



Sisaldab värvilisi lehekülgi
Colour inside

MASINATE OHUTUS. OHUTUSEGA SEOTUD JUHTIMISSÜSTEEMIDE FUNKTSIONAALNE OHUTUS

**Safety of machinery - Functional safety of safety-related
control systems (IEC 62061:2021 +
IEC 62061:2021/AMD1:2024)**

EESTI STANDARDI EESSÕNA**NATIONAL FOREWORD**

See Eesti standard EVS-EN IEC 62061:2021+A1:2024 sisaldab Euroopa standardi EN IEC 62061:2021 ja selle muudatuse A1:2024 ingliskeelset teksti.	This Estonian standard EVS-EN IEC 62061:2021+A1:2024 consists of the English text of the European standard EN IEC 62061:2021 and its amendment A1:2024.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas. Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 23.07.2021, muudatus A1 28.06.2024.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation. Date of Availability of the European standard is 23.07.2021, for A1 28.06.2024.
Muudatusega A1 lisatud või muudetud teksti algus ja lõpp on tekstis tähistatud sümbolitega $\boxed{A_1}$ $\langle A_1 \rangle$. Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	The start and finish of text introduced or altered by amendment A1 is indicated in the text by tags $\boxed{A_1}$ $\langle A_1 \rangle$. The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 13.110; 25.040.99; 29.020

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about standards copyright protection, please contact the Estonian Centre for Standardisation and Accreditation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

EUROPEAN STANDARD

EN IEC 62061 + A1

NORME EUROPÉENNE

EUROPÄISCHE NORM

July 2021, June 2024

ICS 13.110; 25.040.99; 29.020

Supersedes EN 62061:2005 and all of its amendments
and corrigenda (if any)

English Version

**Safety of machinery - Functional safety of safety-related control
systems
(IEC 62061:2021 + IEC 62061:2021/AMD1:2024)**

Sécurité des machines - Sécurité fonctionnelle des
systèmes de commande relatifs à la sécurité
(IEC 62061:2021 + IEC 62061:2021/AMD1:2024)

Sicherheit von Maschinen - Funktionale Sicherheit
sicherheitsbezogener Steuerungssysteme
(IEC 62061:2021 + IEC 62061:2021/AMD1:2024)

This European Standard was approved by CENELEC on 2021-04-26. Amendment A1 was approved by CENELEC on 2024-03-11. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard and its amendment the status of a national standard without any alteration.

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

This European Standard and its Amendment A1 exist in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

© 2024 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62061:2021 E
+ EN IEC 62061:2021/A1:2024 E

European foreword

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

The following dates are fixed:

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

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

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

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

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

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

Endorsement notice

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

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

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

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

A1 Amendment A1 European foreword

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

The following dates are fixed:

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

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

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

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

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

Endorsement notice

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

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

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



INTERNATIONAL STANDARD



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2024 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 Varembe
CH-1211 Geneva 20
Switzerland

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

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

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

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

preview generated by EVS



IEC 62061

Edition 2.1 2024-03
CONSOLIDATED VERSION

INTERNATIONAL STANDARD



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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-8675-3

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

CONTENTS

FOREWORD.....	9
Amendment A1 FOREWORD 	11
INTRODUCTION.....	13
1 Scope.....	14
2 Normative references.....	15
3 Terms, definitions and abbreviations	16
3.1 Alphabetical list of definitions	16
3.2 Terms and definitions	18
3.3 Abbreviations	31
4 Design process of an SCS and management of functional safety	32
4.1 Objective	32
4.2 Design process	32
4.3 Management of functional safety using a functional safety plan	34
4.4 Configuration management.....	36
4.5 Modification	36
5 Specification of a safety function.....	37
5.1 Objective	37
5.2 Safety requirements specification (SRS)	37
5.2.1 General	37
5.2.2 Information to be available	37
5.2.3 Functional requirements specification	38
5.2.4 Estimation of demand mode of operation	38
5.2.5 Safety integrity requirements specification	39
6 Design of an SCS	40
6.1 General.....	40
6.2 Subsystem architecture based on top down decomposition	40
6.3 Basic methodology – Use of subsystem	40
6.3.1 General	40
6.3.2 SCS decomposition.....	41
6.3.3 Sub-function allocation.....	42
6.3.4 Use of a pre-designed subsystem.....	42
6.4 Determination of safety integrity of the SCS.....	43
6.4.1 General	43
6.4.2 PFH.....	43
6.5 Requirements for systematic safety integrity of the SCS.....	44
6.5.1 Requirements for the avoidance of systematic hardware failures	44
6.5.2 Requirements for the control of systematic faults	45
6.6 Electromagnetic immunity.....	46
6.7 Software based manual parameterization.....	46
6.7.1 General	46
6.7.2 Influences on safety-related parameters	46
6.7.3 Requirements for software based manual parameterization	47
6.7.4 Verification of the parameterization tool.....	48
6.7.5 Performance of software based manual parameterization.....	48
6.8 Security aspects.....	48
6.9 Aspects of periodic testing.....	49

