SLOVENSKI STANDARD
kSIST-TS CLC IEC/FprTS 62443-6-1:2024

01-oktober-2024

Zaščita industrijske avtomatizacije in nadzornih sistemov - 1-6. del: Metodologija ocenjevanja varnosti za IEC 62443-2-4

Security for industrial automation and control systems - Part 6-1: Security evaluation methodology for IEC 62443-2-4

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 6-1: Security-Evaluierungsmethodik für IEC 62443-2-4

Sécurité des automatismes industriels et des systèmes de commande - Partie 6-1: Méthodologie d'évaluation de la sécurité pour la IEC 62443-2-4

Ta slovenski standard je istoveten z: **CLC IEC/FprTS 62443-6-1:2024**

ICS:

25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

kSIST-TS CLC IEC/FprTS 62443-6-1:2024 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

FINAL DRAFT
CLC IEC/FprTS 62443-6-1

August 2024

ICS 25.040.40 -

English Version

Security for industrial automation and control systems - Part 6-1: Security evaluation methodology for IEC 62443-2-4 (IEC/TS 62443-6-1:2024)

Sécurité des automatismes industriels et des systèmes de commande - Partie 6-1: Méthodologie d'évaluation de la sécurité pour la IEC 62443-2-4 (IEC/TS 62443-6-1:2024)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 6-1: Security-Evaluierungsmethodik für IEC 62443-2-4 (IEC/TS 62443-6-1:2024)

This draft Technical Specification is submitted to CENELEC members for vote by correspondence.
Deadline for CENELEC: 2024-11-01.

The text of this draft consists of the text of IEC/TS 62443-6-1:2024 (65/1030/DTS).

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, Türkiye and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to a Technical Specification.

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

Project: 79829 Ref. No. CLC IEC/FprTS 62443-6-1:2024 E

European foreword

This document (CLC IEC/FprTS 62443-6-1:2024) consists of the text of document IEC/TS 62443-6-1:2024, prepared by IEC/TC 65 “Industrial-process measurement, control and automation".

This document is currently submitted to voting in accordance with the Internal Regulations, Part 2, Subclause 11.3.3 for acceptance as a CENELEC Technical Specification.

The following date is proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months

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.cencenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 62443-2-4	2015	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers	EN 62443-2-4	2019
+ A1	2017		+ A1	2019

IEC TS 62443-6-1

Edition 1.0 2024-03

TECHNICAL SPECIFICATION

colour inside

Security for industrial automation and control systems – Part 6-1: Security evaluation methodology for IEC 62443-2-4

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 25.040.40

ISBN 978-2-8322-8328-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 6-1: Security evaluation methodology for IEC 62443-2-4

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TS 62443-6-1 has been prepared by IEC technical committee TC 65: Industrial-process measurement, control and automation. It is a Technical Specification.

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

Draft	Report on voting
65/1030/DTS	65/1042A/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 https://www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at https://www.iec.ch/standardsdev/publications.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

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

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document 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

Repeatable and comparable evaluations of the security program according to IEC 62443-2-4[1] require a common understanding for acceptable evaluation criteria and conformance evidence.

This document supports service providers and evaluators to do a conformity assessment by evaluating the security program against the requirements of IEC 62443-2-4.

This document specifies the evaluation methodology to support interested parties, for example during conformity assessment activities to achieve repeatable and reproducible evaluation results against IEC 62443-2-4 requirements.

[1] Throughout the document, when reference is being made to IEC 62443-2-4 (undated), this means IEC 62443-2-4:2015 and IEC 62443-2-4:2015/AMD1:2017 (Ed.1). A consolidated version of IEC 62443-2-4 is available.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 6-1: Security evaluation methodology for IEC 62443-2-4

1 Scope

This part of IEC 62443 specifies the evaluation methodology to support interested parties (e.g. during conformity assessment activities) to achieve repeatable and reproducible evaluation results against IEC 62443-2-4 requirements. This document is intended for first-party, second-party or third-party conformity assessment activity, for example by product suppliers, service providers, asset owners and conformity assessment bodies.

