IEC TR 63074

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

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

IEC TR 63074:2019-05(en)

IEC Central Office
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 It also gives information on projects, replaced and withdrawn publications.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.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC TR 63074

Edition 1.0 2019-05

TECHNICAL REPORT

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 978-2-8322-6818-6

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

CONTENTS

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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

Technical Report IEC TR 63074 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

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

DTR	Report on voting
44/842/DTR	44/843/RVDTR

Full information on the voting for the approval of this Technical Report 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.

A bilingual version of this publication may be issued at a later date.

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 attacks due to the fact that:

– access to the control system is possible, e.g. re-programming of machine functions (including safety);

– "convergence" between standard IT and industrial systems is increasing;

– operating systems have become present in embedded systems, e.g. 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 e.g. unauthorized access, availability and integrity.

As part of an industrial automation system, safety-related control systems of machines can also be subject to security attacks 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 seeing 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 need to 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) according to IEC 62061 or IEC 61508 or Performance Level (PL) according to ISO 13849-1).

With respect to the safety function, the security threats (internal or external) might 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 standard, further information is provided e.g. in IEC 62443 (all parts) or ISO/IEC 27001.

Misuse by physical manipulation is covered in some machinery functional safety standards (e.g. IEC 61496 (all parts) and ISO 14119).

NOTE 4 "Misuse by physical manipulation" is not considered to be the same as physical security in the IEC 62443 (all parts), for example in IEC 62443-2-1:2010, 4.3.3.3. Physical security means for example control (restriction) of access by means of physical obstruction.

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

1 Scope

This Technical Report gives guidance on the use of IEC 62443 (all parts) related to those aspects of security threats and vulnerabilities that could influence functional safety implemented and realized by safety-related control systems (SCS) and could lead to the loss of the ability to maintain safe operation of a machine.

NOTE 1 For example, an attack on a machine (safety function) such that it affects the availability of the machine and can result in a safety function being bypassed.

Considered security aspects of 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.

NOTE 2 For other aspects of security threats and vulnerabilities, the provisions of the IEC 62443 (all parts) can apply.

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, *Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems*

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

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

3 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

Note 1 to entry: This ability depends on the combined aspects of the reliability performance, the maintainability performance and the maintenance support performance.

Note 2 to entry: Required external resources, other than maintenance resources do not affect the availability performance of the item.

Note 3 to entry: In French the term "disponibilité" is also used in the sense of "instantaneous availability". In German the term "Verfügbarkeit" is also used in the sense of "instantaneous availability".

[SOURCE: IEC TS 62443-1-1:2009, 3.2.16, modified – addition of information about German terminology in Note 3]

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
control system
system which responds to an input from, for example, the process, other machine elements, an operator, external control equipment, and generates an output(s) causing the machine to behave in the intended manner

3.1.6
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 – "EUC" replaced by "machine"]

3.1.7
functional safety
part of the safety of the machine and the machine control system which depends on the correct functioning of the safety-related control system, other technology safety-related systems and external risk reduction facilities

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – "EUC" replaced by "machine", "E/E/PE" deleted]

3.1.8
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 12100-1:2010, 3.1, modified – removal of Note 2]

3.1.9
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]

3.1.10
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12]

3.1.11
safety
freedom from risk which is not tolerable

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

3.1.12
safety function
function of a machine whose failure can result in an immediate increase of the risk(s)

[SOURCE: ISO 12100, 3.30]

3.1.13
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]

3.1.14
SCS
Safety-related Control System
part of the control system of a machine which implements a safety function

Note 1 to entry: This is equivalent to SRECS of IEC 62061:2015 or one or several SRP/CS of ISO 13849-1.

[SOURCE: MT 62061, 3.2.3, modified – Note 1 removed]

3.1.15
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 an industrial automation and 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]

3.1.16
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]

3.1.17
Security Level
SL
measure of confidence that the IACS (industrial automation control system) is free from vulnerabilities and functions in the intended manner

[SOURCE: IEC 62443-3-3:2013, 3.1.38, modified – addition of second preferred term "SL", removal of Note]

3.1.18
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 – "risk" replaced by "security risk"]

3.1.19
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", "total exposure" replaced by "the exposure", removal of Notes]