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

oSIST prEN IEC 62061:2019 **en,fr,de**

44/847/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

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

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: ☐ 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 **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.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

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.

TITLE:

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

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

CONTENTS

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)

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

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

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

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

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

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.

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

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

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

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.

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

This standard provides a machine sector specific framework for functional safety of a 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 a 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 machinecontrol system to stop hazardous machine operation. Also 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 standard 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 6.2.4);
- validate the SCS.

This standard 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.