NOTE 1 62443-2-4 specifies requirements for security capabilities of an IACS service provider. These security capabilities can be offered as a security program during integration and maintenance of an automation solution.

NOTE 2 The term “conformity assessment” and the terms first-party conformity assessment activity, second-party conformity assessment activity and third-party conformity assessment activity are defined in ISO/IEC 17000.

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 62443-2-4:2015*, Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*
IEC 62443-2-4:2015/AMD1:2017

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

3.1.1
acceptable evaluation criteria
criteria which may be used for an evaluation

Note 1 to entry: Acceptable evaluation criteria indicated in this document are only examples, which are by no means complete and where also other or alternative evidence can be used to demonstrate the fulfilment of, or conformity to, the related requirement.

3.1.2
evaluator
individual or organisation that performs an evaluation

Note 1 to entry: An evaluator can act in the context of first-party, second-party or third-party conformity assessment activity according ISO/IEC 17000.

[SOURCE: ISO/IEC 25000:2014, 4.10, modified – the note has been added.]

3.1.3
evaluation
systematic determination of the extent to which the subject under evaluation (SuE) meets its specified requirements

[SOURCE: ISO/IEC 12207:2008, 4.12, modified – “an entity” has been replaced with “the subject under evaluation (SuE)".]

3.1.4
evidence of existence
EoE
documentation showing evidence that a process, procedures, templates or checklists had been created to support service provider activities

3.1.5
examine, verb
generate a verdict by analysis using evaluator expertise

[SOURCE: ISO/IEC 18045:2022, 3.9, modified – the note has been removed.]

3.1.6
key performance indicator
KPI
quantifiable measure that an organization uses to gauge or compare performance in terms of meeting its strategic and operational objectives

Note 1 to entry: The key performance indicator can be used to assess the success of applied measures or to demonstrate continuous improvement.

[SOURCE: ISO 18788:2015, 3.2.5, modified – the note has been added.]

3.1.7
overall maturity level
maturity level assigned to the entire security program

Note 1 to entry: Maturity levels are specified in IEC 62443-2-4:2015 and IEC 62443-2-4:2015/AMD1:2017, Table 1.

3.1.8
process
set of interrelated or interacting activities that transform input to output

[SOURCE: ISO 9000:2015, 3.4.1, modified – “use inputs to deliver an intended result” has been replaced with “transform input to output” and the notes have been removed.]

3.1.9
project
integration or maintenance service execution for an asset owner

3.1.10
proof of execution
PoE
documentation or other evidence showing the accomplishment of activities performed as a service provider for an automation solution

Note 1 to entry: In general, evidence of existence is the baseline documentation used during the execution.

3.1.11
reference architecture
generic control system, consisting of hardware and software components, used as a basis for an automation solution

3.1.12
subject under evaluation
SuE
subject agreed to be evaluated, related to conformity to the requirements of the document

Note 1 to entry: 'Subject under evaluation' is similar to the term 'object of conformity assessment' specified in ISO/IEC 17000.

EXAMPLE 1 Processes.

EXAMPLE 2 Systems.

EXAMPLE 3 Solutions.

EXAMPLE 4 Components.

3.1.13
security program
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures, and products that are applicable to the IACS

Note 1 to entry: The security program for IACS service providers refers to the policies and procedures defined by them to address security concerns of the IACS.

[SOURCE: IEC 62443-2-4:2015, 3.1.18]

3.1.14
trustworthiness
ability to meet stakeholders expectations in a verifiable way

[SOURCE:ISO/IEC 30145-2:2020, 3.9, modified – the notes have been removed.]

3.2 Abbreviated terms

EICAR	European Institute for Computer Antivirus Research (www.eicar.com)
EoE	evidence of existence
EWS	engineering workstation
FAT	factory acceptance test
KPI	key performance indicator
ML	maturity level
NDA	non-disclosure agreement
NIST	National Institute of Standards and Technology
PoE	proof of execution
RDP	remote desktop protocol