



BSI Standards Publication

Security for industrial automation and control systems

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

National foreword

This Published Document is the UK implementation of IEC TS 62443-6-2:2025.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 17331 4

ICS 25.040.40

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 January 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

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

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 rd -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

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.

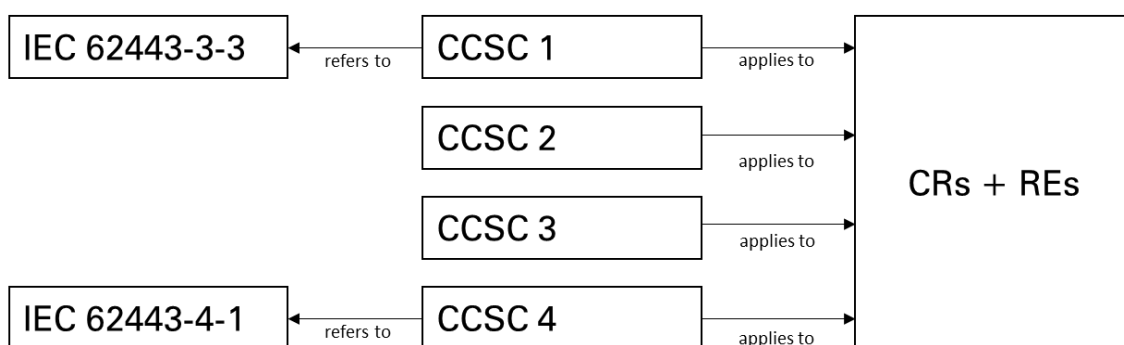


Figure 1 – Relationship between CCSCs and parts of the series or requirements

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.

When applicable the evaluation criteria include the least privilege principle for the specific CRs and REs.

NOTE The fulfilment of CCSC 3 is evaluated as part of "requirement verification results" in 5.7.2.

4.2.5 CCSC 4: Software development process

All of the components defined in this document shall be developed and supported following the secure product development processes described in IEC 62443-4-1.
(Source: IEC 62443-4-2:2019, 4.5)

Clarification

NOTE The following clarification is formally defined as evaluation requirement ER-2 in 5.2.

The secure product development process for the component under evaluation is expected to have at least reached maturity level ML-3 for all IEC 62443-4-1 requirements, i.e. the secure product development was applied for the component under evaluation and the required artefacts are available for review, as needed, during the evaluation.

This requirement applies to the development of hardware, software and firmware.

Artefacts related to IEC 62443-4-1 SUM requirements might not be available if a newly developed component is evaluated. For this case the requirements are not applicable.

4.3 Concept of the evaluation process

4.3.1 General

The concept of the evaluation process for the component under evaluation is mainly based on the clarification of CCSC 4. The evaluation process itself is defined in Clause 5.

4.3.2 Step 1: Evaluation of security context, threat model and component requirements

In support of CCSC 4, a documented security context (SR-1) and a documented threat model (SR-2) for the component under evaluation are expected. The described security context (see 5.3.2) and the specified threat model determine a sound foundation for the selected security requirements (CRs and REs, see 5.4). The relationship between SR-1 to SR-4 and the component under evaluation is shown in Figure 2.

For the component under evaluation the selected CRs are an important input to the subsequent evaluation process.

NOTE IEC 62443 cyber security profiles (according to IEC 62443-1-5) allow e.g. the selection of requirements (CR) from IEC 62443-4-2.

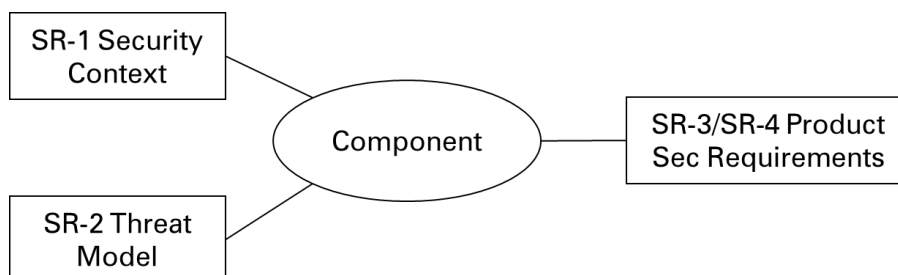


Figure 2 – Component security requirements selection evaluation (Step 1)

The component security requirements selection evaluation corresponds to Step 1 in the evaluation process defined in 5.1.

4.3.3 Step 2: Evaluation of component artefacts

In support of CCSC 4 additional artefacts (e.g. test results, security test reports) are expected and used as evidence during the evaluation process. The evaluation of component artefacts corresponds to step 2 in the process defined in Clause 5. The explicit reference to the IEC 62443-4-1 requirements is given in subclauses 5.3 to 5.8 as referenced requirements. The component security artefacts which are evaluated in step 2 of the evaluation are shown in Figure 3.

NOTE An overview of all referenced requirements is given in Annex C.

