IEC TR 63074

Edition 1.0 2019-05

TECHNICAL REPORT

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

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*