IEC TS 62443-6-2

Edition 1.0 2025-01

TECHNICAL SPECIFICATION

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

IEC TS 62443-6-2:2025-01(en)

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 It also gives information on projects, replaced and withdrawn publications.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, graphical symbols and the glossary. 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 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TS 62443-6-2

Edition 1.0 2025-01

TECHNICAL SPECIFICATION

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40

ISBN 978-2-8327-0141-6

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

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 62443-6-2 has been prepared by 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
65/1101/DTS	65/1109/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/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.

INTRODUCTION

Repeatable and comparable evaluations of IACS components according to IEC 62443-4-2 require a common agreed understanding for applicable evaluation criteria.

This document supports evaluators (e.g. vendors, asset owners, certification organizations or other 3rd parties) to perform a conformity assessment by evaluating an IACS component against the requirements of IEC 62443-4-2.

This document specifies an evaluation methodology for IACS components related to IEC 62443-4-2 and includes applicable evaluation criteria for each requirement of IEC 62443-4-2 and the requested security level for that requirement.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

1 Scope

This document specifies the evaluation methodology to support achieving repeatable and reproducible evaluation results for IACS components under evaluation against IEC 62443-4-2 requirements.

This document does not specify the definition of a complete certification scheme or certification program.

This document does not specify the process evaluations of the secure development lifecycle according to IEC 62443-4-1. The existing secure development lifecycle according to IEC 62443-4-1 is a prerequisite in this evaluation methodology.

This document does not specify particular tools, e.g. for the use in vulnerability or penetration testing.

This document does not focus on IACS components which were not developed according to the lifecycle process of IEC 62443-4-1.

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 62443-4-1:2018, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

IEC 62443-4-2:2019, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

3 Terms, definitions, abbreviated terms and acronyms

3.1 Terms and definitions

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

ISO and IEC maintain terminology 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
artefact
result of executing the development process or documented evidence according to the process requirements of IEC 62443-4-1

Note 1 to entry: Artefact is used with the same meaning as evidence but implies that the processes of IEC 62443-4-1 were applied with maturity level ML-3 or ML-4.

EXAMPLE Documented threat models, definitions and descriptions of security requirements, or test case specifications and results.

3.1.2
component under evaluation
IACS component which is the subject under evaluation

3.1.3
compensating countermeasure
actions taken in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

[SOURCE: IEC 62443-4-2:2019, 3.1.9, modified – "countermeasure employed" has been replaced by "actions taken" and the example has been removed.]

3.1.4
check
generate a verdict by a simple comparison

[SOURCE: ISO/IEC 18045:2022, 3.1]

3.1.5
cryptography

discipline that embodies the principles, means, and methods for the transformation of data in order to hide and recover their semantic content, prevent their unauthorized use, or prevent their undetected modification

[SOURCE: IEC 60050-171:2019, 171-08-08]

3.1.6
essential function
capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under control

[SOURCE: IEC 62443-4-2:2019, 3.1.20, modified – "function or" has been removed and the note has been removed.]

3.1.7
evaluation
systematic determination of the extent to which the IACS component under evaluation meets its specified requirements

Note 1 to entry: In the 62443 series, evaluation is used during conformity assessment.

3.1.8
evaluation activity
determination if the component under evaluation meets the referenced requirements of the standard

3.1.9
evaluation criteria
criteria used to determine whether the component under evaluation fulfills the requirement in a suitable manner

3.1.10
evaluation requirement
preconditions the product supplier has to enable the evaluation

Note 1 to entry: Evaluation requirements apply in addition to the requirements from IEC 62443-4-2 and IEC 62443-4-1.

3.1.11
evaluator
individual or organization that performs the evaluation

[SOURCE: ISO 25040:2011, 4.25]

3.1.12
examine
generate a verdict by analysis using evaluator expertise

[SOURCE: ISO/IEC 18045:2022, 3.9]

3.1.13
least privilege
basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

[SOURCE: IEC 62443-4-2:2019, 3.1.28]

3.1.14
met by component
requirements (i.e. CR and RE) are met by the component itself

3.1.15
met by system integration
requirements (i.e. CR and RE) are met by the system the component is integrated into, i.e. with the assistance of compensating countermeasure

3.1.16
product supplier
manufacturer of hardware and/or software product

[SOURCE: IEC 62443-4-1:2018, 3.1.24]

3.1.17
product security context
security provided to the product by the environment (asset owner deployment) in which the product is intended to be used

Note 1 to entry: The security provided to the product by its intended environment can effectively restrict the threats that are applicable to the product.

[SOURCE: IEC 62443-4-1:2018, 3.1.23]

3.1.18
security testing
security verification and validation testing
testing performed to assess the overall security of a component, product or system when used in its intended product security context and to determine if a component, product or system satisfies the product security requirements and satisfies its designed security purpose

Note 1 to entry: Examples for security testing according to IEC 62443-4-1 are threat mitigation testing, vulnerability testing and penetration testing.

Note 2 to entry: Security verification and validation testing is the term used in IEC 62443-4-1.

[SOURCE: IEC 62443-4-1:2018, 3.1.33, modified — the notes have been added.]

3.1.19
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[SOURCE: IEC 60050-192:2024, 192-01-17, modified – all notes have been removed.]

3.2 Abbreviated terms and acronyms

The following abbreviated terms and acronyms are used in this document.

CCSC common component security constraints
CR component requirement
CVSS common vulnerability scoring system
EDR embedded device requirement
DM defect management
EA evaluation activity
FR foundational requirements
HDR host device requirement
NDR network device requirement
PKI public key infrastructure
RE requirement enhancement
SAR software application requirement
SD secure by design
SG security guidelines
SI security implementation
SL security level
SM security management
SR security requirements
SUM security update management
SVV security verification and validation testing

4 Overview

4.1 Component requirements

This evaluation methodology supports achieving repeatable and reproducible results of the evaluation of IEC 62443-4-2 requirements (see also ISO/IEC 17000).

The evaluation methodology covers all requirements defined in IEC 62443-4-2:

- the common component security constraints (CCSC), and
- the component requirements (CR), with their related requirement enhancements (RE) and component type specific requirements (SAR, EDR, HDR, NDR).

4.2 Clarification for CCSC (common component security constraints)

4.2.1 General

IEC 62443-4-2 defines CCSC 1 to CCSC 4. These constraints are applied by the implementation of the component requirements and assessed as part of the evaluation activities described in this document. The relationship of CCSC 1 to CCSC 4 to other parts in the IEC 62443 series and to the CRs and REs are shown in Figure 1.

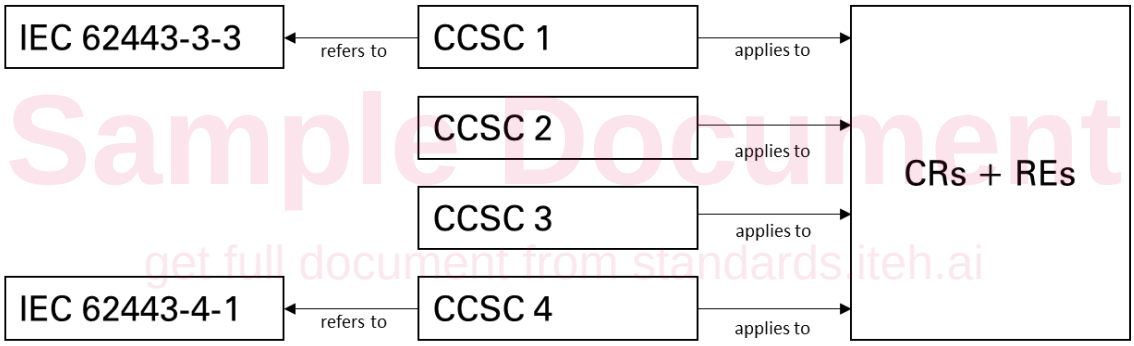

Figure 1 – Relationship between CCSCs and parts of the series or requirements

The definitions of the CCSCs are partly ambiguous and need some clarifications to ensure a consistent use in this evaluation methodology. According to IEC 62443-4-2 the CCSCs have to be applied to all CRs and REs.

4.2.2 CCSC 1: Support of essential functions

The components of the system shall adhere to specific constraints as described in IEC 62443-3-3:2013, Clause 4. (Source: IEC 62443-4-2:2019, 4.2)

Clarification

Subclause 4.2 of IEC 62443-3-3:2013 specifies security constraints related to essential functions which shall be adhered to, e.g. when specifying and implementing control systems. Components might be developed with or without knowledge of the control system in which they will finally be implemented.

If the control system in which they are finally implemented is unknown, then all capabilities related to the component requirements of IEC 62443-4-2 are expected to be built in the component. Alternatively, there have to be assumptions on the capabilities of how these are implemented at the system level, i.e. an assumed system security context has to be explicitly defined and documented as measures expected in the environment, e.g. in a dedicated document.

System essential functions are located at the system level. Component essential functions (see definition in 3.1.6) are defined at the component level.

If dedicated essential functions are supported by the component under evaluation these are expected to be defined in the security context. This becomes explicit in the evaluation step "security context evaluation".

4.2.3 CCSC 2: Compensating countermeasures

There will be cases where one or more requirements specified in this document cannot be met without the assistance of a compensating countermeasure that is external to the component. When this is the case the documentation for that component shall describe the appropriate countermeasures applied by the system to allow the requirement to be met when the component is integrated into a system. (Source: IEC 62443-4-2:2019, 4.3)

Clarification

The selection of security requirements (especially component requirements) is expected to be consistent with any specified compensating countermeasures (see 5.4 "Security requirement selection evaluation"). The selection of security requirements is verified in the evaluation step "security requirement selection evaluation".

NOTE The following clarification is formally defined as evaluation requirement ER-1 in 5.2.

Compensating countermeasures can be accepted during evaluation for a requirement if the product supplier is able to describe how to meet the requirement. An evaluator should in such a case be looking for documentation and indications from the product supplier on whether each technically applicable component requirement (CR) and requirement enhancements (RE) is met by component or met by system Integration.

For each CR and RE which is met by system integration, the following additional rules apply:

- system integration may be described in the defense in depth design (according to IEC 62443-4-1 SD-2 defense in depth design)
- system integration can be satisfied by a combination of configuration and technical component capabilities
- product security guidelines are required for integration and maintenance
- defense in depth measures which are expected in the environment have to be documented (according to IEC 62443-4-1 SG-2 defense in depth measures expected in the environment)

4.2.4 CCSC 3: Least privilege

When required and appropriate, one or more system components (software applications, embedded devices, host devices and network devices) shall provide the capability for the system to enforce the concept of least privilege. Individual system components shall provide the granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability shall be available when required. Granularity of permissions and assignment is dependent on the type of device and the product documentation for the device should define this in the product. (Source: IEC 62443-4-2:2019, 4.4)

Clarification

Least privilege is a basic principle which should be followed for the implementation of access rights for users, i.e. humans, software processes or devices. The least privilege principle is expected to be supported by the component in the context of different capabilities, i.e. the least privilege principle is applied to the component.