

TNI	Meranie, riadenie a automatizácia priemyselných procesov Štruktúra funkčnej bezpečnosti a ochrany	TNI CLC IEC/TR 63069 18 0451
------------	--	--

Industrial-process measurement, control and automation - Framework for functional safety and security

Táto technická normalizačná informácia obsahuje anglickú verziu CLC IEC/TR 63069:2020, IEC/TR 63069:2019.
This Technical standard information includes the English version of CLC IEC/TR 63069:2020,
IEC/TR 63069:2019.

Táto technická normalizačná informácia bola oznámená vo Vestníku ÚNMS SR č. 06/20

130795

TECHNICAL REPORT

CLC IEC/TR 63069

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

February 2020

ICS 13.110; 25.040.40; 29.020

English Version

Industrial-process measurement, control and automation -
Framework for functional safety and security
(IEC/TR 63069:2019)

Mesure, commande et automation dans les processus
industriels – Cadre pour la sécurité et la sûreté fonctionnelle
(IEC/TR 63069:2019)

Industrielle Prozess-Leittechnik, Steuerungs- und
Automatisierungstechnik - Rahmenbedingungen für
Funktionale Sicherheit und IT-Sicherheit
(IEC/TR 63069:2019)

This Technical Report was approved by CENELEC on 2020-01-27.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

CLC IEC/TR 63069:2020 (E)**European foreword**

This document (CLC IEC/TR 63069:2020) consists of the text of IEC/TR 63069:2019 prepared by IEC/TC 65 "Industrial-process measurement, control and automation".

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Technical Report IEC/TR 63069:2019 was approved by CENELEC as a

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61508-1	NOTE	Harmonized as EN 61508-1
IEC 61508-2	NOTE	Harmonized as EN 61508-2
IEC 61508-3	NOTE	Harmonized as EN 61508-3
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified)
IEC 61511 (series)	NOTE	Harmonized as EN 61511 (series)
IEC 62443-2-4:2015	NOTE	Harmonized as EN IEC 62443-2-4:2019 (not modified)
IEC 62443-3-3:2013	NOTE	Harmonized as EN IEC 62443-3-3:2019 (not modified)
IEC 62443-4-1	NOTE	Harmonized as EN IEC 62443-4-1

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61508	series	Functional safety electrical/electronic/programmable electronic safety-related systems	of EN 61508	series
IEC 62443	series	Industrial communication networks Network and system security	- -	series



IEC TR 63069

Edition 1.0 2019-05

TECHNICAL REPORT



Industrial-process measurement, control and automation – Framework for functional safety and security





THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2019 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 Central Office
3, rue de Varembe
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 63069

Edition 1.0 2019-05

TECHNICAL REPORT



Industrial-process measurement, control and automation – Framework for functional safety and security

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.40; 29.020

ISBN 978-2-8322-6925-1

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

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
0.1 Purpose of this document	6
0.2 Background.....	6
0.3 Issues on the terminology	6
0.4 Target audience	6
1 Scope.....	7
2 Normative references	7
3 Terms, definitions, symbols, abbreviated terms and conventions	7
3.1 Terms and definitions defined for this document	7
3.2 Abbreviated terms.....	15
3.3 Explanation for common terms with different definitions	15
4 Context of security related to functional safety.....	20
4.1 Description of functions.....	20
4.2 Security environment	20
5 Guiding principles	22
6 Life cycle recommendations for co-engineering	22
6.1 General.....	22
6.2 Managing security related safety aspects.....	25
7 Risk assessment considerations	25
7.1 Risk assessment at higher level.....	25
7.2 Trade-off analysis	26
7.3 Considerations for threat-risk assessment <security>	26
7.3.1 General	26
7.3.2 Recommendations to the threat-risk assessment <security>	27
7.3.3 Considerations related to security countermeasures	27
7.3.4 Vulnerabilities and examples of root causes	27
7.4 Malevolent and unauthorized actions	27
7.4.1 General	27
7.4.2 Reasonably foreseeable misuse (safety).....	28
7.4.3 Prevention of malevolent and unauthorized actions (security)	28
7.4.4 Combination of password protection measures	28
8 Incident response readiness and incident handling	28
8.1 General.....	28
8.2 Incident response readiness	28
8.3 Incident handling	28
Bibliography.....	30
Figure 1 – Overview of functions of an IACS	20
Figure 2 – Safety domain and security domain.....	21
Figure 3 – Security environment	21
Figure 4 – Safety and security interaction	23
Figure 5 – Safety and security risk assessments as part of a risk assessment at higher level.....	26

Table 1 – Terms with multiple definitions	15
Table 2 – Recommended activities in life cycle stages	24

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION –
FRAMEWORK FOR FUNCTIONAL SAFETY AND SECURITY**

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".

IEC TR 63069 has been prepared by IEC technical committee TC 65: Industrial-process measurement, control and automation.

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

Draft DTR	Report on voting
65/698/DTR	65/713A/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 document has been drafted in accordance with the ISO/IEC Directives, Part 2.

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.

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

0.1 Purpose of this document

Many sector specific guides, standards and technical specifications have been developed in the fields of safety and security. However, a generic document for framework for safety and security is largely expected by industry actors. Even the terms "safety" and "security" are sometimes used for different meanings in these documents. As a result, it can be difficult to apply them holistically at the same time to a manufacturing system.

0.2 Background

Security has become a new factor to be considered in system engineering. The parts of the IEC 61508 series published in 2010 took into account that security can impact functional safety.

In IEC TC 65 (Industrial-process measurement, control and automation), considerable concerns arose with respect to the impacts of security incidents to safety functions in IACS (industrial automation and control systems); many complex systems of that kind are becoming connected systems (particularly by interaction based on wireless connectivity from sensors/actuators to complete plants, grids, etc.) for maintenance and operations. The overall question was: "How to design and manage safety and security – in cooperation, integrated, or separate system?"

0.3 Issues on the terminology

Definitions of some terms, such as "safety", "security" and "risk", are sometimes different in different documents. Although they are consistent in a set of documents in each area of safety and security, they can be inconsistent when both standards are applied at the same time. From these reasons, the terminology is carefully used in this document.

0.4 Target audience

The target audience of this document includes, but is not limited to,

- asset owners (including those responsible for concept and governance),
- system integrators (including those responsible for design and realisation),
- product suppliers (including those responsible for design and realisation),
- service providers (including operators and maintainers), and
- authorities (including those responsible for assessment and audit).

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – FRAMEWORK FOR FUNCTIONAL SAFETY AND SECURITY

1 Scope

This document explains and provides guidance on the common application of IEC 61508 (all parts) and IEC 62443 (all parts) in the area of industrial-process measurement, control and automation.

This document can apply to other industrial sectors where IEC 61508 (all parts) and IEC 62443 (all parts) are applied.

NOTE Usage or reference of this document for industry specific sector standards is encouraged.

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 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62443 (all parts), *Security for industrial automation and control systems*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN