerous failure diagnostic coverage is computed using the following equation, where *DC* is the diagnostic coverage, λ_{DD} is the detected dangerous failure rate and λ_{Dtotal} is the total dangerous failure rate:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}} \quad (1)$$

Note 3 to entry: This definition is applicable providing the individual components have constant failure rates.

[SOURCE: IEC 61508-4:2010, 3.8.6, modified – part of the definition has been moved to a note to entry]

3.2.50

diagnostic test interval

interval between on-line tests to detect faults in a subsystem that has a specified diagnostic coverage

[SOURCE: IEC 61508-4:2010, 3.8.7, modified – replacing safety-related system by subsystem]

3.2.51

failure

termination of the ability of an item (SCS, a subsystem or a subsystem element) to perform a required function

Note 1 to entry: Failures are either random (in hardware) or systematic (in hardware or software).

Note 2 to entry: After a failure, the item has a fault.

Note 3 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

Note 4 to entry: The concept of failure as defined does not apply to items consisting of software only.

[SOURCE: IEC 61508-4:2010, 3.6.4, modified and ISO 12100-1:2010, 3.32]

3.2.52

dangerous failure

failure of an SCS, a subsystem, or a subsystem element that plays a part in implementing the safety function that:

- a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the machine is put into a hazardous or potentially hazardous state; or
- b) decreases the probability that the safety function operates correctly when required

[SOURCE:  IEC 61508-4:2010, 3.6.7, modified – Terminology adapted to machinery 

3.2.53

safe failure

failure of an SCS, a subsystem, or a subsystem element that plays a part in implementing the safety function that:

- a) results in the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state; or
- b) increases the probability of the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state

[SOURCE: IEC 61508-4:2010, 3.6.8, modified – terminology adapted to machinery]

3.2.54

safe failure fraction

SFF

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

Note 1 to entry: The diagnostic coverage (if any) of each subsystem in SCS 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 7.4).

Note 2 to entry: “No effect failures” and “no part failures” (see IEC 61508-4) is not used for SFF calculations.

3.2.55

ratio of dangerous failure

RDF

fraction of the overall failure rate of an element that can result in a dangerous failure

3.2.56

common cause failure

CCF

failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel subsystem, leading to failure of a safety function

[SOURCE: IEC 61508-4:2010, 3.6.10, modified – system failure replaced by failure of a safety function]

3.2.57

random hardware failure

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

[SOURCE: IEC 61508-4:2010, 3.6.5, modified – notes removed]

3.2.58

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

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: 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.

[SOURCE: IEC 61508-4:2010, 3.6.6, modified – note 3 slightly changed, note 4 removed]

3.2.59

application software

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

3.2.60

embedded software

software, supplied as part of a pre-designed subsystem, that is not intended to be modified and that relates to the functioning of, and services provided by, the SCS or subsystem, as opposed to the application software

Note 1 to entry: Firmware and system software are examples of embedded software.

3.2.61

full variability language

FVL

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

Note 1 to entry: Typical example of systems using FVL are general-purpose computers.

Note 2 to entry: FVL is normally found in embedded software and is rarely used in application software.

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

[SOURCE: IEC 61511-1:2016, 3.2.75.3, modified – first part of definition suppressed and link to process sector deleted]

3.2.62

limited variability language

LVL

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

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

Note 2 to entry: 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 to entry: Typical example of systems using LVL: Programmable Logic Controller (PLC) configured for machine control.

[SOURCE: IEC 61511-1:2016, 3.2.75.2, modified – note 1 turned into definition, note 2 deleted, note 3 replaced]

3.2.63

safety-related software

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

3.2.64 verification

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

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.

[SOURCE: IEC 61508-4:2010, 3.8.1, modified – terminology adapted to machinery, note deleted]

3.2.65 validation (of the safety function)

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

[SOURCE: IEC 61508-4:2010, 3.8.2, modified – terminology adapted to machinery, notes deleted]

3.2.66 configuration management

discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the lifecycle

[SOURCE: IEC 61508-4:2010, 3.7.3, modified – note removed]

3.2.67 baseline (configuration)

well-defined set of elements (hardware, software, documentation, tests, etc.) of an SCS at a specific point in time.