7	Design and development of a subsystem.....	49
7.1	General.....	49
7.2	Subsystem architecture design	50
7.3	Requirements for the selection and design of subsystem and subsystem elements.....	51
7.3.1	General	51
7.3.2	Systematic integrity.....	51
7.3.3	Fault consideration and fault exclusion	54
7.3.4	Failure rate of subsystem element	55
7.4	Architectural constraints of a subsystem	58
7.4.1	General	58
7.4.2	Estimation of safe failure fraction (<i>SFF</i>)	59
7.4.3	Behaviour (of the SCS) on detection of a fault in a subsystem.....	61
7.4.4	Realization of diagnostic functions.....	62
7.5	Subsystem design architectures	62
7.5.1	General	62
7.5.2	Basic subsystem architectures	63
7.5.3	Basic requirements	64
7.6	<i>PFH</i> of subsystems	65
7.6.1	General	65
7.6.2	Methods to estimate the <i>PFH</i> of a subsystem.....	65
7.6.3	Simplified approach to estimation of contribution of common cause failure (CCF).....	65
8	Software.....	65
8.1	General.....	65
8.2	Definition of software levels.....	66
8.3	Software – Level 1	67
8.3.1	Software safety lifecycle – SW level 1	67
8.3.2	Software design – SW level 1	68
8.3.3	Module design – SW level 1	70
8.3.4	Coding – SW level 1.....	70
8.3.5	Module test – SW level 1.....	71
8.3.6	Software testing – SW level 1	71
8.3.7	Documentation – SW level 1.....	72
8.3.8	Configuration and modification management process – SW level 1.....	72
8.4	Software level 2	73
8.4.1	Software safety lifecycle – SW level 2	73
8.4.2	Software design – SW level 2.....	74
8.4.3	Software system design – SW level 2	76
8.4.4	Module design – SW level 2	77
8.4.5	Coding – SW level 2.....	78
8.4.6	Module test – SW level 2.....	78
8.4.7	Software integration testing SW level 2.....	78
8.4.8	Software testing SW level 2.....	79
8.4.9	Documentation – SW level 2.....	80
8.4.10	Configuration and modification management process – SW level 2.....	80
9	Validation	81
9.1	Validation principles	81
9.1.1	Validation plan	84

9.1.2	Use of generic fault lists	84
9.1.3	Specific fault lists	84
9.1.4	Information for validation	85
9.1.5	Validation record	85
9.2	Analysis as part of validation	86
9.2.1	General	86
9.2.2	Analysis techniques	86
9.2.3	Verification of safety requirements specification (SRS)	86
9.3	Testing as part of validation	87
9.3.1	General	87
9.3.2	Measurement accuracy	87
9.3.3	More stringent requirements	88
9.3.4	Test samples	88
9.4	Validation of the safety function	88
9.4.1	General	88
9.4.2	Analysis and testing	89
9.5	Validation of the safety integrity of the SCS	89
9.5.1	General	89
9.5.2	Validation of subsystem(s)	89
9.5.3	Validation of measures against systematic failures	90
9.5.4	Validation of safety-related software	90
9.5.5	Validation of combination of subsystems	91
10	Documentation	91
10.1	General	91
10.2	Technical documentation	92
10.3	Information for use of the SCS	93
10.3.1	General	93
10.3.2	Information for use given by the manufacturer of subsystems	94
10.3.3	Information for use given by the SCS integrator	95
Annex A (informative)	Determination of required safety integrity	96
A.1	General	96
A.2	Matrix assignment for the required SIL	96
A.2.1	Hazard identification/indication	96
A.2.2	Risk estimation	96
A.2.3	Severity (Se)	97
A.2.4	Probability of occurrence of harm	97
A.2.5	Class of probability of harm (CI)	100
A.2.6	SIL assignment	100
A.3	Overlapping hazards	102
Annex B (informative)	Example of SCS design methodology	103
B.1	General	103
B.2	Safety requirements specification	103
B.3	Decomposition of the safety function	104
B.4	Design of the SCS by using subsystems	104
B.4.1	General	104
B.4.2	Subsystem 1 design – “guard door monitoring”	105
B.4.3	Subsystem 2 design – “evaluation logic”	106
B.4.4	Subsystem 3 design – “motor control”	107

