IEC TS 63394

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

colour inside

Safety of machinery – Guidelines on functional safety of safety-related control system



IEC TS 63394:2023-02(en)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2023 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 It also gives information on projects, replaced and withdrawn publications.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. 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 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TS 63394

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

colour inside

Safety of machinery – Guidelines on functional safety of safety-related control system

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 29.020; 25.040.99

ISBN 978-2-8322-6533-8

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

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 9
INTRODUCTION 11
1 Scope 12
2 Normative references 12
3 Terms and definitions 13
3.1 Terms and definitions 13
3.2 Alphabetical list of terms, definitions and abbreviated terms 26
4 Typical classification of safety functions in safety of machinery 28
4.1 General 28
4.1.1 Overview 28
4.1.2 Risk assessment and risk reduction according to ISO 12100 28
4.1.3 Risk reduction and interconnection to SCS and SRP/CS 29
4.1.4 Basic assumptions for risk reduction in machinery 29
4.2 Basic safety assumptions for the design and integration of the SCS or SRP/CS 29
4.3 Safety functions 30
4.3.1 General 30
4.3.2 Risk reduction process by safety functions 30
4.3.3 Typical classification of safety functions 31
4.4 Interrelation between ISO 12100 and IEC 62061 or ISO 13849-1 32
4.4.1 General 32
4.4.2 Input information in accordance with IEC 62061 or ISO 13849-1 32
4.4.3 Output information from IEC 62061 or ISO 13849-1 33
4.5 Safety functions for protection of persons 34
4.5.1 General 34
4.5.2 Safety functions for protection of persons based on guards and protective devices 34
4.6 Other safety functions to prevent hazardous situations 35
4.6.1 General 35
4.6.2 Other safety functions 35
4.7 Safety functions for protection of the integrity of the machine 36
4.7.1 General 36
4.7.2 Safety functions for the protection of integrity of the machine 36
4.8 Safety functions and Type-C standards 36
5 Demand mode of operation related to safety functions 37
5.1 General 37
5.2 High demand or continuous mode of operation 37
5.2.1 General 37
5.2.2 Approach of IEC 62061 and ISO 13849-1 38
5.2.3 Rarely activated safety functions 38
5.3 Low demand mode of operation 39
5.3.1 General 39
5.3.2 Approach of IEC 62061 and ISO 13849-1 40
6 Design process of safety functions 40
6.1 General 40
6.2 Design procedure 40
6.3 Evaluation of required safety integrity 41

6.4 Decomposition of a safety function 41
6.5 Subsystem design 41
6.5.1 Architectural constraints 41
6.5.2 Fault accumulation and undetected faults 43
6.5.3 Evaluation of PFH 43
6.6 Examples of safety functions 45
7 Verification procedures for safety functions 45
7.1 General 45
7.2 Verification of the test interval of a safety function 45
7.3 Verification procedures 46
7.4 Initial verification 46
7.5 Periodic verification 47
7.5.1 General 47
7.5.2 Frequency of periodic verification 48
7.6 Verification reporting 49
Annex A (informative) Risk assessment and risk reduction according to ISO 12100 50
A.1 General 50
A.2 Risk assessment principles 50
A.2.1 General 50
A.2.2 Basic information to be available (as input to risk assessment) 50
A.2.3 Risk analysis 51
A.3 Risk reduction by means of safeguarding and complementary protective measures 55
A.3.1 General 55
A.3.2 Inherently safe design measures 56
A.3.3 Selection of safeguarding and complementary protective measures 56
A.4 Other protective measures (procedure based) 58
A.4.1 General 58
A.4.2 Procedures for maintenance 58
A.4.3 Organizational work procedures 58
A.5 Guards and protective devices according to ISO 12100 59
A.5.1 General 59
A.5.2 Interlocking guard with a start function, with manual reset function 59
A.5.3 Protective device according to ISO 12100 60
A.5.4 Manual local control device (and procedure) 60
A.5.5 Manual parameter selection device (and procedure) 61
A.5.6 Manual operating mode selection device (and procedure) 61
A.5.7 Energy control device (and procedure) 61
A.6 Matrix assignment approach 61
A.6.1 Overview 61
A.6.2 General 62
A.6.3 Methodology of IEC 62061:2021, Annex A 62
A.7 Risk graph approach 63
A.7.1 General 63
A.7.2 Methodology of ISO 13849-1:2015, Annex A with assigned SIL 63
Annex B (informative) Methodology of SCS or SRP/CS design 65
B.1 General 65
B.2 Functional safety plan 65
B.3 Safety requirements specification 66