Note 1 to entry: A baseline serves as a basis for verification, validation, modification and changes.

Note 2 to entry: If an element is changed, the status of the baseline is intermediate until a new baseline is defined.

3.2.68 safe state

state of the machine when safety is achieved

Note 1 to entry: The safe state doesn't include the restoration of initial equipment failures.

[SOURCE: IEC 61508-4:2010, 3.1.13, modified – terminology adapted to machinery, original note deleted, note 1 added]

3.2.69 security

- 1) measures taken to protect a system
- 2) condition of a system that results from the establishment and maintenance of measures to protect the system
- 3) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss

- 4) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems
- 5) prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

Note 1 to entry: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.99]

3.3 Abbreviations

Abbreviations used in this document are shown in Table 2.

Table 2 – Abbreviations used in IEC 62061

CCF	Common Cause Failure(s)
DC	Diagnostic Coverage
EMC	Electromagnetic Compatibility
FVL	Full Variability Language
I/O	Input/Output
LVL	Limited Variability Language
HFT	Hardware Fault Tolerance
HW	Hardware
PFH, PFH_D	average frequency of dangerous failure per Hour
MRT	Mean Repair Time
MTTF	Mean Time To Failure
$MTTF_D$	Mean Time to Dangerous Failure
MTTR	Mean Time To Restoration
PFD	probability of dangerous failure on demand
PFD_{avg}	average probability of dangerous failure on demand
PL	Performance Level
PLC	Programmable Logic Controller
RDF	Ratio of Dangerous Failure
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SCS	Safety-Related Control System
SRS	Safety Requirements Specification
SW	Software

4 Design process of an SCS and management of functional safety

4.1 Objective

The objective of Clause 4 is to describe the design process and the tasks that have to be completed to realize each safety function performed by the related part of the control system for a given machine.

4.2 Design process

If as a result of the risk assessment of the whole machine according to ISO 12100 (see Figure 2), a need for risk reduction has been identified and if certain selected risk reduction measures depend on the control system, corresponding safety functions have to be specified.

NOTE 1 Examples of safety functions are given in [A1](#) Annex G. [A1](#)

