SLOVENSKI STANDARD
SIST EN IEC 62061:2021/oprA1:2023

01-junij-2023

Varnost strojev - Funkcijska varnost nadzornih sistemov, povezanih z varnostjo - Dopolnilo A1

Amendment 1 - Safety of machinery - Functional safety of safety-related control systems

Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme

Amendement 1 - Sécurité des machines - Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité

Ta slovenski standard je istoveten z: **EN IEC 62061:2021/prA1:2023**

ICS:

13.110	Varnost strojev	Safety of machinery
25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control

SIST EN IEC 62061:2021/oprA1:2023 **en,fr,de**

44/995/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:	
IEC 62061/AMD1 ED2	
DATE OF CIRCULATION:	CLOSING DATE FOR VOTING:
2023-04-28	**2023-07-21**
SUPERSEDES DOCUMENTS:	
44/985/CD, 44/991/CC	

IEC TC 44 : SAFETY OF MACHINERY - ELECTROTECHNICAL ASPECTS

SECRETARIAT:	SECRETARY:
United Kingdom	Mrs Nyomee Hla-Shwe Tun
OF INTEREST TO THE FOLLOWING COMMITTEES: SC 65A	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.

FUNCTIONS CONCERNED:

☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☒ SAFETY

☒ SUBMITTED FOR CENELEC PARALLEL VOTING	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING
Attention IEC-CENELEC parallel voting 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.	

This document is still under study and subject to change. It should not be used for reference purposes.

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,
- any relevant “in some countries” clauses to be included should this proposal proceed. Recipients are reminded that the enquiry stage is the final stage for submitting "in some countries" clauses. See AC/22/2007.

TITLE:

Amendment 1 - Safety of machinery - Functional safety of safety-related control systems

PROPOSED STABILITY DATE: 2026

NOTE FROM TC/SC OFFICERS:

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

AMENDMENT 1

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.

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
XX/XX/FDIS	XX/XX/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,
- replaced by a revised edition, or
- amended.

_____

1 Scope

Replace, in paragraph 6 of Clause 1, 3rd dash, "IEC TR 63074" with "IEC TS 63074".

3.2.52 dangerous failure

Replace, in source, text "[SOURCE: IEC 61508-4:2010, 3.6.4, modified – Terminology adapted to machinery and figure replaced by textual description and ISO 12100-1:2010, 3.34]" with "[SOURCE: IEC 61508-4:2010, 3.6.7, modified – Terminology adapted to machinery]"

4.2 Design process

Replace, in NOTE 1 of Subclause 4.2, "Annex H" with "Annex G".

6.5.2 Requirements for the control of systematic faults

Replace, in NOTE 2 of Subclause 6.5.2, "IEC 61784-3:2016" with "IEC 61784-3:2021".

6.8 Security aspects

Replace, in NOTE 2 of Subclause 6.8, "IEC TR 63074" with "IEC TS 63074".

Replace, in NOTE 2 of Subclause 6.8, "ISO/IEC 27001:2013" with "ISO/IEC 27001:2021".

7.3.3.3 Fault exclusion

Replace, in first NOTE of Subclause 7.3.3.3, "NOTE" with "NOTE 1"

Replace, in second NOTE of Subclause 7.3.3.3, "NOTE" with "NOTE 2"

7.3.4.2 Relationship of relevant parameters

Replace, in 10th paragraph of Subclause 7.3.4.2, "the useful lifetime of the component" with "T_{10D} of the component"

*Add, after 10th paragraph of Subclause 7.3.4.2, a new note "*NOTE 5 Similar to Formula (11) T_{10} is evaluated by $T_{10} = \frac{B_{10}}{n_{op}}$."