B.3.1 General 66
B.3.2 Functional requirements 66
B.3.3 Safety integrity requirements 66
B.4 Protection against unexpected start-up 67
B.5 Decomposition of the safety function 67
B.5.1 General 67
B.5.2 Subsystem architecture based on top-down decomposition 67
B.6 Design of the SCS by using subsystems 67
B.7 Requirements for systematic safety integrity 68
B.7.1 General 68
B.7.2 SCS level 68
B.7.3 Subsystem level 70
B.8 Electromagnetic immunity 71
B.9 Software-based manual parameterization 71
B.10 Security aspects 73
B.11 Aspects of testing 73
B.12 Design and development of a subsystem 74
B.12.1 General 74
B.12.2 Subsystem architecture design 74
B.12.3 Fault consideration and fault exclusion 76
B.12.4 Architectural constraints of a subsystem 76
B.12.5 Subsystem design architectures 78
B.12.6 PFH value of subsystems 78
B.13 Validation 78
B.14 Documentation 80
Annex C (informative) Examples of $MTTF_D$ values for single components 83
Annex D (informative) Examples for diagnostic coverage (DC) 84
D.1 General 84
D.2 Influence of cabling, wiring and interconnections 85
D.2.1 General 85
D.2.2 "Serial wiring" 85
D.3 Use of manufacturing process information 86
D.3.1 General 86
D.3.2 Use of expected timing or awaiting of signal status 86
D.4 Typical DC measures 86
Annex E (informative) Measures for the achievement of functional safety with regards to electromagnetic phenomena 88
E.1 General 88
E.2 Measures 88
E.2.1 General 88
E.2.2 Recommendation for electrical/electronic items of equipment (devices or apparatus) 88
E.2.3 Recommendation for the integration of an SCS or SRP/CS into the electrical equipment of the machine 89
Annex F (informative) Guidelines for software 90
F.1 General 90
F.2 Documentation 90
F.3 Activities 92
Annex G (informative) Examples of safety functions 97

G.1 General 97
G.2 Safety functions 97
G.2.1 Basic information 97
G.2.2 Detailed description of safety requirements 98
G.2.3 Example of interlocking guard 99
Annex H (informative) Evaluation of PFH value of a subsystem 101
H.1 General 101
H.2 Table allocation approach (IEC 62061) 101
H.3 Simplified formulas for the estimation of PFH value (IEC 62061) 101
H.4 Approaches of IEC 61508, IEC 62061 and ISO 13849-1 101
H.4.1 General 101
H.4.2 Approach of IEC 61508 102
H.4.3 Approach of IEC 62061 103
H.4.4 Approach of ISO 13849-1:2015, Annex K 103
H.5 Basic considerations regarding exponential and Weibull distributions 107
H.5.1 Exponential distribution 107
H.5.2 Weibull distribution 107
H.6 T_{10} and B_{10} 109
H.6.1 General 109
H.6.2 T_{10} with exponential distribution 109
H.6.3 T_{10} with Weibull distribution 110
H.7 Overview of PFH formulas 112
H.7.1 Definitions 112
H.7.2 Formulas 112
H.7.3 Examples 114
H.8 Methodology for the estimation of CCF 116
H.9 Basic subsystem architecture A (1oo1) 117
H.9.1 General 117
H.9.2 PFH 118
H.9.3 Simplified Weibull approach 118
H.10 Basic subsystem architecture C (1oo1D) 119
H.10.1 General 119
H.10.2 Fault reaction performed by another subsystem 119
H.10.3 Fault reaction to be considered in the subsystem 120
H.10.4 PFH 122
H.10.5 Influence of CCF 122
H.11 Basic subsystem architecture B (1oo2) 123
H.11.1 General 123
H.11.2 PFH 124
H.11.3 Influence of CCF 124
H.12 Basic subsystem architecture D (1oo2D) 124
H.12.1 General 124
H.12.2 PFH evaluation of Term A 126
H.12.3 PFH evaluation of Term B 126
H.12.4 PFH evaluation of Term C and Term D 126
H.12.5 PFH 127
H.12.6 Influence of CCF 127