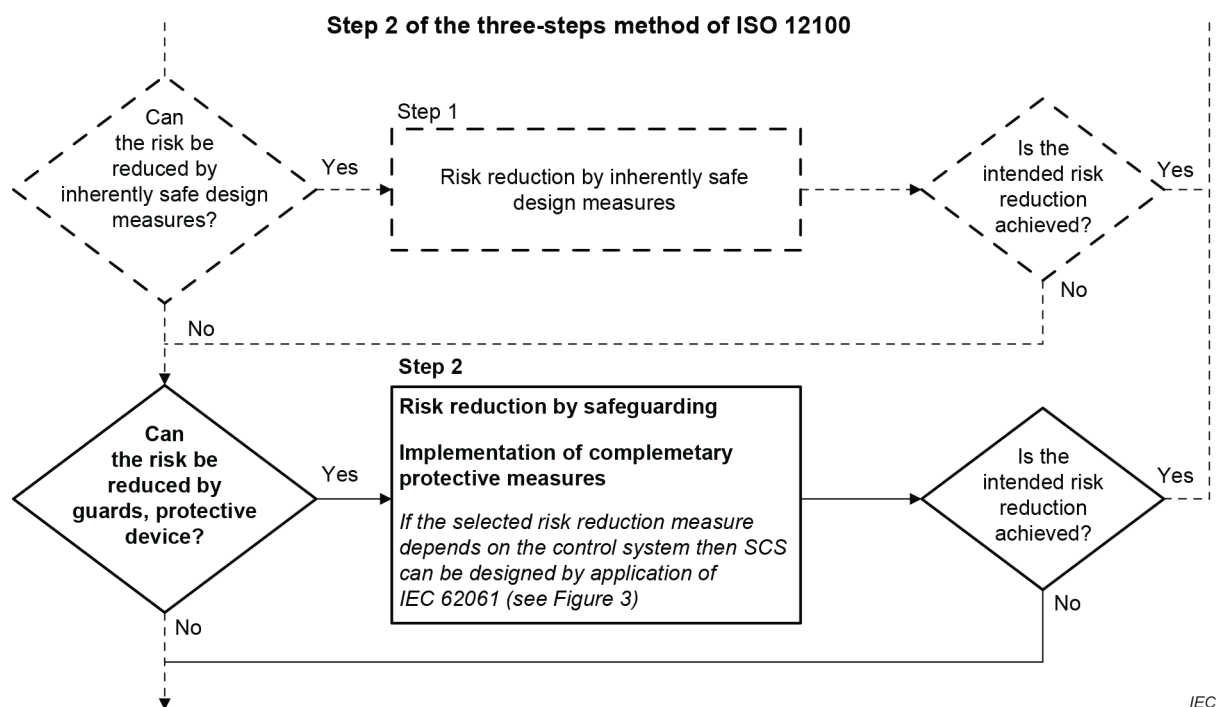
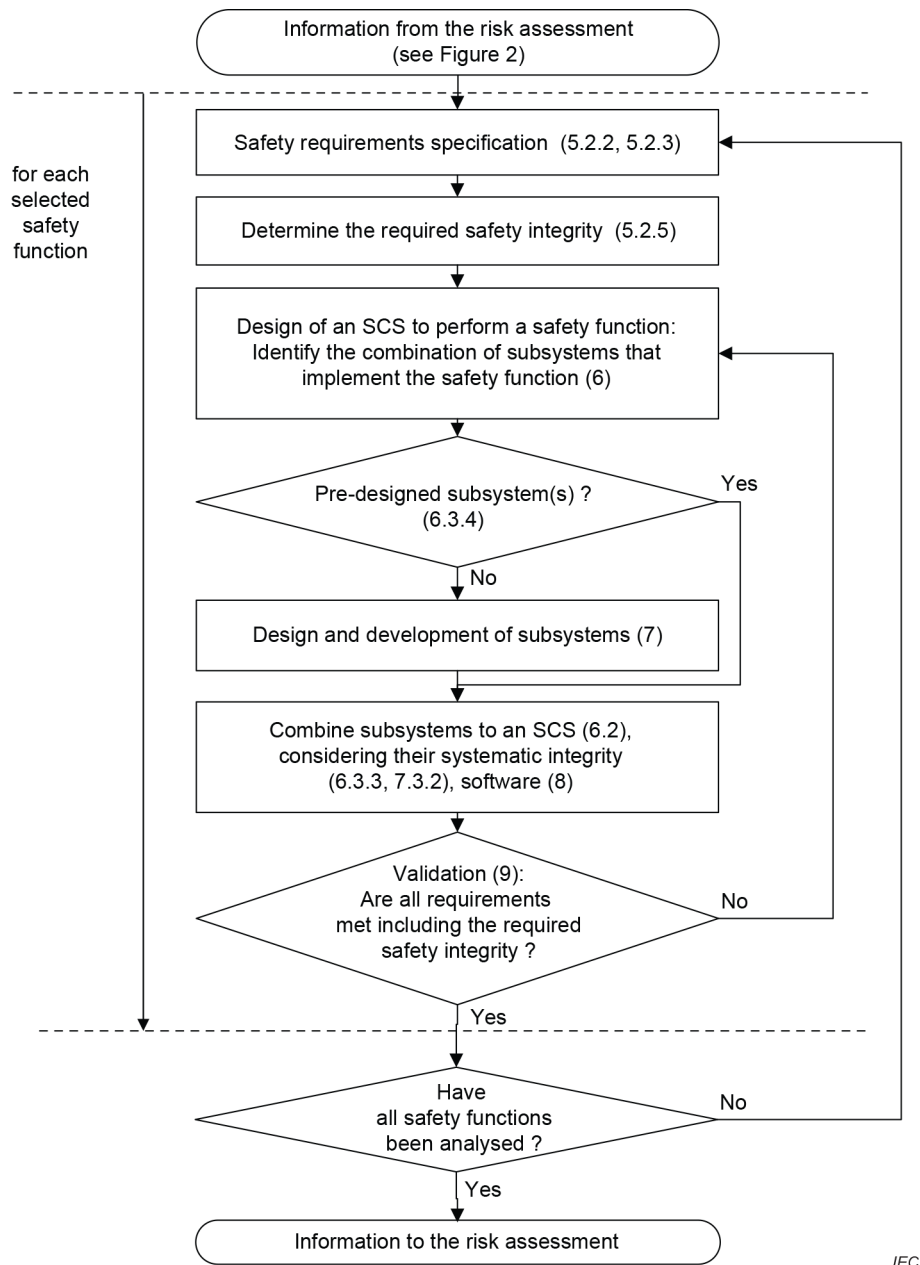


