# IEC 62061

Edition 2.2 2026-03

# INTERNATIONAL STANDARD

CONSOLIDATED VERSION

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

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8327-1166-8

IEC 62061:2021-03+AMD1:2024-03+AMD2:2026-03 CSV(en)

**THIS PUBLICATION IS COPYRIGHT PROTECTED**
**Copyright © 2026 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

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

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

**IEC publications search - webstore.iec.ch/advsearchform**
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

**IEC Just Published - webstore.iec.ch/justpublished**
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

**IEC Customer Service Centre - webstore.iec.ch/csc**
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

**IEC Products & Services Portal - products.iec.ch**
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

**Electropedia - www.electropedia.org**
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

**Warning! Make sure that you obtained this publication from an authorized distributor.**

# CONTENTS

FOREWORD ..... 7
INTRODUCTION ..... 9
1 Scope ..... 10
2 Normative references ..... 11
3 Terms, definitions and abbreviations ..... 12
3.1 Alphabetical list of definitions ..... 12
3.2 Terms and definitions ..... 14
3.3 Abbreviations ..... 27
4 Design process of an SCS and management of functional safety ..... 27
4.1 Objective ..... 27
4.2 Design process ..... 28
4.3 Management of functional safety using a functional safety plan ..... 30
4.4 Configuration management ..... 32
4.5 Modification ..... 32
5 Specification of a safety function ..... 33
5.1 Objective ..... 33
5.2 Safety requirements specification (SRS) ..... 33
5.2.1 General ..... 33
5.2.2 Information to be available ..... 33
5.2.3 Functional requirements specification ..... 34
5.2.4 Estimation of demand mode of operation ..... 34
5.2.5 Safety integrity requirements specification ..... 35
6 Design of an SCS ..... 36
6.1 General ..... 36
6.2 Subsystem architecture based on top down decomposition ..... 36
6.3 Basic methodology – Use of subsystem ..... 36
6.3.1 General ..... 36
6.3.2 SCS decomposition ..... 37
6.3.3 Sub-function allocation ..... 38
6.3.4 Use of a pre-designed subsystem ..... 38
6.4 Determination of safety integrity of the SCS ..... 39
6.4.1 General ..... 39
6.4.2 PFH ..... 39
6.5 Requirements for systematic safety integrity of the SCS ..... 40
6.5.1 Requirements for the avoidance of systematic hardware failures ..... 40
6.5.2 Requirements for the control of systematic faults ..... 41
6.6 Electromagnetic immunity ..... 42
6.7 Software based manual parameterization ..... 42
6.7.1 General ..... 42
6.7.2 Influences on safety-related parameters ..... 42
6.7.3 Requirements for software based manual parameterization ..... 43
6.7.4 Verification of the parameterization tool ..... 44
6.7.5 Performance of software based manual parameterization ..... 44
6.8 Security aspects ..... 44
6.9 Aspects of periodic testing ..... 45
7 Design and development of a subsystem ..... 45

7.1 General ..... 45
7.2 Subsystem architecture design ..... 46
7.3 Requirements for the selection and design of subsystem and subsystem elements ..... 47
7.3.1 General ..... 47
7.3.2 Systematic integrity ..... 47
7.3.3 Fault consideration and fault exclusion ..... 50
7.3.4 Failure rate of subsystem element ..... 51
7.4 Architectural constraints of a subsystem ..... 54
7.4.1 General ..... 54
7.4.2 Estimation of safe failure fraction ($SFF$) ..... 55
7.4.3 Behaviour (of the SCS) on detection of a fault in a subsystem ..... 57
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 $PFH$ of subsystems ..... 62
7.6.1 General ..... 62
7.6.2 Methods to estimate the $PFH$ of a subsystem ..... 62
7.6.3 Simplified approach to estimation of contribution of common cause failure (CCF) ..... 63
8 Software ..... 63
8.1 General ..... 63
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 ..... 68
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 ..... 72
8.4.3 Software system design – SW level 2 ..... 73
8.4.4 Module design – SW level 2 ..... 74
8.4.5 Coding – SW level 2 ..... 75
8.4.6 Module test – SW level 2 ..... 75
8.4.7 Software integration testing SW level 2 ..... 76
8.4.8 Software testing SW level 2 ..... 76
8.4.9 Documentation – SW level 2 ..... 77
8.4.10 Configuration and modification management process – SW level 2 ..... 77
9 Validation ..... 78
9.1 Validation principles ..... 78
9.1.1 Validation plan ..... 81
9.1.2 Use of generic fault lists ..... 81