H.13 Basic subsystem architecture D (1oo2D) with two periods of time consideration 127
H.13.1 General 127
H.13.2 PFH evaluation of Term A 128
H.13.3 PFH evaluation of Term B 128
H.13.4 PFH evaluation of Term C and Term D 128
H.13.5 PFH 129
H.13.6 Influence of CCF 129
Annex I (informative) Commented examples of current regulations 130
I.1 General 130
I.2 European Union 130
I.2.1 General European legislation 130
I.2.2 New proposed machinery regulation (under preparation) 130
I.2.3 Relevant legislation 131
I.2.4 Duties of the manufacturer of the machine 131
I.3 North America – USA 132
I.4 North America – Canada 132
I.5 South America – Brazil 132
I.6 China 133
I.7 Japan 133
Annex J (informative) Combination of modes of operation 134
J.1 General 134
J.2 Basic approaches with different modes of operation 134
J.2.1 General 134
J.2.2 Risk reduction measures on low demand mode of operation 135
J.3 Use of subsystems in different modes of operation 136
J.3.1 General 136
J.3.2 Example with different modes of operation 136
J.3.3 Subsystem(s) used for different modes of operation 138
Bibliography 141

Figure 1 – Integration within the risk reduction process of ISO 12100 29
Figure 2 – Decomposition of an SCS or SRP/CS 30
Figure 3 – Risk reduction process by safety functions 31
Figure 4 – High demand mode of operation 38
Figure 5 – Process for determining high demand mode of operation 39
Figure 6 – Low demand mode of operation 40
Figure A.1 – SIL assignment approach 63
Figure A.2 – Risk graph approach of ISO 13849-1:2015, Figure A.1 with assigned SIL 64
Figure B.1 – Example of decomposition of a safety function 68
Figure B.2 – Possible effects of security risk(s) to a SCS (IEC TR 63074:2019, Figure 2) 73
Figure B.3 – Rarely activated safety functions and mode of operation of subsystems 76
Figure H.1 – Cumulative distribution functions (CDF) 111
Figure H.2 – Common cause failure 117
Figure H.3 – Basic subsystem architecture A (1oo1) reliability block diagram 117
Figure H.4 – Unavailability function of basic subsystem architecture A (1oo1) 117

Figure H.5 – 1oo1 reliability block diagram, simplified Weibull approach 118
Figure H.6 – Basic subsystem architecture C (1oo1D) logical view with safe state initiation using another subsystem 119
Figure H.7 – Basic subsystem architecture C (1oo1D) reliability block diagram with safe state initiation using another subsystem 119
Figure H.8 – Unavailability functions of basic subsystem architecture C (1oo1D) 120
Figure H.9 – Basic subsystem architecture C (1oo1D) logical view with fault reaction 120
Figure H.10 – Basic subsystem architecture C (1oo1D) reliability block diagram with fault reaction 121
Figure H.11 – Unavailability functions of basic subsystem architecture C (1oo1D) 121
Figure H.12 – Basic subsystem architecture B (1oo2) reliability block diagram 123
Figure H.13 – Unavailability functions of basic subsystem architecture B (1oo2) 123
Figure H.14 – Basic subsystem architecture D (1oo2D) reliability block diagram 125
Figure H.15 – Unavailability functions of basic subsystem architecture D (1oo2D) 125
Figure J.1 – Basic approach in high demand or continuous mode of operation based on IEC 61508 (and IEC 62061) 134
Figure J.2 – Basic approach in low demand mode of operation based on IEC 61508 (and IEC 61511) 135
Figure J.3 – Functional view 137
Figure J.4 – Logical view 137
Figure J.5 – Decomposition view 138
Figure J.6 – Quantitative SIL evaluation using the approach of ratio of probability of failures of each subsystem 139
Figure J.7 – Example of quantitative SIL evaluation using the approach of ratio of probability of failures of each subsystem 140

Table 1 – Terms used in this document 26
Table 2 – Input information for the safety requirements specification (SRS) 33
Table 3 – Output information from SCS or SRP/CS design on overall risk assessment 33
Table 4 – Safety functions for protection of persons 34
Table 5 – Other safety functions 35
Table 6 – Safety functions for the protection of integrity of the machine 36
Table 7 – Architectural constraints for high demand mode of operation 42
Table A.1 – Basic information for risk assessment according to ISO 12100 51
Table A.2 – Determination of limits of machinery according to ISO 12100 52
Table A.3 – Principles of hazard identification according to ISO 12100 53
Table A.4 – Risk estimation according to ISO 12100 54
Table A.5 – Additional considered aspects during risk estimation according to ISO 12100 54
Table A.6 – Guards according to ISO 12100 59
Table A.7 – Examples of protective devices according to ISO 12100 60
Table B.1 – Overview functional safety plan 65
Table B.2 – Overview of basic functional requirements 66
Table B.3 – SIL and limits of **PFH** values 67
Table B.4 – Avoidance of systematic failures (SCS or SRP/CS level) 69
Table B.5 – Control of systematic failures (SCS or SRP/CS level) 69

