



**SLOVENSKI STANDARD**  
**oSIST prEN IEC 62061:2019**  
**01-julij-2019**

---

**Varnost strojev - Funkcijska varnost nadzornih sistemov, povezanih z varnostjo**

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

**Ta slovenski standard je istoveten z: prEN IEC 62061**

**ICS:**

13.110	Varnost strojev	SIST EN IEC 62061:2021	Safety of machinery
25.040.40	Merjenje in krmiljenje industrijskih postopkov		Industrial process measurement and control

**oSIST prEN IEC 62061:2019**

**en,fr,de**





## COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: <b>IEC 62061 ED2</b>	
DATE OF CIRCULATION: <b>2019-04-26</b>	CLOSING DATE FOR VOTING: <b>2019-07-19</b>
SUPERSEDES DOCUMENTS: <b>44/827/CD, 44/844A/CC</b>	

IEC TC 44 : SAFETY OF MACHINERY - ELECTROTECHNICAL ASPECTS	
SECRETARIAT: United Kingdom	SECRETARY: Mrs Nyomee Hla-Shwe Tun
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: <input type="checkbox"/> Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: <input type="checkbox"/> EMC <input type="checkbox"/> ENVIRONMENT <input type="checkbox"/> QUALITY ASSURANCE <input checked="" type="checkbox"/> SAFETY	
<input checked="" type="checkbox"/> SUBMITTED FOR CENELEC PARALLEL VOTING <b>Attention IEC-CENELEC parallel voting</b> The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	<input type="checkbox"/> NOT SUBMITTED FOR CENELEC PARALLEL VOTING

SIST EN IEC 62061:2021

This document is still under study and subject to change. It should not be used for reference purposes. 39b/sist-en-iec-62061-2021  
 Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

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

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

**Copyright © 2019 International Electrotechnical Commission, IEC.** All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

## CONTENTS

FOREWORD.....	9
INTRODUCTION.....	12
1 Scope.....	13
2 Normative references .....	14
3 Terms, definitions and abbreviations .....	15
3.1 Alphabetical list of definitions.....	15
3.2 Terms and definitions.....	17
3.3 Abbreviations.....	28
4 Design process of an SCS and management of functional safety.....	29
4.1 Objective .....	29
4.2 Design process .....	29
4.3 Management of functional safety using a functional safety plan .....	31
4.4 Configuration management .....	32
4.5 Modification .....	33
5 Specification of a safety function .....	33
5.1 Objective .....	33
5.2 Safety Requirements Specification (SRS).....	33
5.2.1 Information to be available.....	34
5.2.2 Functional requirements specification .....	34
5.2.3 Safety integrity requirements specification.....	35
6 Design of an SCS .....	35
6.1 General.....	35
6.2 Subsystem architecture based on top down decomposition .....	36
6.3 Basic methodology – Use of subsystem .....	36
6.3.1 General .....	36
6.3.2 SCS architecture design based on subsystems.....	36
6.3.3 Sub-function allocation .....	38
6.3.4 Use of a pre-designed subsystem .....	38
6.4 Determination of safety integrity of the SCS.....	38
6.4.1 General .....	38
6.4.2 Average frequency of dangerous failures .....	39
6.5 Requirements for systematic safety integrity of the SCS .....	39
6.5.1 Requirements for the avoidance of systematic hardware failures .....	39
6.5.2 Requirements for the control of systematic faults.....	40
6.6 Electromagnetic immunity .....	41
6.7 Software based manual parameterization.....	41
6.7.1 General .....	41
6.7.2 Influences on safety-related parameters .....	41
6.7.3 Requirements for software based manual parameterization .....	42
6.7.4 Verification of the parameterization tool.....	43
6.7.5 Performance of software based manual parameterization .....	43
6.8 Security aspects .....	43
6.9 Aspects of periodic testing .....	44
6.9.1 General principle .....	44