Figure 2 – Integration within the risk reduction process of ISO 12100 (extract)

NOTE 2 Figure 2 shows where the SCS contributes to the risk reduction process of ISO 12100: Step 2. The SCS supports the combined protective measures by the implementation of safety functions. ISO 12100 also provides general design rules for the machine which are applicable for the design of the SCS (see 6.2.11 and 6.2.12 of ISO 12100:2010).

The design process (see Figure 3) of each safety function implemented by a safety-related control system (SCS) shall include at least the safety function specification (see Clause 5) and the safety-related control system design (see Clause 6) and the associated verification and validation activities.



NOTE Each step described in the process flow diagram includes also verification activities.

Figure 3 – Iterative process for design of the safety-related control system

The realization of a safety function following the determined required safety integrity shall either be done by

- using an already developed SCS that meets the required safety integrity, or
- designing a new SCS using pre-designed subsystems according to Clause 6 or designing new subsystems according to Clause 7, or a combination of both.

If additional design considerations for software are necessary, Clause 8 applies.

A safety function can be implemented by one or more subsystem(s) of a safety-related control system (SCS), and several safety functions can share one or more subsystem(s) (e.g. a logic unit, power control element(s)), see examples in Figure 4. A control system can be subdivided into a safety-related part and a non-safety-related part. It is possible that one subsystem, which is involved in the implementation of safety functions, is also involved in the implementation of control functions. The designer may use any of the technologies available, singly or in combination.

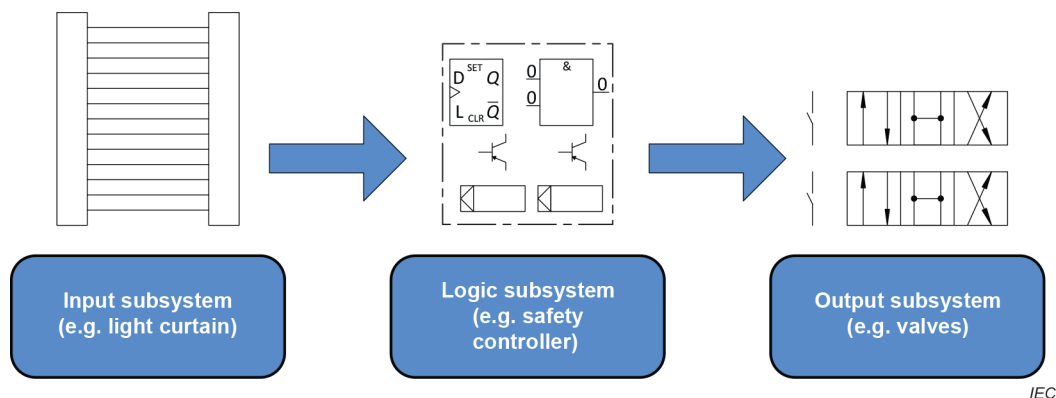


Figure 4 – Example of a combination of subsystems as one SCS

4.3 Management of functional safety using a functional safety plan

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

NOTE 1 For further information, see IEC 61508-1:2010, Clause 6.

A functional safety plan shall be drawn up and documented for each SCS design project, and shall be updated as necessary. The functional safety plan is intended to provide measures for preventing incorrect specification, implementation, or modification issues.