Table B.6 – Avoidance of systematic failures (subsystem level) 70
Table B.7 – Control of systematic failures (subsystem level) 71
Table B.8 – Software-based manual parameterization 72
Table B.9 – Cause and effects of rarely activated safety functions 76
Table B.10 – Architectural constraints and basic requirements on a subsystem 77
Table B.11 – Overview of validation process with required information 79
Table B.12 – Technical documentation based on the design process (Table 9 of IEC 62061:2021, modified) 81
Table B.13 – Overview of documentation 82
Table C.1 – $MTTF_D$ or B_{10D} values for components (derived from ISO 13849-1:2015) 83
Table C.2 – Relationship of λ_D, $MTTF_D$ and B_{10D} 83
Table D.1 – Measures to prevent of short circuit 85
Table D.2 – DC values and recommended measures 87
Table E.1 – Non-exhaustive list of recommendations regarding EMI measures for integration of devices or equipment into the electrical equipment of the machine 89
Table F.1 – Documents for SW level 1 and SW level 2 90
Table F.2 – Coding guidelines 91
Table F.3 – Overview of protocols 92
Table F.4 – SW level 1 – Overview of basic activities 93
Table F.5 – SW level 2 – Overview of basic activities (1/2) 94
Table F.5 – SW level 2 – Overview of basic activities (1/2) (continued) 95
Table F.6 – SW level 2 – Overview of basic activities (2/2) 96
Table G.1 – Examples of safety functions and associated safety-related devices 97
Table G.2 – Basic information related to the safety requirements specification 98
Table G.3 – Example of safety-related parameters for a safety function with required SIL 1 100
Table G.4 – Example of safety-related parameters for a safety function with required SIL 3 100
Table H.1 – Formulas for basic subsystem architecture A (1oo1) 112
Table H.2 – Formulas for basic subsystem architecture C (1oo1D) 113
Table H.3 – Formulas for basic subsystem architecture B (1oo2) 113
Table H.4 – Formulas for basic subsystem architecture D (1oo2D) 114
Table H.5 – Examples of PFH values based on B_{10D} 115
Table H.6 – Examples of PFH values based on T_{10D} and B_{10D} 116
Table J.1 – $PFD_{avg\ max}$ and PFH_{max} for respective target SIL 140

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SAFETY OF MACHINERY – GUIDELINES ON 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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TS 63394 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
44/980/DTS	44/989/RVDTS

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

The language used for the development of this Technical Specification 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 will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document 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

In the context of the safety of machinery, the sector standard IEC 62061, along with ISO 13849-1, provides requirements and guidance to the manufacturers of machines to design, develop and integrate a safety-related control system (SCS) or safety-related parts of control systems (SRP/CS), respectively, including input devices and final elements whatever the technology (mechanical, pneumatic, hydraulic and electrical technologies).

The following aspects are relevant:

– the classification of safety functions,

– the architecture of the realization of safety functions,

– the modes of operation of safety functions,

– the calculation based on the used technology.

Therefore, safety functions can be classified as follows:

– Safety functions that stop the dangerous movement(s) of the machine and that are mainly performed by SCS or SRP/CS of machines for the protection of persons. Typical examples are interlocking guards, sensitive protective equipment, two-hand control devices and emergency stop.

– Safety functions that protect the integrity of the machine against its destruction and that in a second step can have an impact on the protection of persons. Typical examples are protective devices, devices for limiting pressure or temperature (also defined as "safety-related parameters", e.g. position, speed, temperature or pressure, deviate from limits defined in the control system).

– Other safety functions that are not covered by the two previous cases.

NOTE 1 The different kinds of safety functions are defined and in line with the classifications and definitions of ISO 12100 and ISO 13849-1.

The subsystem architectures to perform safety function(s) are considered.

NOTE 2 In IEC 62061:2021, information is introduced to map SIL (Safety Integrity Level) classification of IEC 62061/IEC 61508 and classification of ISO 13849-1 in terms of categories, architectures, designated architectures and PL (Performance Level). In order to allow backward compatibility, these different criteria are considered in this document.

Depending on the mode of operation of the safety function, criteria and calculations will be considered in order to fulfil the requirements of this document and in order to be in line with existing regulations (e.g. such as recommendations for use in Europe) and other requirements already defined in existing standards, for example on test periodicity.

In order to consider mechanical, pneumatic, hydraulic and electrical technologies, applications for the safety functions, architectures and mode of operation, the associated calculations are evaluated.