6.9.2	Proof test.....	44
7	Design and development of a subsystem.....	45
7.1	General.....	45
7.2	Subsystem architecture design .....	46
7.3	Requirements for the selection and design of subsystem and subsystem elements.....	46
7.3.1	General .....	46
7.3.2	Systematic integrity .....	46
7.3.3	Fault consideration and fault exclusion .....	49
7.3.4	Failure rate of subsystem element .....	50
7.4	Architectural constraints of a subsystem .....	52
7.4.1	General .....	52
7.4.2	Estimation of safe failure fraction (SFF).....	53
7.4.3	Behaviour (of the SCS) on detection of a fault in a subsystem .....	54
7.4.4	Realization of diagnostic functions.....	55
7.5	Subsystem design architectures.....	56
7.5.1	General .....	56
7.5.2	Basic subsystem architectures.....	56
7.5.3	Basic requirements .....	57
7.6	Probability of dangerous random hardware failures of subsystems.....	58
7.6.1	General .....	58
7.6.2	Methods to estimate the PFH of a subsystem .....	58
7.6.3	Methods to estimate the PFD <sub>avg</sub> of a subsystem .....	58
7.6.4	Simplified approach to estimation of contribution of common cause failure (CCF).....	58
8	Software.....	59
8.1	General.....	59
8.2	Definition of Software Levels.....	59
8.3	Software Level 1 .....	60
8.3.1	Software safety lifecycle SW Level 1 .....	60
8.3.2	Software Design SW Level 1 .....	61
8.3.3	Module design SW Level 1 .....	63
8.3.4	Coding SW Level 1 .....	64
8.3.5	Module test SW Level 1 .....	64
8.3.6	Software testing SW Level 1 .....	64
8.3.7	Documentation SW Level 1.....	65
8.3.8	Configuration and modification management process SW Level 1.....	65
8.4	Software Level 3 .....	66
8.4.1	Software safety lifecycle SW Level 3 .....	66
8.4.2	Software Design SW Level 3 .....	68
8.4.3	Software system design SW Level 3 .....	69
8.4.4	Module design SW Level 3 .....	70
8.4.5	Coding SW Level 3 .....	70
8.4.6	Module test SW Level 3.....	71
8.4.7	Software integration testing SW Level 3 .....	71
8.4.8	Software testing SW Level 3.....	71
8.4.9	Documentation SW Level 3.....	73
8.4.10	Configuration and modification management process SW Level 3.....	73
9	Validation .....	73

9.1	Validation principles.....	73
9.1.1	Validation plan.....	77
9.1.2	Use of generic fault lists .....	77
9.1.3	Specific fault lists .....	78
9.1.4	Information for validation .....	78
9.1.5	Validation record .....	79
9.2	Analysis as part of validation .....	79
9.2.1	General .....	79
9.2.2	Analysis techniques .....	79
9.2.3	Verification of safety requirements specification for safety functions .....	79
9.3	Testing as part of validation .....	80
9.3.1	General .....	80
9.3.2	Measurement accuracy.....	80
9.3.3	More stringent requirements .....	81
9.3.4	Number of test samples .....	81
9.4	Validation of the safety function .....	81
9.4.1	General .....	81
9.4.2	Analysis and testing.....	82
9.5	Validation of the safety integrity of the SCS .....	82
9.5.1	Validation of subsystem(s).....	82
9.5.2	Validation of measures against systematic failures .....	82
9.5.3	Validation of safety-related software .....	83
9.5.4	Validation of combination of subsystems .....	83
9.5.5	Verification of safety integrity.....	84
10	Documentation .....	84
10.1	General.....	84
10.2	Technical documentation .....	84
10.3	Information for use of the SCS .....	85
10.3.1	General .....	85
10.3.2	Information for use given by the manufacturer of subsystems .....	86
10.3.3	Information for use given by the SCS integrator .....	86
Annex A (informative)	Determination of required safety integrity .....	88
A.1	General.....	88
A.2	Matrix assignment for the required SIL.....	88
A.2.1	Hazard identification/indication .....	88
A.2.2	Risk estimation .....	88
A.2.3	Severity (Se) .....	89
A.2.4	Probability of occurrence of harm .....	89
A.2.5	Class of probability of harm (CI) .....	92
A.2.6	SIL assignment.....	92
A.3	Overlapping hazards .....	94
Annex B (informative)	Example of SCS design methodology .....	95
B.1	General.....	95
B.2	Safety requirements specification .....	95
B.3	Decomposition of the safety function.....	95
B.4	Design of the SCS by using subsystems .....	97
B.4.1	General .....	97
B.4.2	Subsystem 1 design – “guard door monitoring” .....	97