B.4.5	Evaluation of the SCS	108
B.4.6	PFH.....	108
B.5	Verification.....	109
B.5.1	General	109
B.5.2	Analysis.....	109
B.5.3	Tests	109
Annex C (informative)	Examples of $MTTF_D$ values for single components.....	110
C.1	General.....	110
C.2	Good engineering practices method.....	110
C.3	Hydraulic components	110
C.4	$MTTF_D$ of pneumatic, mechanical and electromechanical components.....	111
Annex D (informative)	Examples for diagnostic coverage (DC).....	113
Annex E (informative)	Methodology for the estimation of susceptibility to common cause failures (CCF).....	115
E.1	General.....	115
E.2	Methodology	115
E.2.1	Requirements for CCF.....	115
E.2.2	Estimation of effect of CCF.....	115
Annex F (informative)	Guideline for software level 1	118
F.1	Software safety requirements	118
F.2	Coding guidelines	119
F.3	Specification of safety functions	120
F.4	Specification of hardware design	121
F.5	Software system design specification.....	123
F.6	Protocols	125
Annex G (informative)	Examples of safety functions	128
Annex H (informative)	Simplified approaches to evaluate the PFH value of a subsystem.....	129
H.1	Table allocation approach	129
H.2	Simplified formulas for the estimation of PFH	131
H.2.1	General	131
H.2.2	Basic subsystem architecture A: single channel without a diagnostic function	131
H.2.3	Basic subsystem architecture B: dual channel without a diagnostic function	132
H.2.4	Basic subsystem architecture C: single channel with a diagnostic function	132
H.2.5	Basic subsystem architecture D: dual channel with a diagnostic function(s)	138
H.3	Parts count method	138
Annex I (informative)	The functional safety plan and design activities.....	140
I.1	General.....	140
I.2	Example of a machine design plan including a safety plan.....	140
I.3	Example of activities, documents and roles.....	140
Annex J (informative)	Independence for reviews and testing/verification/validation activities.....	143
J.1	Software design	143
J.2	Validation.....	143

Annex ZA (normative) Normative references to international publications with their corresponding European publications	145
Annex ZZ (informative) Relationship between this European standard and the essential requirements of Directive 2006/42/EC [2006 OJ L 157] aimed to be covered	147
Bibliography	148
Figure 1 – Scope of this document	15
Figure 2 – Integration within the risk reduction process of ISO 12100 (extract)	32
Figure 3 – Iterative process for design of the safety-related control system	33
Figure 4 – Example of a combination of subsystems as one SCS	34
Figure 5 – By activating a low demand safety function at least once per year it can be assumed to be high demand	39
Figure 6 – Examples of typical decomposition of a safety function into sub-functions and its allocation to subsystems	42
Figure 7 – Example of safety integrity of a safety function based on allocated subsystems as one SCS	43
Figure 8 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ A logical representation	63
Figure 9 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ B logical representation	63
Figure 10 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ C logical representation	63
Figure 11 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ D logical representation	64
Figure 12 – V-model for SW level 1	67
Figure 13 – V-model for software modules customized by the designer for SW level 1	68
Figure 14 – V-model of software safety lifecycle for SW level 2	74
Figure 15 – Overview of the validation process	83
Figure A.1 – Parameters used in risk estimation	96
Figure A.2 – Example proforma for SIL assignment process	102
Figure B.1 – Decomposition of the safety function	104
Figure B.2 – Overview of design of the subsystems of the SCS	104
Figure F.1 – Plant sketch	120
Figure F.2 – Principal module architecture design	123
Figure F.3 – Principal design approach of logical evaluation	124
Figure F.4 – Example of logical representation (program sketch)	125
Figure H.1 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ A logical representation	131
Figure H.2 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ B logical representation	132
Figure H.3 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ C logical representation	132
Figure H.4 – Correlation of basic subsystem architecture C and the pertinent fault handling function $\langle A_1 \rangle$	133
Figure H.5 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ C with external fault handling function	134
Figure H.6 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ C with external fault diagnostics	135
Figure H.7 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ C with external fault reaction	135
Figure H.8 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ C with internal fault diagnostics and internal fault reaction	135
Figure H.9 – $\boxed{A_1}$ Basic subsystem architecture $\langle A_1 \rangle$ D logical representation	138