NOTE 3 For example, most calculations inside standards are based on the exponential law that is typically applicable to electronic technology. For mechanic or other technologies, Weibull distribution is applied and exponential distribution is not used, except under restrictions.

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

1 Scope

In the context of the safety of machinery, the sector standard IEC 62061, along with ISO 13849-1, provides requirements to manufacturers of machines for the design, development and integration of safety-related control systems (SCS) or safety-related parts of control systems (SRP/CS), depending on technology used (mechanical, pneumatic, hydraulic or electrical technologies) to perform safety function(s). This document does not replace ISO 13849-1 and IEC 62061. This document gives additional guidance to the application of IEC 62061 or ISO 13849-1. This document:

– gives guidelines and specifies additional requirements for specific safety functions based on the methodology of ISO 12100, which are relevant in machinery and respecting typical boundary conditions of machinery;

– considers safety functions which are designed for high demand mode of operation yet are rarely operated, called rarely activated safety functions;

NOTE 1 IEC 62061:2021 completely covers high demand. However, other safety functions related to the protection of the machine itself and indirectly of persons are considered more in detail in this document.

– gives additional information for the calculation of failure rates using other (non-electronic) technologies based e.g. on Weibull distribution, because all the formula defined in IEC 62061 and ISO 13849-1 are based on exponential distribution.

Therefore, the basis for these guidelines and additional requirements is

– a typical classification of safety functions;

– a consideration of typical architectures used for designing safety functions;

– a consideration of modes of operation of safety functions;

– the derivation and evaluation of PFH formulas for subsystems considering the used technology.

NOTE 2 These guidelines can also be used for application of ISO 13849-1 for the design process of SRP/CS.

This document does not address low demand mode of operation according to IEC 61508.

This document does not take into account either layer of protection analysis (LOPA) or basic process control system (BPCS), according to IEC 61511 as a risk reduction measure.

This document considers all lifecycle phases of the machine regarding functional safety, and SCS or SRP/CS.

NOTE 3 The user of the machine needs information from the machine manufacturer for the safe operation of the machine, e.g. useful lifetime of components, maintenance information, testing of safety functions if necessary.

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 62061:2021, *Safety of machinery – Functional safety of safety-related control systems*

IEC TR 63074:2019, *Safety of machinery – Security aspects related to functional safety of safety-related control systems*

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

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

ISO 13850:2015, *Safety of machinery – Emergency stop function – Principles for design*

ISO 13851:2019, *Safety of machinery – Two-hand control devices – Principles for design and selection*

ISO 14118:2017, *Safety of machinery – Prevention of unexpected start-up*

ISO 14119:2013, *Safety of machinery – Interlocking devices associated with guards – Principles for design and selection*

3 Terms and definitions

3.1 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

3.1.1
application software
software specific to the application, that is implemented by the designer of the SCS or SRP/CS, generally containing logic sequences, limits and expressions that control the appropriate input, output, calculations, and decisions necessary to meet the SCS or SRP/CS functional requirements

[SOURCE: IEC 62061:2021, 3.2.59, modified – "or SRP/CS" added to the definition]

3.1.2
architectural constraint
set of architectural requirements that limit the SIL that can be claimed for a subsystem

[SOURCE: IEC 62061:2021, 3.2.46]

3.1.3
architecture
specific configuration of hardware and software elements in an SCS or SRP/CS

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

3.1.4
average frequency of a dangerous failure per hour
PFH
average frequency of dangerous failure of an SCS or SRP/CS to perform a specified safety function over a given period of time

Note 1 to entry: The term PFH corresponds to the probability of dangerous failures per hour (PFH_D) of IEC 62061:2005, IEC 62061:2005/AMD1:2012, and IEC 62061:2005/AMD2:2015.

Note 2 to entry: The term "average probability of dangerous failure per hour" PFH_D is used in ISO 13894-1 and can be considered to be identical to the PFH according to the IEC 61508 series.

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

3.1.5
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 – Abbreviated term added, system failure replaced by failure of a safety function]

3.1.6
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]

3.1.7
continuous mode of operation
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 IEC 62061:2021, 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 – The definition "continuous mode of operation" taken from the broader definition of "mode of operation", notes added]

3.1.8
dangerous failure
failure of an SCS or SRP/CS, 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]

3.1.9
demand
event that causes the SCS or SRP/CS 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 or SRP/CS 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.

[SOURCE: IEC 62061:2021, 3.2.25, modified – "or SRP/CS" added]

3.1.10
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:

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

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 – The second part of the definition has been moved to a note to entry]

3.1.11
diagnostic function
function intended to detect faults in the SCS or SRP/CS 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.