B.4.3	Subsystem 2 design – “evaluation logic” .....	99
B.4.4	Subsystem 3 design – “motor control” .....	99
B.4.5	Evaluation of the SCS .....	99
B.5	Verification .....	100
B.5.1	Analysis .....	100
B.5.2	Tests .....	100
Annex C (informative)	Examples of MTTF <sub>D</sub> values for single components .....	101
C.1	General .....	101
C.2	Good engineering practices method .....	101
C.3	Hydraulic components .....	101
C.4	MTTF <sub>D</sub> of pneumatic, mechanical and electromechanical components .....	101
Annex D (normative)	Low demand requirements .....	103
D.1	General .....	103
D.2	Normative references .....	103
D.3	Terms and definitions .....	103
D.4	Design process of an SCS and management of functional safety .....	103
D.5	Specification of a safety function .....	103
D.6	Design of an SCS .....	104
D.7	Design and development of subsystem .....	105
D.8	Software .....	106
D.9	Validation .....	106
D.10	Documentation .....	106
Annex E (informative)	Examples for diagnostic coverage (DC) .....	107
Annex F (informative)	Methodology for the estimation of susceptibility to common cause failures (CCF) .....	109
F.1	General .....	109
F.2	Methodology .....	109
F.2.1	Requirements for CCF .....	109
F.2.2	Estimation of effect of CCF .....	109
Annex G (informative)	Guideline for Software level 1 .....	111
G.1	Software safety requirements .....	111
G.2	Coding guidelines .....	112
G.3	Specification of safety functions .....	112
G.4	Specification of hardware design .....	114
G.5	Software system design specification .....	115
G.6	Protocols .....	118
Annex H (informative)	((void)) .....	120
Annex I (informative)	Examples of safety functions .....	121
I.1	Examples of safety functions .....	121
I.2	Example of low demand function .....	122
Annex J (informative)	((void)) .....	126
Annex K (informative)	Simplified approaches to evaluate the PFH value of a subsystem .....	127
K.1	Table allocation approach .....	127
K.2	Simplified Formulas for the estimation of PFH .....	129
K.2.1	General .....	129
K.2.2	Basic subsystem architecture A: single channel without a diagnostic function .....	129

K.2.3	Basic subsystem architecture B: dual channel without a diagnostic function .....	130
K.2.4	Basic subsystem architecture C: single channel with a diagnostic function .....	130
K.2.5	Basic subsystem architecture D: dual channel with a diagnostic function(s) .....	135
K.3	Parts count method .....	135
Annex L ((void))	.....	137
Annex M (informative)	The functional safety plan and design activities .....	138
M.1	General .....	138
M.2	Example of a machine design plan including a safety plan .....	138
M.3	Example of activities, documents and roles .....	138
Bibliography	.....	141
Figure 1	- Relationship of this standard to other standards .....	14
Figure 2	- Integration within the risk reduction process of ISO 12100 (excerpt) .....	29
Figure 3	- Iterative process for design of the safety-related control system .....	30
Figure 4	- Examples of combination of subsystems as one SCS .....	31
Figure 5	- Examples of typical decomposition of a safety function into sub-functions and its allocation to subsystems .....	37
Figure 6	- Example of safety integrity of a safety function based on allocated subsystems as one SCS .....	38
Figure 7	- Subsystem A logical representation .....	56
Figure 8	- Subsystem B logical representation .....	57
Figure 9	- Subsystem C logical representation .....	57
Figure 10	- Subsystem D logical representation .....	57
Figure 11	- V-model for SW level 1 .....	60
Figure 12	- V-model for software modules customized by the designer for SW level 1 .....	60
Figure 13	- V-model of software safety lifecycle for SW Level 3 .....	66
Figure 14	- Overview of the validation process .....	76
Figure A.1	- Parameters used in risk estimation .....	88
Figure A.2	- Example proforma for SIL assignment process .....	93
Figure B.1	- Decomposition of the safety function .....	96
Figure B.2	- Overview of design of the subsystems of the SCS .....	97
Figure D.1	- Example of safety integrity of a safety function based on allocated subsystems as one SCS .....	104
Figure G.1	- Plant sketch .....	113
Figure G.2	- Principal module architecture design .....	116
Figure G.3	- Principal design approach of logical evaluation .....	117
Figure G.4	- Example of logical representation (program sketch) .....	118
Figure I.1	- Relationship between demand of a safety function, failure and trip limit in a safety function .....	123
Figure I.2	- Typical configuration of a gas turbine .....	124
Figure K.1	- Subsystem A logical representation .....	129
Figure K.2	- Subsystem B logical representation .....	130
Figure K.3	- Subsystem C logical representation .....	130



