IEC TS 63074

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

colour inside

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



IEC TS 63074:2023-02(en)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2023 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 Varembé
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 It also gives information on projects, replaced and withdrawn publications.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. 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 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TS 63074

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

colour inside

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.

® Registered trademark of the International Electrotechnical Commission

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*

3 Terms, definitions, and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
asset
physical or logical object having either a perceived or actual value to a control system

[SOURCE: IEC 62443-3-3:2013, 3.1.1, modified – "the IACS" replaced by "a control system", removal of Note 1 to entry]

3.1.2
attack
assault on a system that derives from an intelligent threat

[SOURCE: IEC 62443-3-3:2013, 3.1.3, modified – removal of Notes 1 and 2 to entry]

3.1.3
availability
ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided

[SOURCE: IEC TS 62443-1-1:2009, 3.2.16, modified – Notes deleted]

3.1.4
confidentiality
assurance that information is not disclosed to unauthorized individuals, processes, or devices

[SOURCE: IEC TS 62443-1-1:2009, 3.2.28]

3.1.5
machine control system
system that responds to input signals from the machine, a process and/or from an operator and generates output signals causing the machine to operate in the desired manner

Note 1 to entry: The machine control system includes input and output devices, including sensors and actuators.

Note 2 to entry: “Signals” can also be data.

[SOURCE: IEC 61508-4:2010, 3.3.3, modified – The term defined has been changed, "process" has been changed to "machine", Note to entry amended and Note 2 to entry added]

3.1.6
cybersecurity
<of the machine control system> set of activities necessary to protect network and information systems of the machine control system, the users of such systems, and other persons from cyber threats, typically regarding the aspects of confidentiality, integrity and availability

3.1.7
cyber threat
<of the machine control system> potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons, typically exploiting vulnerabilities of a machine system

3.1.8
dangerous failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the machine is put into a hazardous or potentially hazardous state; or
b) decreases the probability that the safety function operates correctly when required

[SOURCE: IEC 61508-4:2010, 3.6.7, modified – in item a) “EUC” has been replaced by "machine"]

3.1.9
functional safety
part of the overall safety relating to the machine and the machine control system that depends on the correct functioning of the safety-related control systems and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – "EUC" replaced by "machine", "E/E/PE safety-related systems" replaced by “safety-related control systems”]

3.1.10
integrator
entity who designs, manufactures or assembles an integrated manufacturing system and is responsible for the safety strategy, including the protective measures, control interfaces and interconnections of the control system

Note 1 to entry: The integrator may be for example a manufacturer, assembler, engineering company, or entity with the overall responsibility for the machine.

[SOURCE: IEC 62061:2021, 3.2.13]

3.1.11
machinery
machine
assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application

Note 1 to entry: The term "machinery" also covers an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

[SOURCE: ISO 12100:2010, 3.1, modified – removal of Note 2]

3.1.12
network and information systems
<of the machine control system> means or devices that contribute to or participate in the transmission or exchange of data

Note 1 to entry: Network and information systems can be:

a) an electronic communications network within the meaning of transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, radio, optical or other electromagnetic means used for a machine;

b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

3.1.13
protective measure
measure intended to achieve risk reduction, implemented

– by the designer (inherently safe design, safeguarding and complementary protective measures, information for use) and/or

– by the user (organization: safe working procedures, supervision, permit-to-work systems; provision and use of additional safeguards; use of personal protective equipment; training)

[SOURCE: ISO 12100:2010, 3.19, modified – removal of Note]

3.1.14
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12]

3.1.15
safety
freedom from risk which is not tolerable

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

3.1.16
safety function
function of a machine whose failure can result in an immediate increase of the risk(s)

[SOURCE: ISO 12100:2010, 3.30]

3.1.17
safety integrity
probability of a safety-related control system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

[SOURCE: IEC 61508-4:2010, 3.5.4, modified –"an E/E/PE safety-related system" replaced by "a safety-related control system", removal of Notes]

3.1.18
safety-related control system
SCS
part of the control system of a machine which implements a safety function by one or more subsystems

[SOURCE: IEC 62061, 3.2.3, modified – Note 1 to entry omitted]

3.1.19
security
a) measures taken to protect a system

b) condition of a system that results from the establishment and maintenance of measures to protect the system

c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss

d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems

e) prevention of illegal or unwanted penetration of, or interference with, the proper and intended operation of a machinery and its control system

Note 1 to entry: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.99, modified – in item e) “industrial automation and control system” replaced by “a machinery and its control system”]

3.1.20
countermeasure
security countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

[SOURCE: IEC TS 62443-1-1:2009, 3.2.33, modified – addition of second preferred term "security countermeasure", removal of Note]

3.1.21
security risk
expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence

[SOURCE: IEC TS 62443-1-1:2009, 3.2.87, modified – in the term, "risk" replaced by "security risk"]

3.1.22
security risk assessment
process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize the exposure

[SOURCE: IEC TS 62443-1-1:2009, 3.2.88, modified –"risk assessment" replaced by "security risk assessment" in the term, "total exposure" replaced by "the exposure", removal of Notes.]

3.1.23
subsystem
entity of the top-level architectural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function

[SOURCE: IEC 61508-4:2010, 3.4.4, modified – removal of references to 3.6.7 a) within the definition]

3.1.24
threat
circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

[SOURCE: IEC 62443-3-3:2013, 3.1.44]

3.1.25
user of the machine
entity with the overall responsibility for the use of the machine

3.1.26
vulnerability
<of the machine control system> weakness of a machine control system or a countermeasure that can be exploited by one or more threats to violate the machine control system's integrity

3.1.27
vulnerability assessment
formal description and evaluation of the vulnerabilities in a system

[SOURCE: IEC 62443-2-1:2010, 3.1.44]

3.2 Abbreviated terms

CVSS	common vulnerability scoring system
DoS	denial of service
IT	information technology
JTAG	joint test action group
LAN	local area network
PL	performance level
PLC	programmable logic controller
SCS	safety-related control system
SD	secure digital
SIL	safety integrity level
USB	universal serial bus
VPN	virtual private network
WLAN	wireless local area network

4 Safety and security overview

4.1 General

The relationship between safety and security aspects can be characterized as follows:

– a machine has appropriate protective measures;
– security countermeasures applied for a machine are to be appropriate in order to avoid degradation of the performance of protective measures that implement safety function(s) (including safety-related data).

NOTE Persons who are qualified to implement security countermeasures are not necessarily the same people who are qualified to implement SCS. Therefore it is reasonable to mutually exchange information and support.

4.2 Safety objectives

Safety of machinery is based on risk assessment which can be performed in accordance with ISO 12100 and where available, by following a type-C standard for specific machine types, in combination with the derived risk reduction measures which can be performed by safety function(s).