ICS 13.110, 25.040.99, 29.020 PREDBEŽNÁ SLOVENSKÁ TECHNICKÁ NORMA Apríl 2024

STN P	**Bezpečnosť strojových zariadení Usmernenia týkajúce sa funkčnej bezpečnosti riadiaceho bezpečnostného systému**	**STN P CLC IEC/TS 63394** 33 2200

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 03/24

Obsahuje: CLC IEC/TS 63394:2024, IEC TS 63394:2023

obsahuje farebné strany

138449

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC IEC/TS 63394

February 2024

ICS 13.110; 29.020; 25.040.99

English Version

Safety of machinery - Guidelines on functional safety of safety-related control system (IEC/TS 63394:2023)

Sécurité des machines - Lignes directrices sur la sécurité fonctionnelle des systèmes de commande relatifs à la sécurité
(IEC/TS 63394:2023)

Sicherheit von Maschinen - Leitlinien zur funktionalen Sicherheit sicherheitsbezogener Steuerungssysteme
(IEC/TS 63394:2023)

This Technical Specification was approved by CENELEC on 2024-01-22.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

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

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

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

CLC IEC/TS 63394:2024 (E)

European foreword

This document (CLC IEC/TS 63394:2024) consists of the text of IEC/TS 63394:2023 prepared by IEC/TC 44 "Safety of machinery - Electrotechnical aspects".

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

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

Endorsement notice

The text of the International Technical Specification IEC/TS 63394:2023 was approved by CENELEC as a European Technical Specification/Technical Report without any modification.

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

IEC 60204-1:2016	NOTE	Approved as EN 60204-1:2018
IEC 60947-5-3:2013	NOTE	Approved as EN 60947-5-3:2013 (not modified)
IEC 60947-5-8:2020	NOTE	Approved as EN IEC 60947-5-8:2021 (not modified)
IEC 60947-7-1	NOTE	Approved as EN 60947-7-1
IEC 60947-7-2	NOTE	Approved as EN 60947-7-2
IEC 61000-6-7	NOTE	Approved as EN 61000-6-7
IEC 61025:2006	NOTE	Approved as EN 61025:2007 (not modified)
IEC 61496-1	NOTE	Approved as EN IEC 61496-1
IEC 61508-1:2010	NOTE	Approved as EN 61508-1:2010 (not modified)
IEC 61508-4:2010	NOTE	Approved as EN 61508-4:2010 (not modified)
IEC 61508-5:2010	NOTE	Approved as EN 61508-5:2010 (not modified)
IEC 61508-6:2010	NOTE	Approved as EN 61508-6:2010 (not modified)
IEC 61508-7:2010	NOTE	Approved as EN 61508-7:2010 (not modified)
IEC 61800-5-2:2016	NOTE	Approved as EN 61800-5-2:2017 (not modified)
IEC 61511 (series)	NOTE	Approved as EN 61511 (series)
IEC 61649:2008	NOTE	Approved as EN 61649:2008 (not modified)
ISO 11161:2007	NOTE	Approved as EN ISO 11161:2007 (not modified)
ISO 13855:2010	NOTE	Approved as EN ISO 13855:2010 (not modified)

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

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

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

Publication	Year	Title	EN/HD	Year
IEC 62061	2021	Safety of machinery - Functional safety of safety-related control systems	EN IEC 62061	2021
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	EN ISO 12100	2010
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	EN ISO 13850	2015
ISO 13851	2019	Safety of machinery - Two-hand control devices - Principles for design and selection	EN ISO 13851	2019
ISO 14118	2017	Safety of machinery - Prevention of unexpected start-up	EN ISO 14118	2018
ISO 14119	2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection	EN ISO 14119	2013

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)

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

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*