Figure K.4 - Correlation of subsystem C and the pertinent fault handling function .....	131
Figure K.5 - Subsystem C with external fault handling function .....	131
Figure K.6 – Subsystem C with external fault diagnostics .....	132
Figure K.7 – Subsystem C with external fault reaction .....	133
Figure K.8 – Subsystem C with internal fault diagnostics and internal fault reaction .....	133
Figure K.9 - Subsystem D logical representation.....	135
Figure M.1 – Example of a machine design plan including a safety plan .....	138
Figure M.2 – Example of activities, documents and roles .....	139
Table 1 – SIL and limits of PFH values .....	35
Table 2 – Required SIL and PFH of pre-designed subsystem.....	38
Table 3 – Relevant information for each subsystem .....	45
Table 4 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem .....	53
Table 5 – Overview of basic requirements and interrelation to basic subsystem architectures.....	58
Table 6 – Different levels of software .....	59
Table 7 – Minimum levels of independence for review, testing and verification activities SW Level 1 .....	61
Table 8 – Minimum levels of independence for review, testing and verification activities SW Level 3 .....	67
Table 9 – Minimum levels of independence for validation activities .....	77
Table 10 – Documentation of an SCS .....	85
Table A.1 – Severity (Se) classification.....	89
Table A.2 – Frequency and duration of exposure (Fr) classification .....	90
Table A.3 – Probability (Pr) classification.....	91
Table A.4 – Probability of avoiding or limiting harm (Av) classification .....	91
Table A.5 – Parameters used to determine class of probability of harm (Cl).....	92
Table A.6 – Matrix assignment for determining the required SIL (or PL <sub>r</sub> ) for a safety function.....	93
Table B.1 – Safety requirements specification – example of overview .....	95
Table B.2 – Systematic integrity – example of overview .....	100
Table B.3 – Verification by tests .....	100
Table C.1 – Standards references and MTTF <sub>D</sub> or B <sub>10D</sub> values for components.....	102
Table D.1 – SIL and limits of PFD <sub>avg</sub> values in low demand mode of operation .....	103
Table E.1 – Estimates for diagnostic coverage (DC) .....	107
Table F.1 – Criteria for estimation of CCF.....	109
Table F.2 – Criteria for estimation of CCF.....	110
Table G.1 – Example of relevant documents related to the simplified V-model .....	111
Table G.2 – Examples of coding guidelines.....	112
Table G.3 – Specified safety functions .....	113
Table G.4 – Relevant list of input and output signals.....	114
Table G.5 – Example of simplified cause and effect matrix.....	118
Table G.6 – Verification of software system design specification.....	119
Table G.7 – Software code review .....	119

Table G.8 – Software validation .....	119
Table I.1 – Examples of typical safety functions .....	121
Table K.1 – Allocation of PFH value of a subsystem .....	128
Table K.2 – Relationship between $B_{10D}$ , operations and $MTTF_D$ .....	129

**iTeh Standards**  
**(<https://standards.iteh.ai>)**  
**Document Preview**

[SIST EN IEC 62061:2021](https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021)

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

## FOREWORD

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

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

This second edition cancels and replaces the previous edition. This edition constitutes a technical revision and it includes the following significant technical changes:

1. structure has been changed and contents have been updated to reflect the design process of the safety function
2. standard extended to non-electrical technologies
3. standard extended to low demand mode for specific applications (Annex D)
4. definitions updated to be aligned with IEC 61508
5. functional safety plan introduced and configuration management updated (Section 4)
6. requirements on parametrization expanded (Section 6)
7. reference to requirements on security added (Section 6.8)
8. requirements on periodic testing added (Section 6.9)
9. various improvements and clarification on architectures and reliability calculations (Sections 6 and 7)
10. shift from SILCL to maximum SIL of a subsystem (Section 7)
11. use cases for software described including requirements (Section 8)

- 60 12. requirements on independence for software verification (Section 8) and validation  
61 activities (Sections 9) added  
62 13. new informative annex with examples (Annex I)  
63 14. new informative annexes on typical  $MTTF_D$  values, diagnostics and calculation  
64 methods for the architectures (Annexes C, E and K)

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

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

66  
67 Full information on the voting for the approval of this standard can be found in the report on  
68 voting indicated in the above table.

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

70

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[SIST EN IEC 62061:2021](https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021)

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

71 The committee has decided that the contents of this publication will remain unchanged until  
72 the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data  
73 related to the specific publication. At this date, the publication will be

- 74 • reconfirmed,
- 75 • withdrawn,
- 76 • replaced by a revised edition, or
- 77 • amended.

78

79 The National Committees are requested to note that for this publication the stability date  
80 is 20XX.

81 THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED  
82 AT THE PUBLICATION STAGE.

83

## iTeh Standards (<https://standards.iteh.ai>) Document Preview

[SIST EN IEC 62061:2021](https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021)

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

84

## INTRODUCTION

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

89 IEC 62061 and ISO 13849-1 specify requirements for the design and implementation of  
90 safety-related control systems of machinery. This standard is machine sector specific within  
91 the framework of IEC 61508.

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

96 It is intended to facilitate the specification of the safety functions intended to achieve the risk  
97 reduction of machine when it is intended to be achieved by safety-related control systems.

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

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

- 110 • assign the required safety integrity for each safety function to be implemented by SCS;
- 111 • enable the design of the SCS appropriate to the assigned safety (control) function(s);
- 112 • integrate safety-related subsystems designed in accordance with other applicable  
113 functional safety-related standards (see 6.2.4);
- 114 • validate the SCS.

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