9.1.3 Specific fault lists ..... 81
9.1.4 Information for validation ..... 82
9.1.5 Validation record ..... 82
9.2 Analysis as part of validation ..... 83
9.2.1 General ..... 83
9.2.2 Analysis techniques ..... 83
9.2.3 Verification of safety requirements specification (SRS) ..... 83
9.3 Testing as part of validation ..... 84
9.3.1 General ..... 84
9.3.2 Measurement accuracy ..... 84
9.3.3 More stringent requirements ..... 85
9.3.4 Test samples ..... 85
9.4 Validation of the safety function ..... 85
9.4.1 General ..... 85
9.4.2 Analysis and testing ..... 86
9.5 Validation of the safety integrity of the SCS ..... 86
9.5.1 General ..... 86
9.5.2 Validation of subsystem(s) ..... 86
9.5.3 Validation of measures against systematic failures ..... 87
9.5.4 Validation of safety-related software ..... 87
9.5.5 Validation of combination of subsystems ..... 88
10 Documentation ..... 88
10.1 General ..... 88
10.2 Technical documentation ..... 88
10.3 Information for use of the SCS ..... 90
10.3.1 General ..... 90
10.3.2 Information for use given by the manufacturer of subsystems ..... 90
10.3.3 Information for use given by the SCS integrator ..... 91
Annex A (informative) Determination of required safety integrity ..... 93
A.1 General ..... 93
A.2 Matrix assignment for the required SIL ..... 93
A.2.1 Hazard identification/indication ..... 93
A.2.2 Risk estimation ..... 93
A.2.3 Severity (Se) ..... 94
A.2.4 Probability of occurrence of harm ..... 94
A.2.5 Class of probability of harm (Cl) ..... 97
A.2.6 SIL assignment ..... 97
A.3 Overlapping hazards ..... 99
Annex B (informative) Example of SCS design methodology ..... 100
B.1 General ..... 100
B.2 Safety requirements specification ..... 100
B.3 Decomposition of the safety function ..... 100
B.4 Design of the SCS by using subsystems ..... 101
B.4.1 General ..... 101
B.4.2 Subsystem 1 design – “guard door monitoring” ..... 101
B.4.3 Subsystem 2 design – “evaluation logic” ..... 103
B.4.4 Subsystem 3 design – “motor control” ..... 104
B.4.5 Evaluation of the SCS ..... 104
B.4.6 PFH ..... 105

B.5 Verification ..... 105
B.5.1 General ..... 105
B.5.2 Analysis ..... 105
B.5.3 Tests ..... 106
Annex C (informative) Examples of $MTTF_D$ values for single components ..... 107
C.1 General ..... 107
C.2 Good engineering practices method ..... 107
C.3 Hydraulic components ..... 107
C.4 $MTTF_D$ of pneumatic, mechanical and electromechanical components ..... 108
Annex D (informative) Examples for diagnostic coverage ($DC$) ..... 110
Annex E (informative) Methodology for the estimation of susceptibility to common cause failures (CCF) ..... 112
E.1 General ..... 112
E.2 Methodology ..... 112
E.2.1 Requirements for CCF ..... 112
E.2.2 Estimation of effect of CCF ..... 112
Annex F (informative) Guideline for software level 1 ..... 115
F.1 Software safety requirements ..... 115
F.2 Coding guidelines ..... 116
F.3 Specification of safety functions ..... 117
F.4 Specification of hardware design ..... 118
F.5 Software system design specification ..... 120
F.6 Protocols ..... 122
Annex G (informative) Examples of safety functions ..... 125
Annex H (informative) Simplified approaches to evaluate the $PFH$ value of a subsystem ..... 126
H.1 Table allocation approach ..... 126
H.2 Simplified formulas for the estimation of $PFH$ ..... 128
H.2.1 General ..... 128
H.2.2 Basic subsystem architecture A: single channel without a diagnostic function ..... 128
H.2.3 Basic subsystem architecture B: dual channel without a diagnostic function ..... 129
H.2.4 Basic subsystem architecture C: single channel with a diagnostic function ..... 129
H.2.5 Basic subsystem architecture D: dual channel with a diagnostic function(s) ..... 135
H.3 Parts count method ..... 136
Annex I (informative) The functional safety plan and design activities ..... 137
I.1 General ..... 137
I.2 Example of a machine design plan including a safety plan ..... 137
I.3 Example of activities, documents and roles ..... 137
Annex J (informative) Independence for reviews and testing/verification/validation activities ..... 142
J.1 Software design ..... 142
J.2 Validation ..... 142
Bibliography ..... 144