The functional safety plan shall identify the relevant activities (see Figure 3) and shall be adapted to the project. See examples in Annex I.

NOTE 2 The functional safety plan can be part of a global machine design plan.

NOTE 3 The content of the functional safety plan depends 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 functional safety plan shall:

- a) identify the relevant activities specified in Clauses 5 to 9 and details of when they shall take place;
- 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, results of a 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.

NOTE 4 The level of appropriate competency of the involved persons (i.e. training, technical knowledge, experience and qualifications) are taken into account. The appropriateness of competence is considered in relation to the particular application, taking into account all relevant factors including:

- a) the responsibilities of the person;
 - b) the level of supervision required;
 - c) the potential consequences in the event of failure of the SCS;
 - d) the safety integrity levels of the SCS;
 - e) the novelty of the design, design procedures or application;
 - f) previous experience and its relevance to the specific duties to be performed and the technology being employed;
 - g) the type of competence appropriate to the circumstances (for example qualifications, experience, relevant training and subsequent practice, and leadership and decision-making abilities);
 - h) engineering knowledge appropriate to the application area and to the technology;
 - i) safety engineering knowledge appropriate to the technology;
 - j) knowledge of the legal and safety regulatory framework;
 - k) relevance of qualifications to specific activities to be performed.
- e) identify or establish the procedures and resources to record and maintain information relevant to the functional safety of an SCS;

NOTE 5 The following are 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 SCS modifications).
- f) describe the strategy for configuration management (see 4.4) taking into account relevant organizational issues, such as authorized persons and internal structures of the organization;
- g) describe the strategy for modification (see 4.5);
- h) 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;
- i) establish a validation plan comprising:
- results of previous verification;
 - 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 SCS shall 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 6 The validation plan indicates whether the SCS and its subsystems are to be subject to routine testing, type testing and/or sample testing.

4.4 Configuration management

The main operational aspects of configuration management are

- **identification** of the structure of the SCS, identifies e.g. system, subsystems, functions, function blocks, management documents, tools for creating a baseline;
- **controlling** of the release of an element created during each lifecycle phase at a specific point in time;
- **recording** and **reporting** of the status of each element which is and/or will be part of a baseline;
- **audit** and **review** of all elements and maintaining consistency among all elements of a baseline.

Procedures shall be developed for configuration management of the SCS during the overall, SCS system and software safety lifecycle phases, including in particular:

- a) the point, in respect of specific phases, at which formal configuration control is to be implemented;
- b) the procedures to be used for uniquely identifying all constituent parts of hardware and software;
- c) the procedures for preventing unauthorized items from entering service.

The configuration management procedures shall be implemented in accordance with the functional safety plan (see 4.3).

The procedures for an appropriate change-control-process shall consider the requirements of procedures for defining a unique baseline of each version of the SCS.

4.5 Modification

If a modification is to be implemented, then relevant activities shall be identified specifically and an action plan shall be prepared and documented before carrying out any modification.

NOTE 1 The request for a modification can arise from, for example:

- safety requirements specification changed;
- conditions of actual use;
- incident/accident experience;
- change of material processed;
- obsolescence;
- modifications of the machine or of its operating modes.

NOTE 2 Interventions (e.g. adjustment, setting, repairs) on the SCS made in accordance with the information for use or instruction manual for the SCS are not considered to be a modification in the context of this subclause.

The reason(s) for the request for a modification shall be documented.

The effect of the requested modification shall be analysed to establish the effect on the safety function.

The modification impact analysis and the effect on the functional safety of the SCS shall be documented.

All accepted modifications that have an effect on the SCS shall initiate a return to an appropriate design phase for its hardware and/or for its software (e.g. specification, design, integration, installation, commissioning, and validation). All subsequent phases and management procedures shall then be carried out in accordance with the procedures specified for the specific phases in this document. All relevant documents shall be revised, amended and reissued accordingly.

5 Specification of a safety function

5.1 Objective

This clause sets out the procedures to specify the requirements of safety function(s) to be implemented by the SCS.