7.4.1 Estimation of safe failure fraction (SFF)

*Replace, in 1st paragraph, b) of Subclause 7.4.2, "*component failure data*" with "failure rate data"*

Replace, in 5th paragraph of Subclause 7.4.2, "EXAMPLE 2" with "EXAMPLE 1"

Replace, in 5th paragraph of Subclause 7.4.2, Formula (13) with Formula

$$\text{SFF} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \approx \frac{\sum \lambda_{DD}}{\sum \lambda_D} \tag{13}$$

Replace, in 5th paragraph of Subclause 7.4.2, Formula of 1st EXAMPLE with

$$\text{SFF} \approx \frac{\lambda_{DD1}}{\lambda_{D1}} = \frac{DC_1\,\lambda_{D1}}{\lambda_{D1}} = DC_1 \tag{14}$$

Replace, in 5th paragraph of Subclause 7.4.2, Formula of 2nd EXAMPLE with

$$\text{SFF} \approx \frac{\lambda_{DD1} + \lambda_{DD2}}{\lambda_{D1} + \lambda_{D2}} = \frac{DC_1\,\lambda_{D1} + DC_2\,\lambda_{D2}}{\lambda_{D1} + \lambda_{D2}} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}}} \tag{15}$$

7.4.3.3 Diagnostic coverage (DC)

Replace, in 1st paragraph of Subclause 7.4.3.3, Formula (14) with

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \tag{16}$$

Table 6 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem

Replace, in NOTE 3 of Table 6, "7.4.3.2" with "7.5.3"

Figure 8 – Subsystem A logical representation

Replace, in Figure 8 title, "Subsystem" with "Basic subsystem architecture".

Figure 9 – Subsystem B logical representation

Replace, in Figure 9 title, "Subsystem" with "Basic subsystem architecture".

Figure 10 – Subsystem C logical representation

Replace, in Figure 10 title, "Subsystem" with "Basic subsystem architecture".

Figure 11 – Subsystem D logical representation

Replace, in Figure 11 title, "Subsystem" with "Basic subsystem architecture".

8.4.1.2 Software safety lifecycle model – SW level 2

Replace, in last sentence of the 2nd paragraph of Subclause 8.4.1.2, "9.5.3" with "9.5.4".

Figure 14 – V-model of software safety lifecycle for SW level 2

Replace, in Figure 14, "Software system specification" with " Software system design specification".

A.2.4.2 Frequency and duration of exposure

Remove, in 3rd paragraph, 1st sentence, the text "(referred to a period ≥ to one year)"

Table A.6 – Matrix assignment for determining the required SIL (or PL_r) for a safety function

Renumber, in Table A.6, the last "NOTE 3" to "NOTE 4".

B.4.2.4.2 Annex H approaches

Replace, in the second paragraph of Subclause B.4.2.4.2, "T_2 = 1/C = n_{op}/8 760 h*" with "*T_2 = 1 / C = 8 760 h / n_{op}*".*

B.4.4.4.2 Annex H approaches

Replace, in the second paragraph of Subclause B.4.4.4.2, "T_2 = 1/C = n_{op}/8 760 h" with "T_2 = 1 / C = 8 760 h / n_{op}".

B.4.5.1 Target

Replace, in 1st paragraph of Subclause B.4.5.1, "6.4.2" with "6.4.1".

B.4.5.3 Architectural constraints

Replace, in 1st paragraph of Subclause B.4.5.3, "6.4.2" with "6.4.1".

Table C.1 – Standards references and $MTTF_D$ or B_{10D} values for components

Add, in Table C.1 5th row ("Hydraulic components 250 000 > nop" and 3rd column ("Other relevant standards"), "ISO 4413".

Replace, in the 1st sentence of Table C.1 NOTE 3, "in the subsequent SCS" with "provided by another subsystem of the SCS.".

Table D.1 (2/2)

Replace, in the 2nd row and last column of Table D.1 (2/2), "moving cart" with "moving part or final element".

Replace, in the 6st row and last column of Table D.1 (2/2), "(placed in series or in parallel on the logic)" with "(placed in series or on two separate inputs of the logic".

E.1 General

Replace, in the 1st paragraph of Subclause E.1, "two simple qualitative approaches" with "a simple qualitative approach".