Figure 1 – Scope of this document ..... 11

Figure 2 – Integration within the risk reduction process of ISO 12100 (extract) ..... 28
Figure 3 – Iterative process for design of the safety-related control system ..... 29
Figure 4 – Example of a combination of subsystems as one SCS ..... 30
Figure 5 – By activating a low demand safety function at least once per year it can be assumed to be high demand ..... 35
Figure 6 – Examples of typical decomposition of a safety function into sub-functions and its allocation to subsystems ..... 38
Figure 7 – Example of safety integrity of a safety function based on allocated subsystems as one SCS ..... 39
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 ..... 61
Figure 11 – Basic subsystem architecture D logical representation ..... 61
Figure 12 – V-model for SW level 1 ..... 65
Figure 13 – V-model for software modules customized by the designer for SW level 1 ..... 65
Figure 14 – V-model of software safety lifecycle for SW level 2 ..... 71
Figure 15 – Overview of the validation process ..... 80
Figure A.1 – Parameters used in risk estimation ..... 93
Figure A.2 – Example proforma for SIL assignment process ..... 99
Figure B.1 – Decomposition of the safety function ..... 101
Figure B.2 – Overview of design of the subsystems of the SCS ..... 101
Figure F.1 – Plant sketch ..... 117
Figure F.2 – Principal module architecture design ..... 120
Figure F.3 – Principal design approach of logical evaluation ..... 121
Figure F.4 – Example of logical representation (program sketch) ..... 122
Figure H.1 – Basic subsystem architecture A logical representation ..... 128
Figure H.2 – Basic subsystem architecture B logical representation ..... 129
Figure H.3 – Basic subsystem architecture C logical representation ..... 129
Figure H.4 – Correlation of basic subsystem architecture C and the pertinent fault handling function ..... 130
Figure H.5 – Basic subsystem architecture C with external fault handling function ..... 131
Figure H.6 – Basic subsystem architecture C with external fault diagnostics ..... 132
Figure H.7 – Basic subsystem architecture C with external fault reaction ..... 132
Figure H.8 – Basic subsystem architecture C with internal fault diagnostics and internal fault reaction ..... 133
Figure H.9 – Basic subsystem architecture D logical representation ..... 135
Figure I.1 – Example of a machine design plan including a safety plan ..... 137
Figure I.2 – Example of activities, documents and roles *(1 of 2)* ..... 139

Table 1 – Terms used in IEC 62061 ..... 12
Table 2 – Abbreviations used in IEC 62061 ..... 27
Table 3 – SIL and limits of $PFH$ values ..... 35
Table 4 – Required SIL and $PFH$ of pre-designed subsystem ..... 39
Table 5 – Relevant information for each subsystem ..... 46

Table 6 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem ..... 55
Table 7 – Overview of basic requirements and interrelation to basic subsystem architectures ..... 62
Table 8 – Different levels of application software ..... 63
Table 9 – Documentation of an SCS ..... 89
Table A.1 – Severity (Se) classification ..... 94
Table A.2 – Frequency and duration of exposure (Fr) classification ..... 95
Table A.3 – Probability (Pr) classification ..... 96
Table A.4 – Probability of avoiding or limiting harm (Av) classification ..... 97
Table A.5 – Parameters used to determine class of probability of harm (Cl) ..... 97
Table A.6 – Matrix assignment for determining the required SIL (or $PL_r$) for a safety function ..... 98
Table B.1 – Safety requirements specification – example of overview ..... 100
Table B.2 – Systematic integrity – example of overview ..... 105
Table B.3 – Verification by tests ..... 106
Table C.1 – Standards references and $MTTF_D$ or $B_{10D}$ values for components ..... 108
Table D.1 – Estimates for diagnostic coverage ($DC$) (1 of 2) ..... 110
Table E.1 – ~~Criteria for estimation of CCF~~ Estimation of CCF factor *(β)* ..... 113
Table E.2 – Criteria for estimation of CCF ..... 114
Table F.1 – Example of relevant documents related to the simplified V-model ..... 115
Table F.2 – Examples of coding guidelines ..... 116
Table F.3 – Specified safety functions ..... 118
Table F.4 – Relevant list of input and output signals ..... 119
Table F.5 – Example of simplified cause and effect matrix ..... 122
Table F.6 – Verification of software system design specification ..... 123
Table F.7 – Software code review ..... 123
Table F.8 – Software validation ..... 124
Table G.1 – Examples of typical safety functions ..... 125
Table H.1 – Allocation of $PFH$ value of a subsystem ..... 127
Table H.2 – Relationship between $B_{10D}$, operations and $MTTF_D$ ..... 128
Table H.3 – Minimum value of $1/\lambda_{D\ FH}$ for the applicability of $PFH$ equation (H.~~4~~3) ..... 133
Table J.1 – Minimum levels of independence for review, testing and verification activities ..... 142
Table J.2 – Minimum levels of independence for validation activities ..... 142

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 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.