Figure I.1 – Example of a machine design plan including a safety plan.....	140
Figure I.2 – Example of activities, documents and roles (1 of 2).....	141
Table 1 – Terms used in IEC 62061	16
Table 2 – Abbreviations used in IEC 62061	31
Table 3 – SIL and limits of <i>PFH</i> values	39
Table 4 – Required SIL and <i>PFH</i> of pre-designed subsystem	43
Table 5 – Relevant information for each subsystem	50
Table 6 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem.....	59
Table 7 – Overview of basic requirements and interrelation to basic subsystem architectures.....	64
Table 8 – Different levels of application software	66
Table 9 – Documentation of an SCS.....	93
Table A.1 – Severity (Se) classification	97
Table A.2 – Frequency and duration of exposure (Fr) classification	98
Table A.3 – Probability (Pr) classification	99
Table A.4 – Probability of avoiding or limiting harm (Av) classification	100
Table A.5 – Parameters used to determine class of probability of harm (Cl)	100
Table A.6 – Matrix assignment for determining the required SIL (or PL_r) for a safety function	101
Table B.1 – Safety requirements specification – example of overview	103
Table B.2 – Systematic integrity – example of overview	108
Table B.3 – Verification by tests	109
Table C.1 – Standards references and $MTTF_D$ or B_{10D} values for components	111
Table D.1 – Estimates for diagnostic coverage (<i>DC</i>) (1 of 2)	113
Table E.1 – Criteria for estimation of CCF	116
Table E.2 – $\overline{A_1}$ Estimation of CCF factor (β) $\overline{A_1}$	117
Table F.1 – Example of relevant documents related to the simplified V-model	118
Table F.2 – Examples of coding guidelines	119
Table F.3 – Specified safety functions	121
Table F.4 – Relevant list of input and output signals	122
Table F.5 – Example of simplified cause and effect matrix	125
Table F.6 – Verification of software system design specification	126
Table F.7 – Software code review	126
Table F.8 – Software validation	127
Table G.1 – Examples of typical safety functions	128
Table H.1 – Allocation of <i>PFH</i> value of a subsystem	130
Table H.2 – Relationship between B_{10D} , operations and $MTTF_D$	131
Table H.3 – Minimum value of $1/\lambda_D$ F_H for the applicability of <i>PFH</i> equation $\overline{A_1}$ (H.3) $\overline{A_1}$	136
Table J.1 – Minimum levels of independence for review, testing and verification activities.....	143

Table J.2 – Minimum levels of independence for validation activities 143

Table ZZ.1 — Correspondence between this European standard and Annex 1 of
Directive] 2006/42/EC [2006 OJ L 157] 147

This document is a preview generated by EVS

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.

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

This second edition cancels and replaces the first edition, published in 2005, Amendment 1:2012 and Amendment 2:2015. This edition constitutes a technical revision.

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

- structure has been changed and contents have been updated to reflect the design process of the safety function,
- standard extended to non-electrical technologies,
- definitions updated to be aligned with IEC 61508-4,
- functional safety plan introduced and configuration management updated (Clause 4),
- requirements on parametrization expanded (Clause 6),
- reference to requirements on security added (Subclause 6.8),
- requirements on periodic testing added (Subclause 6.9),

- various improvements and clarification on architectures and reliability calculations (Clause 6 and Clause 7),
- shift from "SILCL" to "maximum SIL" of a subsystem (Clause 7),
- use cases for software described including requirements (Clause 8),
- requirements on independence for software verification (Clause 8) and validation activities (Clause 9) added,
- new informative annex with examples (Annex G),
- new informative annexes on typical $MTTF_D$ values, diagnostics and calculation methods for the architectures (Annex C, Annex D and Annex H).

