

---

**Zaščita industrijske avtomatizacije in kontrolnih sistemov - 2-6. del: Metodologija ocenjevanja zaščite za IEC 62443-4-2 (IEC/TS 62443-6-2:2025)**

Security for industrial automation and control systems – Part 6-2: Security evaluation methodology for IEC 62443-4-2 (IEC/TS 62443-6-2:2025)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 6-2:  
Sicherheitsbewertungsverfahren für IEC 62443-4-2 (IEC/TS 62443-6-2:2025)

Sécurité des automatismes industriels et des systèmes de commande - Partie 6-2:  
Méthodologie d'évaluation de la sécurité pour la IEC 62443-4-2 (IEC/TS 62443-6-2:2025)

**Ta slovenski standard je istoveten z: CLC/IEC TS 62443-6-2:2025**

**ICS:**

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

**SIST-TS CLC IEC/TS 62443-6-2:2026 en,fr,de**

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

TECHNICAL SPECIFICATION  
SPÉCIFICATION TECHNIQUE  
TECHNISCHE SPEZIFIKATION

**CLC/IEC TS 62443-6-2**

October 2025

ICS 25.040.40

English Version

**Security for industrial automation and control systems - Part 6-2:  
Security evaluation methodology for IEC 62443-4-2  
(IEC/TS 62443-6-2:2025)**

Sécurité des automatismes industriels et des systèmes de  
commande - Partie 6-2: Méthodologie d'évaluation de la  
sécurité pour la IEC 62443-4-2  
(IEC/TS 62443-6-2:2025)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil  
6-2: Sicherheitsbewertungsverfahren für IEC 62443-4-2  
(IEC/TS 62443-6-2:2025)

This Technical Specification was approved by CENELEC on 2025-10-13.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

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.

get full document from [standards.iteh.ai](https://standards.iteh.ai)



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/TS 62443-6-2:2025 (E)****European foreword**

This document (CLC IEC/TS 62443-6-2:2025) consists of the text of IEC/TS 62443-6-2:2025, prepared by CLC/TC 65X "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.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

**Endorsement notice**

The text of the International Technical Specification IEC/TS 62443-6-2:2025 was approved by CENELEC as a European Technical Specification without any modification.

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

ISO/IEC 18045:2022 NOTE Approved as EN ISO/IEC 18045:2023 (not modified)

ISO/IEC 17000:2020 NOTE Approved as EN ISO/IEC 17000:2020 (not modified)

Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

## 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](http://www.cencenelec.eu).

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62443-4-1	2018	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements	EN IEC 62443-4-1	2018
IEC 62443-4-2	2019	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	EN IEC 62443-4-2	2019

Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)



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

Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

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

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references .....	8
3 Terms, definitions, abbreviated terms and acronyms .....	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms and acronyms .....	11
4 Overview .....	12
4.1 Component requirements.....	12
4.2 Clarification for CCSC (common component security constraints) .....	12
4.2.1 General .....	12
4.2.2 CCSC 1: Support of essential functions .....	12
4.2.3 CCSC 2: Compensating countermeasures .....	13
4.2.4 CCSC 3: Least privilege .....	13
4.2.5 CCSC 4: Software development process .....	14
4.3 Concept of the evaluation process .....	14
4.3.1 General .....	14
4.3.2 Step 1: Evaluation of security context, threat model and component requirements .....	14
4.3.3 Step 2: Evaluation of component artefacts .....	15
5 Evaluation process .....	15
5.1 Process overview.....	15
5.2 Evaluation requirements .....	16
5.2.1 General .....	16
5.2.2 Reference.....	16
5.2.3 Evaluation requirement ER-1 .....	16
5.2.4 Evaluation requirement ER-2 .....	17
5.2.5 Evaluation requirement ER-3 .....	17
5.3 Security context evaluation .....	17
5.3.1 Development lifecycle requirements .....	17
5.3.2 Security context and artefacts.....	17
5.4 Security requirement selection evaluation .....	19
5.4.1 General .....	19
5.4.2 Reference.....	19
5.4.3 Evaluation activity EA-10 .....	19
5.4.4 Evaluation activity EA-11 .....	19
5.5 Design documentation evaluation.....	19
5.5.1 Component design.....	19
5.5.2 Externally provided and custom developed components .....	20
5.6 Security guideline evaluation .....	20
5.6.1 General .....	20
5.6.2 Reference.....	21
5.6.3 Evaluation activity EA-16 .....	21
5.7 Component requirement evaluation.....	21
5.7.1 Component requirement verification existence .....	21
5.7.2 Component requirement verification results .....	22
5.7.3 Component requirement by testing .....	22

5.7.4	Component requirement verification completeness .....	23
5.8	Security testing evaluation .....	24
5.8.1	Security test reports .....	24
5.8.2	Independence of activities .....	24
5.8.3	Examination of test results.....	25
5.8.4	Vulnerability assessment metric.....	25
6	Evaluation criteria.....	27
6.1	Preliminary note.....	27
6.2	FR-1: Identification and authentication control .....	27
6.3	FR-2: Use control.....	34
6.4	FR-3: System integrity .....	39
6.5	FR-4: Data confidentiality.....	46
6.6	FR-5: Restricted data flow .....	47
6.7	FR-6: Timely response to events.....	49
6.8	FR-7: Resource availability .....	50
Annex A (normative)	Component specification .....	53
A.1	Preliminary note.....	53
A.2	Component description .....	53
A.3	Artefacts .....	53
A.4	Security guideline .....	54
A.5	Design documentation .....	54
Annex B (normative)	Evaluation report requirements .....	55
B.1	Preliminary note.....	55
B.2	Evaluation summary.....	55
B.3	Design documentation .....	55
B.4	Security guideline .....	55
B.5	Results of the component requirement verification .....	55
B.6	Vulnerability analysis .....	56
B.7	Overall assessment .....	56
Annex C (informative)	Use of artefacts in the evaluation process .....	57
Annex D (informative)	Examples .....	59
D.1	Artefacts for 3 <sup>rd</sup> -party and custom developed components .....	59
D.1.1	General .....	59
D.1.2	Custom developed components .....	59
D.1.3	Commercial off-the-shelf (COTS).....	59
D.1.4	Community-based Open Source (OSS).....	60
D.2	Evaluation criteria.....	60
Bibliography	.....	62
Figure 1	– Relationship between CCSCs and parts of the series or requirements .....	12
Figure 2	– Component security requirements selection evaluation (Step 1).....	14
Figure 3	– Component security artefacts evaluation (Step 2) .....	15
Figure 4	– Evaluation process.....	16
Figure D.1	– Community-based open-source software chain .....	60
Table 1	– Evaluation criteria for FR-1: Identification and authentication control.....	28
Table 2	– Evaluation criteria for FR-2: Use control .....	34

Table 3 – Evaluation criteria for FR-3: System integrity .....	39
Table 4 – Evaluation criteria for FR-4: Data confidentiality .....	46
Table 5 – Evaluation criteria for FR-5: Restricted data flow .....	47
Table 6 – Evaluation criteria for FR-6: Timely response to events .....	49
Table 7 – Evaluation criteria for FR-7: Resource availability .....	50
Table C.1 – Reuse of artefacts from IEC 62443-4-1 processes in the evaluation process .....	57
Table D.1 – Example evaluation criteria application .....	61

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

## 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](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are described in greater detail at [www.iec.ch/publications](http://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](http://webstore.iec.ch) in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

## 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 3<sup>rd</sup> 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.

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

# 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 cryptology**

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