5.2 Safety requirements specification (SRS)

5.2.1 General

Each safety function shall be specified by:

- functional requirements specification (see 5.2.3);
- safety integrity requirements specification (see 5.2.5)

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

Where a product standard specifies the safety requirements for the design of an SCS or subsystem (e.g. ISO 13851 for two-hand control devices), these should be considered.

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 SCS:

- 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 of machine,
 - cycle time,
 - response time performance,
 - environmental conditions,
 - interaction of person(s) with the machine (e.g. repairing, setting, cleaning);
- all information relevant to the safety function(s) which can have an influence on the SCS design including, for example:
 - a description of the behaviour of the machine that a safety function is intended to achieve or to prevent;
 - all interfaces between the safety functions, and between safety functions and any other function (either within or outside the machine);
 - required fault reaction functions of the safety function.

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

5.2.3 Functional requirements specification

The functional requirements specification shall describe details of each safety function to be performed including as applicable:

- a description of each safety function;
- the condition(s) (e.g. operating mode) of the machine in which the safety function shall be active, disabled, configured or parameterized;
- the priority of those functions that can be simultaneously active and that can cause conflicting action;
- the reset of a safety function;
- the frequency of operation of each safety function (rate of operating cycles, duty cycle);
- demand mode of operation;

NOTE 1 For definitions refer to 3.2.26, 3.2.27, 3.2.28.

- the required response time of each safety function;
- the interface(s) of the safety functions to other machine functions;

NOTE 2 This could include a description of methods intended to give status information to users of the machinery.

- 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;
- tests and any associated facilities (e.g. test equipment, test access ports);
- a description of the operating environment (e.g. electromagnetic immunity, temperature, humidity, dust, chemical substances, mechanical vibration and shock);

NOTE 3 The specification of the electromagnetic environmental condition is within the scope of IEC 61000-1-2. The electromagnetic environment is defined as the totality of electromagnetic phenomena existing at a particular location. These phenomena can vary over time.

The electromagnetic environment is influenced by, for example:

- fixed and moving sources of electromagnetic energy,
- low, medium and high voltage equipment,
- control, signalling, communication and power systems,
- intentional radiators,
- physical processes (e.g. atmospheric discharges, switching actions),
- random or infrequent transients,

which all can produce disturbances that adversely impact the safety-related system or element under consideration.

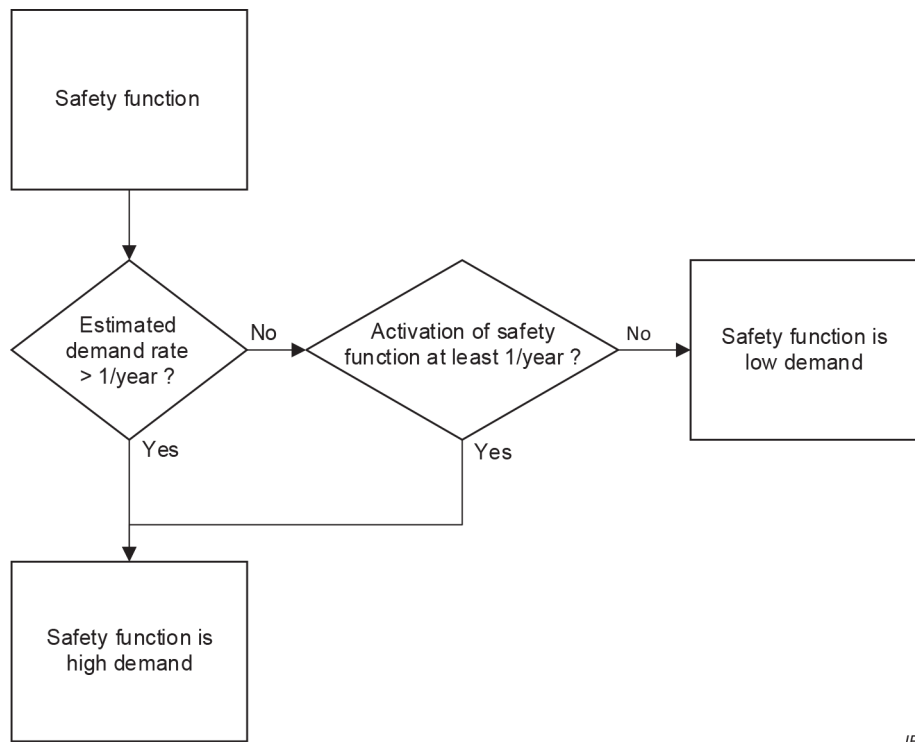
- rate of operating cycles, duty cycle, and/or utilisation category, for devices intended for use in the safety function;