[SOURCE: IEC 62061:2021, 3.2.19, modified – "or SRP/CS" added]

3.1.12
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]

3.1.13
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 SRP/CS or subsystem, as opposed to the application software

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

[SOURCE: IEC 62061:2021, 3.2.60, modified – "or SRP/CS" added]

3.1.14
failure
termination of the ability of an item (SCS or SRP/CS, 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: ISO 12100:2010, 3.34, modified – "(SCS or SRP/CS, a subsystem or a subsystem element)" added and note 1 to entry added]

3.1.15
fault
abnormal condition that may cause a reduction in, or loss of, the capability of an SCS or SRP/CS, a subsystem, or a subsystem element to perform a required function

Note 1 to entry: In IEC 60050-192:2015, 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]

3.1.16
fault reaction function
function that is initiated when a fault within an SCS or SRP/CS is detected by the SCS or SRP/CS diagnostic function

[SOURCE: IEC 62061:2021, 3.2.20, modified – "or SRP/CS" added to the definition]

3.1.17
fault tolerance
ability of an SCS or SRP/CS, 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, note to entry omitted]

3.1.18
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 omitted and link to process sector deleted]

3.1.19
functional safety
part of the overall safety of the machine and the machine control system that depends on the correct functioning of the SCS or SRP/CS and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – Using terms machine, machine control system, SCS and SRP/CS]

3.1.20
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 62061:2021, 3.2.35]

3.1.21
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, modified – Terminology adapted to machinery, note 1 shortened, note 2 added]

3.1.22
harm
physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5]

3.1.23
hazard
potential source of harm

Note 1 to entry: The term "hazard" can be qualified in order to define its origin (for example, mechanical hazard, electrical hazard) or the nature of the potential harm (for example, electric shock hazard, cutting hazard, toxic hazard, fire hazard).

Note 2 to entry: The hazard envisaged by this definition either

- is permanently present during the intended use of the machine (for example, motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature), or
- can appear unexpectedly (for example, explosion, crushing hazard as a consequence of an unintended/unexpected start-up, ejection as a consequence of a breakage, fall as a consequence of acceleration/deceleration).

Note 3 to entry: The French term "phénomène dangereux" should not be confused with the term "risque", which was sometimes used instead in the past.

[SOURCE: ISO 12100:2010, 3.6]

3.1.24
hazardous situation
circumstance in which a person is exposed to at least one hazard

Note 1 to entry: The exposure can result in harm immediately or over a period of time.

[SOURCE: ISO 12100:2010, 3.10]

3.1.25
hazard zone
danger zone
any space within and/or around machinery in which a person can be exposed to a hazard

[SOURCE: ISO 12100:2010, 3.11]

3.1.26
high demand mode of operation
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 IEC 62061:2021, 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 – The definition of "high demand mode of operation" taken from the definition of "mode of operation", notes added]

3.1.27
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.

3.1.28
low demand mode of operation
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 – The definition of "low demand mode of operation" taken from the broader definition of "mode of operation"]

3.1.29
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, modified – Note 2 to entry omitted]

3.1.30
machine control system
MCS
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"]

3.1.31
mean repair time
MRT
expected overall 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; and
- the effective time to repair; and
- the time before the component is put back into operation.

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 the definition, Note 1 made similar to IEC 62061:2021, 3.2.39, Note 2 added]

3.1.32
mean time to failure
MTTF
average value of expectation of the time to failure

[SOURCE: IEC 60050-192, 192-05-11, modified – "operating" removed from the term, "average value" added to the definition, and Original notes removed]

3.1.33
mean time to dangerous failure
$MTTF_D$
expectation of the mean time to dangerous failure

Note 1 to entry: Definition derived from IEC 60050-192:2015, 192-05-11 but restricted to dangerous failures.]

3.1.34
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).

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

3.1.35
pre-designed SCS or subsystem
SCS or subsystem which meets the relevant requirements of a functional safety standard

[SOURCE: IEC 62061:2021, 3.2.5]

3.1.36
probability of dangerous failure on demand
PFD
safety unavailability (see IEC 60050-192) of an SCS or SRP/CS 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 t. 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]

3.1.37
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]

3.1.38
proof test
periodic test that can detect dangerous undetected faults and degradation in an SCS or SRP/CS and its subsystems so that, if necessary, the relevant parts of the SCS or SRP/CS 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 or SRP/CS 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 % is usually not possible.