This consolidated version of the official IEC Standard and its amendments has been prepared for user convenience.

IEC 62061 edition 2.2 contains the second edition (2021-03) [documents 44/885/FDIS and 44/888/RVD], its amendment 1 (2024-03) [documents 44/1020/FDIS and 44/1024/RVD] and its amendment 2 (2026-03) [documents 44/1074/FDIS and 44/1081/RVD].

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

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 amendments 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.

# 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.

# 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 IEC ~~TR~~ TS 63074.

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

Figure 1 illustrates the scope of this document.

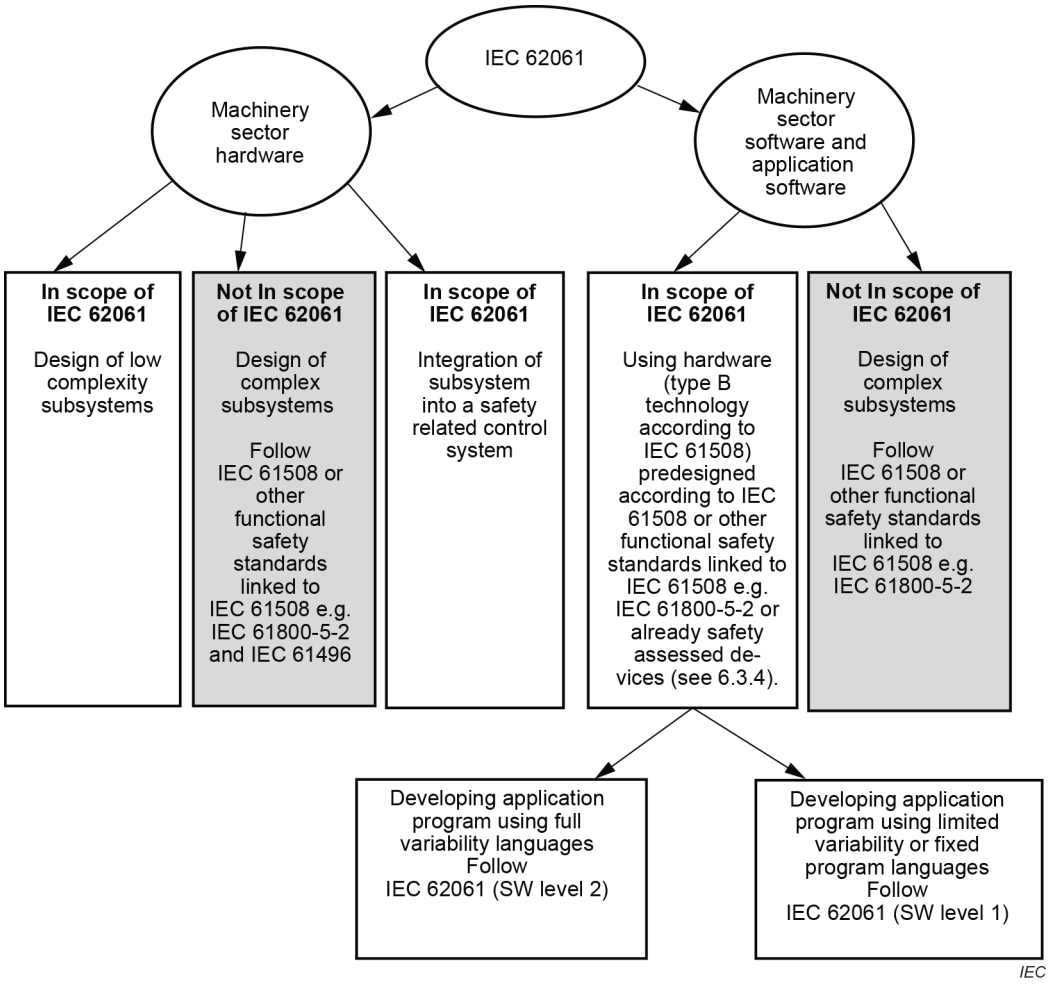



**Figure 1 – Scope of this document**

## 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 ($PFD_{\text{avg}}$) | 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 [t1, t2] is generally noted by U (t1, t2).

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 $\gamma$).

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, $\lambda_{DD}$ is the detected dangerous failure rate and $\lambda_{Dtotal}$ 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, 3.6.47, modified – Terminology adapted to machinery ~~and figure replaced by textual description and ISO 12100-1:2010, 3.34~~]

**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 supressed 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.