NOTE 4 The duty cycle of subsystems or subsystem elements can be higher than required for the safety function, e.g. when used also for non-safety-related machine functions (the total number of cycles is to be considered).

- other specific requirements which can impact functional safety.

5.2.4 Estimation of demand mode of operation

The demand mode of operation shall be estimated by applying the respective definitions. While low demand mode operation is possible for a safety function, this document concentrates on high demand and continuous mode. When demand rate is estimated to be low, a high demand mode can be assumed by activation of the safety function at least once per year. Then apply this document for the design. This is a straightforward application of the definition and shown in Figure 5 as a workflow.



IEC

Figure 5 – By activating a low demand safety function at least once per year it can be assumed to be high demand

5.2.5 Safety integrity requirements specification

The safety integrity requirements for each safety function shall be derived from the risk assessment to ensure the necessary risk reduction can be achieved. In this document, a safety integrity requirement is expressed as a target failure measure for the *PFH*.

The required safety integrity for each safety function to be carried out by an SCS shall be specified in terms of SIL according to Table 3 and documented.

Table 3 – SIL and limits of *PFH* values

SIL	Limits of <i>PFH</i> values (1/h)
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

The determination of the required safety integrity is the result of the risk assessment and refers to the amount of the risk reduction to be carried out by the SCS. Examples of a methodology are given in Annex A.

NOTE 1 Where a product standard specifies a required SIL for a safety function then this takes precedence over Annex A.

NOTE 2 Further guidance on relationship between risk assessment according to ISO 12100 and product standards is provided in ISO TR 22100-1.

6 Design of an SCS

6.1 General

The SCS shall be designed in accordance with the safety requirements specification (see 5.2), using one or several subsystems by:

- selection of subsystems (see 6.2, 6.3 and Clause 7);
- determining the safety integrity (see 6.4);
- complying to the requirements of the systematic safety integrity of the SCS (see 6.5), including, where applicable, electromagnetic immunity (see 6.6), security (see 6.8), periodic testing (see 6.9) and, software (see 6.7 and Clause 8).

6.2 Subsystem architecture based on top down decomposition

The following Clause 6 describes the design process of an SCS. An SCS can include:

- one or several pre-designed subsystem(s), and/or
- one or several subsystem(s) developed according to this document, based on subsystem element(s) (see Clause 7).

NOTE 1 The designer of a pre-designed subsystem can be a manufacturer of the machine or a device manufacturer.

NOTE 2 The relevant safety integrity characteristic values come from the designer of pre-designed subsystem.

6.3 Basic methodology – Use of subsystem

6.3.1 General

Each safety function identified in the risk reduction process (see Clause 4) is performed by an SCS consisting of one or several subsystems. A failure of any subsystem will result in the loss of the whole safety function. Subclause 6.2 describes the principle of this allocation task.

Where an SCS or part of an SCS (i.e. its subsystem(s)) is to implement both safety functions 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 safety functions and other functions is sufficiently independent (i.e. that the normal operation or failure of any other functions do not affect the safety functions).

NOTE 1 Sufficient independence of implementation is 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 SCS. IEC 61508-3:2010, Annex F describes techniques for achieving non-interference between software elements.

For an SCS or its subsystems that implements safety 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 functions of the different safety integrity levels is sufficiently independent.

NOTE 2 Sufficient independence of implementation is established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.

Where digital data communication is used as a part of an SCS implementation, it shall satisfy the relevant requirements of IEC 61508-2:2010, 7.4.11 (which refers to IEC 61784-3 (all parts) for functional safety fieldbuses) in accordance with the SIL target(s) of the safety function(s).