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

3.1.39
protective measure
measure intended to achieve risk reduction

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

3.1.40
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]

3.1.41
rarely activated safety function
safety function designed for high demand mode of operation where the frequency of demands is presumed to be at least one time per year, but can be sometimes less than one time per year

Note 1 to entry: When estimating the demand mode of operation, the demand rate is assumed to be at least one time per year: Nevertheless, it is possible that the safety function will not be demanded over the course of one year. The term "rarely activated safety function" reflects this special circumstance.

3.1.42
ratio of dangerous failure
RDF
fraction of the overall failure rate of an element that can result in a dangerous failure

[SOURCE: IEC 62061:2021, 3.2.55]

3.1.43
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]

3.1.44
safe failure
failure of an SCS or SRP/CS, 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]

3.1.45
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 IEC 62061:2021, 7.4).

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

[SOURCE: IEC 62061:2021, 3.2.54, modified – The abbreviated term "SFF" has been formatted as a non-variable term]

3.1.46
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.

Note 2 to entry: IEC 62061 considers "fault reaction function" in the context of "safe state" of the machine. For HFT = 0 and SFF < 60 %, when upon detection of a dangerous failure a "safe state" cannot be achieved, warnings (or alarms) can be sufficient to inform the user exposed to the risk.

[SOURCE: IEC 62061:2021, 3.2.68, modified – Note 2 added]

3.1.47
safety
freedom from unacceptable risk

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

3.1.48
safety function
function implemented by an SCS or SRP/CS 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 or SRP/CS.

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]

3.1.49
safety integrity
probability of an SCS or SRP/CS 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, and 5 deleted]

3.1.50
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

[SOURCE: IEC 62061:2021, 3.2.24]

3.1.51
safety-related control system
SCS
part of the control system of the machine which implements a safety function by one or more subsystems

[SOURCE: IEC 62061:2021, 3.2.3]

3.1.52
safety-related part of a control system
SRP/CS
part of a control system that responds to safety-related input signals and generates safety-related output signals

Note 1 to entry: The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

[SOURCE: ISO 13849-1:2015, 3.1.1]

3.1.53
safety-related software
software that is used to implement safety functions in a safety-related system

[SOURCE: IEC 62061:2021, 3.2.63]

3.1.54
security
a) measures taken to protect a system
b) condition of a system that results from the establishment and maintenance of measures to protect the system
c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss
d) 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
e) 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]

3.1.55
sub-function
part of a safety function whose failure can result in a failure of the safety function

[SOURCE: IEC 62061:2021, 3.2.36, modified – Note to entry removed]

3.1.56
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 definition 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]

3.1.57
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.

[SOURCE: IEC 62061:2021, 3.2.6]

3.1.58
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]

3.1.59
systematic safety integrity
part of the safety integrity of an SCS or SRP/CS or its subsystems relating to its resistance to systematic failures in a dangerous mode of failure

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]

3.1.60
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]

3.1.61
useful lifetime
minimum elapsed time between the installation of the SCS or SRP/CS or subsystem or subsystem element and the point in time when component failure rates of the SCS or SRP/CS 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 – The term "worst case" omitted, terminology adapted to machinery, note 1 added, example deleted]

3.1.62
validation
<of the safety function> confirmation by examination (e.g. tests, analysis) that the SCS or SRP/CS meets the functional safety requirements of the specific application

[SOURCE: IEC 61508-4:2010, 3.8.2, modified – The domain "of the safety function" added, Terminology adapted to machinery, notes deleted]

3.1.63
verification
confirmation by examination (e.g. tests, analysis) that the SCS or SRP/CS, its subsystems or subsystem elements meet the requirements set by the relevant specification

Note 1 to entry: Initial verification of safety-related control system (SCS) according to IEC 62061 or safety-related parts of a control system (SRP/CS) according to ISO 13849-1 is performed before being placed into service. Initial verification corresponds to the validation process described in IEC 62061:2021, Clause 9 or in ISO 13849-1:2015, Clause 10.

Note 2 to entry: Periodic verification of safety-related control system (SCS) according to IEC 62061 or safety-related parts of a control system (SRP/CS) according to ISO 13849-1 is performed at regular intervals during the operation of the SCS or SRP/CS. IEC 62061:2021, 6.9 "periodic tests" are part of periodic verification.

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 62061:2021, 3.2.64, modified – "or SRP/CS", note 1 and note 2 added]

3.1.64
well-tried component
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.

[SOURCE: IEC 62061:2021, 3.2.43]

3.1.65
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: IEC 62061:2021, 3.2.44]

3.2 Alphabetical list of terms, definitions and abbreviated terms

Terms used throughout this document are given in Table 1. Also included are some common abbreviated terms related to machinery safety.

