

© Copyright SEK Svensk Elstandard. Reproduction in any form without permission is prohibited.

Safety of machinery – Security aspects related to functional safety of safety-related control systems

(IEC Technical Specification 63074:2023)

Nationellt förord

En teknisk specifikation, TS, utarbetad inom IEC är avsedd att ge vägledning beträffande specifikationer eller provningsmetoder eller ge specifikationer för teknikområden under snabb utveckling. Ett förslag till internationell standard, som det inte varit möjligt att nå tillräcklig enighet kring, kan också fastställas som TS, för att användas på försök (som förstandard) och för att efter eventuella justeringar eller bearbetningar senare fastställas som internationell standard. En teknisk specifikation ska omprövas inom tre år.

ICS 13.110.00; 29.020.00

Detta dokument är fastställt av SEK Svensk Elstandard, som också kan lämna upplysningar om **sakinnehållet**.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se



TECHNICAL SPECIFICATION



Safety of machinery – Security aspects related to functional safety of safety-related control systems

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 29.020

ISBN 978-2-8322-6468-3

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

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms, definitions, and abbreviated terms	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms.....	12
4 Safety and security overview	12
4.1 General.....	12
4.2 Safety objectives	12
4.3 Security objectives.....	13
5 Security aspects related to functional safety	15
5.1 General.....	15
5.1.1 Security risk assessment	15
5.1.2 Security risk response strategy.....	16
5.2 Security countermeasures.....	16
5.2.1 General	16
5.2.2 Identification and authentication	18
5.2.3 Use control	18
5.2.4 System integrity.....	18
5.2.5 Data confidentiality	18
5.2.6 Restricted data flow	19
5.2.7 Timely response to events	19
5.2.8 Resource availability.....	19
6 Cybersecurity and functional safety of machinery	19
6.1 General.....	19
6.2 Aspects related to the protection against corruption	19
6.3 Security countermeasures against corruption.....	20
6.3.1 General	20
6.3.2 Potential sources of cyber threats.....	20
6.3.3 Multi-factor authentication	20
6.3.4 Network architecture.....	20
6.3.5 Portable devices.....	21
6.3.6 Wireless communication	21
6.3.7 Remote access.....	21
6.3.8 Attack through direct physical connection	22
7 Verification and maintenance of security countermeasures	22
8 Information for the user of the machine(s)	22
Annex A (informative) Basic information related to threats and threat modelling approach	23
A.1 Evaluation of threats	23
A.2 Examples of threat related to a safety-related device	24
Annex B (informative) Security risk assessment triggers	26
B.1 General.....	26
B.2 Event driven triggers.....	26

Annex C (informative) Example of information flow between device supplier, manufacturer of machine, integrator and user of machine	27
C.1 General.....	27
C.2 Example 1 – Design phase of the machine.....	27
C.3 Example 2 – Use phase of the machine	27
Bibliography.....	29
Figure 1 – Relationship between threat(s), vulnerabilities, consequence(s) and security risk(s) for SCS performing safety function(s).....	14
Figure 2 – Possible effects of security risk(s) to an SCS	14
Figure A.1 – Safety-related device and possible accesses	25
Figure C.1 – Example of generic information flow during design phase	27
Figure C.2 – Example of generic information flow during use phase.....	28
Figure C.3 – Example of information flow during use phase in context of IEC 62443-2-4.....	28
Table 1 – Overview of foundational requirements and possible influence(s) on an SCS	17

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SAFETY OF MACHINERY – SECURITY ASPECTS RELATED TO
FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS**

FOREWORD

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

IEC TS 63074 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects. It is a Technical Specification.

This first edition cancels and replaces the first edition of IEC TR 63074 published in 2019. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to IEC TR 63074:2019:

- a) new Clause 6 on Cybersecurity and functional safety of machinery;
- b) new Figure A.1;
- c) new Clause C.3 Example 2 – Use phase of the machine.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
44/964/DTS	44/987/RVDTS

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

The language used for the development of this Technical Specification is English.

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this 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.

INTRODUCTION

Industrial automation systems can be exposed to security threats exploiting vulnerabilities due to the fact that:

- access to the control system is possible, for example re-programming of machine functions (including safety);
- "convergence" between standard IT and industrial systems is increasing;
- operating systems have become present in embedded systems, for example IP-based protocols are replacing proprietary network protocols and data is exchanged directly from the SCADA network into the office world;
- software is developed by reusing existing third-party software components;
- remote access from suppliers has become the standard way of operations / maintenance, with an increased cyber security risk regarding for example unauthorized access, availability and integrity.

In the context of the machine, the machine control system represents an industrial automation system.

The safety-related control system of machines is part of the machine control system and can therefore also be subject to security threats that can result in a loss of the ability to maintain safe operation of a machine.

NOTE 1 The risk potential of attack opportunities is significant due to the trends and developments of threats and the amount of known vulnerabilities. Security objectives are mainly described in terms of confidentiality, integrity and availability, which in general will be identified and prioritized by using a risk-based approach.

Functional safety objectives consider the risk by estimating the severity of harm and the probability of occurrence of that harm. The effects of any risk (hazardous event) determine the requirements for safety integrity (safety integrity level (SIL) in accordance with IEC 62061 for safety-related control systems or the IEC 61508 series for electrical/electronic/programmable electronic safety-related systems, or the Performance Level (PL) in accordance with ISO 13849-1 for safety-related parts of control systems).

With respect to the safety function, the security threats (internal or external) can influence the safety integrity and the overall system availability.

NOTE 2 In order to ensure the security objectives, IEC 62443-3-3 defines and recommends security requirements ("foundational requirements") to be fulfilled by the relevant system.

NOTE 3 The overall security strategy is not covered in this document; further information is provided for example in the IEC 62443 series or ISO/IEC 27001.

Measures to prevent reasonably foreseeable misuse by physical manipulation are addressed in some machinery functional safety standards (e.g. the IEC 61496 series and ISO 14119).

NOTE 4 Measures to prevent reasonably foreseeable misuse by physical manipulation are not the same as physical security in the IEC 62443 series.

SAFETY OF MACHINERY – SECURITY ASPECTS RELATED TO FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

1 Scope

This technical specification identifies the relevant aspects of the IEC 62443 series related to security threats and vulnerabilities that are considered for the design and implementation of safety-related control systems (SCS) which can lead to the loss of the ability to maintain safe operation of a machine.

Typical security aspects related to the machine with potential relation to SCS are:

- vulnerabilities of the SCS either directly or indirectly through the other parts of the machine which can be exploited by security threats that can result in security attacks (security breach);
- influence on the safety characteristics and ability of the SCS to properly perform its function(s);
- typical use case definition and application of a corresponding threat model.

Non-safety-related aspects of security threats and vulnerabilities are not considered in this document.

NOTE Non-safety-related parts of the machine control system can also be affected by security threats with possible impact on operation of a machine, such as productivity, performance or quality. For these aspects, refer to the IEC 62443 series.

The focus of this document is on intentional malicious actions. However, intentional hardware manipulation (e.g. wiring, exchange of components) or foreseeable misuse by physical manipulation of SCS (e.g. physical bypass) is not considered in this document.

This document does not cover security requirements for information technology (IT) products and for the design of devices used in the SCS (e.g., product specific standards can be available, such as IEC TS 63208).

2 Normative references

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

IEC 62061:2021, *Safety of machinery – Functional safety of safety-related control systems*