The text of this International Standard is based on the following documents:

Draft	Report on voting
44/885/FDIS	44/888/RVD

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 International Standard is English.

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

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

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

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

A1 Amendment A1 FOREWORD

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

Amendment 1 to IEC 62061:2021 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

The text of this Amendment is based on the following documents:

Draft	Report on voting
44/1020/FDIS	44/1024/RVD

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 Amendment 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/publications/.

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

- reconfirmed,
- withdrawn, or
- revised. [A1](#)

This document is a preview generated by EVS

INTRODUCTION

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

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

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

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

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

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

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

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

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

1 Scope

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

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

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

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

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

This document:

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

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

This document does not cover

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

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

Figure 1 illustrates the scope of this document.

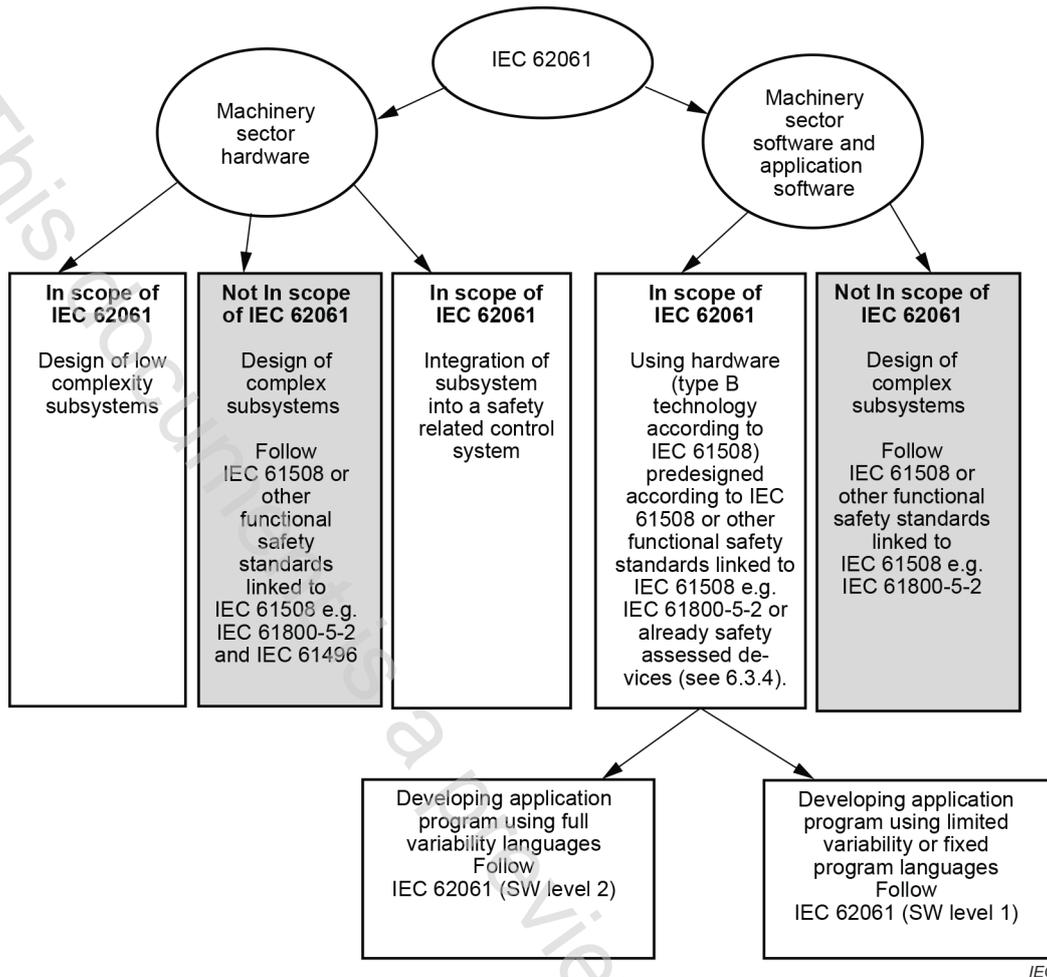


Figure 1 – Scope of this document

2 Normative references

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

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

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

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

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

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

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

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

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

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

3 Terms, definitions and abbreviations

3.1 Alphabetical list of definitions

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

Table 1 – Terms used in IEC 62061

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