Table 1 – Terms used in this document

Term	Definition number
application software	3.1.1
architectural constraint	3.1.2
architecture	3.1.3
average frequency of dangerous failure per hour (PFH)	3.1.4
common cause failure (CCF)	3.1.5
configuration management	3.1.6
continuous mode	3.1.7
dangerous failure	3.1.8
demand	3.1.9
diagnostic coverage (DC)	3.1.10
(SCS or SRP/CS) diagnostic function	3.1.11
diagnostic test interval	3.1.12
embedded software	3.1.13
failure	3.1.14
fault	3.1.15
(SCS or SRP/CS) fault reaction function	3.1.16
fault tolerance	3.1.17
full variability language (FVL)	3.1.18

Term	Definition number
functional safety	3.1.19
hardware fault tolerance (HFT)	3.1.20
hardware safety integrity	3.1.21
harm	3.1.22
hazard	3.1.23
hazardous situation	3.1.24
hazard zone	3.1.25
high demand mode of operation	3.1.26
limited variability language (LVL)	3.1.27
low demand mode	3.1.28
machinery (machine)	3.1.29
machine control system (MCS)	3.1.30
mean repair time (MRT)	3.1.31
mean time to failure (MTTF)	3.1.32
mean time to dangerous failure ($MTTF_D$)	3.1.33
mean time to restoration (MTTR)	3.1.34
pre-designed (SCS or subsystem)	3.1.35
probability of dangerous failure on demand (PFD)	3.1.36
process safety time	3.1.37
proof test	3.1.38
protective measure	3.1.39
random hardware failure	3.1.40
rarely activated safety function	3.1.41
ratio of dangerous failure (RDF)	3.1.42
risk	3.1.43
safe failure	3.1.44
safe failure fraction (SFF)	3.1.45
safe state	3.1.46
safety	3.1.47
safety function	3.1.48
safety integrity	3.1.49
safety integrity level (SIL)	3.1.50
safety-related control system (SCS)	3.1.51
safety-related parts of a control system (SRP/CS)	3.1.52
safety-related software	3.1.53
security	3.1.54
sub-function	3.1.55
subsystem	3.1.56
subsystem element	3.1.57
systematic failure	3.1.58
systematic safety integrity	3.1.59
target failure measure	3.1.60
useful lifetime	3.1.61
validation (of the safety function)	3.1.62

Term	Definition number
verification	3.1.63
well-tried component	3.1.64
well-tried safety principles	3.1.65

4 Typical classification of safety functions in safety of machinery

4.1 General

4.1.1 Overview

The risk assessment process is realized by applying ISO 12100 to define safety functions.

NOTE Additional guidance given in all subclauses of this document are based on safety functions designed according to IEC 62061 or ISO 13849-1.

4.1.2 Risk assessment and risk reduction according to ISO 12100

ISO 12100 is a fundamental safety standard that provides an overall framework and guidance for the design of machines that are safe for their intended use. It gives provisions:

– for identification of the hazards and for estimation and evaluation of the risks associated with the machine;
– on how to remove hazards or provide sufficient risk reduction:
– and guidance on the documentation and verification of the risk assessment and risk reduction achieved.

If the hazard cannot be removed and is necessary to reduce the risk associated with the hazard by implementing protective measures, such protective measures shall be applied in the following sequence, referred to as the three-step risk reduction strategy:

– Step 1: Inherently safe design measures;
– Step 2: Safeguarding and/or complementary protective measures;
– Step 3: Information for use.

ISO 12100 also provides a strategy for standards developers for the preparation of consistent and appropriate type-B and type-C standards.

ISO 12100 is a type-A standard and, according to this classification, IEC 62061 and ISO 13849-1, and ISO 13849-2 are type-B1 standards.

NOTE 1 ISO 12100 is the basis for a set of standards which has the following structure:

– Type-A standards (basic safety standards) giving basic concepts, principles for design and general aspects that can be applied to machinery;
– Type-B standards (generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery:
  - Type-B1 standards on particular safety aspects (for example, safety distances, surface temperature, noise);
  - Type-B2 standards on safeguards (for example, two-hand controls, interlocking devices, pressure-sensitive devices, guards);
– Type-C standards (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

NOTE 2 Additional information on the relationship between ISO 13849-1 and ISO 12100 can be found in ISO/TR 22100-2. This relationship is also valid for IEC 62061.

NOTE 3 Many local regulations are referencing or linked to ISO 12100, IEC 62061 or ISO 13849-1. Annex I gives an overview of different regulatory approaches regarding safety of machinery.