E.2.2 Estimation of effect of CCF

Replace, in the 1st paragraph, 2nd sentence of Subclause E.2.2, "safety-related parts of the control system" with "SCS".

Figure H.1 – Subsystem A logical representation

Replace, in Figure H.1 title, "Subsystem" with "Basic subsystem architecture".

Figure H.2 – Subsystem B logical representation

Replace, in Figure H.2 title, "Subsystem" with "Basic subsystem architecture".

H.2.4.1 General

Replace, in 3rd paragraph of Subclause H.2.4.1, "7.4.3" with "7.4.3.2".

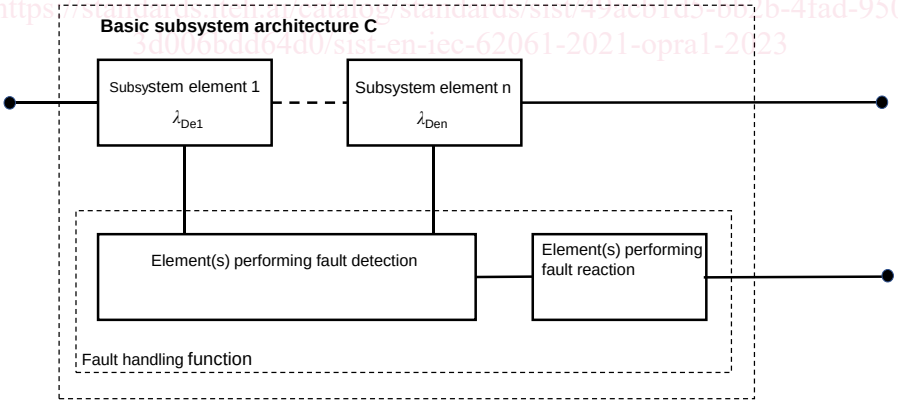
Figure H.3 – Subsystem C logical representation

Replace, in Figure H.3 title, "Subsystem" with "Basic subsystem architecture".

Figure H.4 – Correlation of subsystem C and the pertinent fault handling function

Replace, in Figure H.4 title, "subsystem" with "basic subsystem architecture".

Replace, in Figure H.4, the Figure with the following new Figure:



H.2.4.2 External fault handling function

Remove, in Subclause H.2.4.2, 2nd paragraph.

Figure H.5 – Subsystem C with external fault handling function

Replace, in Figure H.5 title, "Subsystem" with "Basic subsystem architecture".

H.2.4.3 Fault handling partially or completely done within the subsystem

Replace, in the 4th paragraph of Subclause H.2.4.3, "(H.4)" with "(H.3)".

Replace, in NOTE 1 of Subclause H.2.4.3, "fault reaction function channel (λ_{DFR})" with "fault handling function channel ($\lambda_{D\ FH}$)".

Table H.3 – Minimum value of $1/\lambda_{D\ FH}$ for the applicability of *PFH* equation (H.4)

Replace, in Table H.3 title, "(H.4)" with "(H.3)".

Figure H.6 – Subsystem C with external fault diagnostics

Replace, in Figure H.6 title, "Subsystem" with "Basic subsystem architecture".

Figure H.7 – Subsystem C with external fault reaction

Replace, in Figure H.7 title, "Subsystem" with "Basic subsystem architecture".

Figure H.8 – Subsystem C with internal fault diagnostics and internal fault reaction

Replace, in Figure H.8 title, "Subsystem" with "Basic subsystem architecture".

Figure H.9 – Subsystem D logical representation

Replace, in Figure H.9 title, "Subsystem" with "Basic subsystem architecture".

Figure I.2 – Example of activities, documents and roles *(1 of 2)*

Replace, in Figure I.2, Key EE, "expert engineer or operator" with " expert engineer".

Replace, in Figure I.2, "production specification" with "product specification".

Figure I.2 – Example of activities, documents and roles *(2 of 2)*

Replace, in Figure I.2, Key EE, "expert engineer or operator" with " expert engineer".