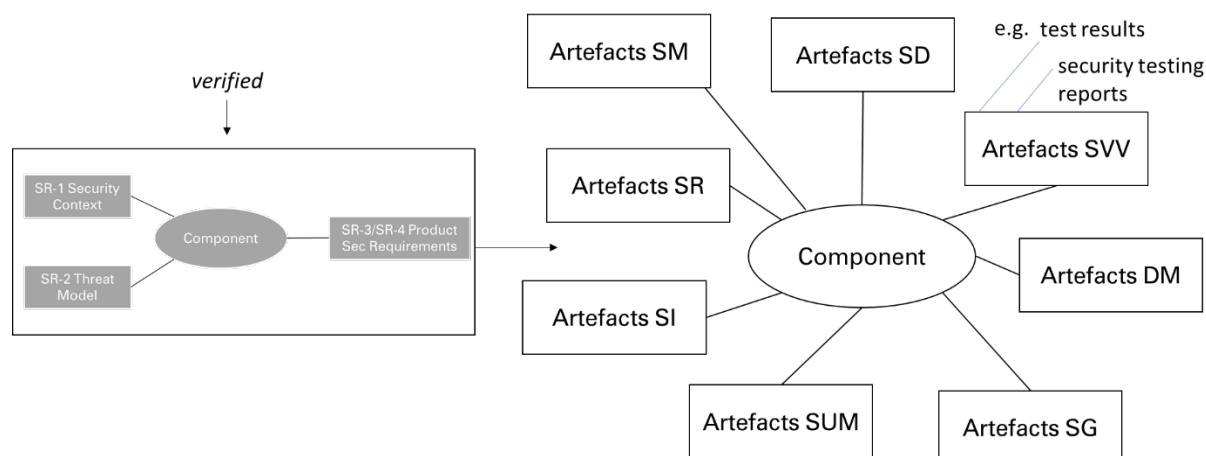


Figure 3 – Component security artefacts evaluation (Step 2)

5 Evaluation process

5.1 Process overview

The evaluation process is a sequence of mandatory evaluation activities. The evaluation activities should be applied in the given order. The activities form the basis for the evaluation process and support its consistency. The evaluation process is performed by the evaluator. An alternative sequence can result in an inconclusive or inconsistent evaluation result.

The evaluation activities specified in this document are based on two principles:

- 1) Evaluation of the requirements specified in IEC 62443-4-2 (i.e. CRs and REs) that are implemented in and provided by the component under evaluation;
- 2) Evaluation of the security development process applied to the requirements in 1) according to the requirements specified in IEC 62443-4-1 (see IEC 62443-4-2, CCSC 4).

For each requirement that the evaluator examines, the evaluator obtains evidence from the product supplier (i.e. the artefacts) to determine if the product meets that requirement.

If any evaluation activity is inconclusive, the evaluation process is not complete or could only be completed as failed.

The evaluation process and its evaluation activities are grouped into two steps (see Figure 4):

- Step 1: Evaluation of security context, threat model and component requirements (see 4.3.2), and evaluation of the sound foundation up to the selection of the CRs and the SL of each requirement;
- Step 2: Evaluation of component artefacts (see 4.3.3) which give an indication how the security capability was designed, implemented, documented and tested. The artefacts can be used to determine whether requirements by IEC 62443-4-1 are met.

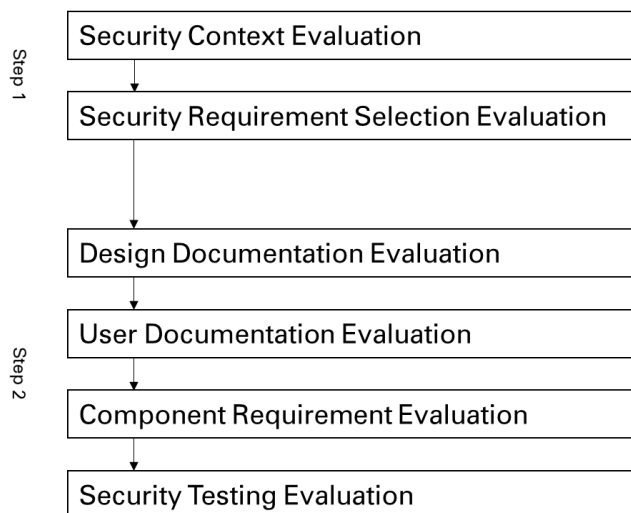


Figure 4 – Evaluation process

NOTE IEC 62443-4-2 has some requirements where 'internationally recognized and proven security practices and recommendations' are required to be adhered to when implementing a security capability. Since related security best practices and technologies are constantly changing, it is important that personnel performing evaluation activities are well versed in this topic.

The results of the evaluation process should be reported. The content of the evaluation report is given in Annex B.

5.2 Evaluation requirements

5.2.1 General

This document does not introduce additional technical and process requirements compared to those in IEC 62443-4-2 and IEC 62443-4-1. Only clarifications for CCSC according to 4.2 which have a significant impact on the evaluation process lead to formally defined evaluation requirements.

5.2.2 Reference

Referenced clarifications:

- CCSC 2: Compensating countermeasures
- CCSC 4: Software development process

NOTE For a general overview of referenced requirements from IEC 62443-4-1 in Clause 5 see Annex C.

5.2.3 Evaluation requirement ER-1

The evaluator shall check for each applicable component requirement (CR) and requirement enhancements (RE) if the requirement is met by the component itself, met by system integration, or either option, based on a product supplier specification.

5.2.4 Evaluation requirement ER-2

The evaluator shall check that the product supplier provided artefacts to prove that the component under evaluation was developed according to an IEC 62443-4-1 with a maturity level of at minimum ML-3 for all requirements, i.e. the product supplier is able to demonstrate that related evidence exists.

5.2.5 Evaluation requirement ER-3

The evaluator shall perform all evaluation activities.

5.3 Security context evaluation

5.3.1 Development lifecycle requirements

5.3.1.1 General

The component under evaluation is implemented based on the full product development lifecycle requirements as required by IEC 62443-4-1.

NOTE A security evaluation methodology for IEC 62443-4-1 itself is outside the scope of this document. Annex C provides an overview for which security practices of IEC 62443-4-1 artefacts are reused within this evaluation methodology for IEC 62443-4-2.

5.3.1.2 Reference

Referenced requirements:

- CCSC 4: Software development process
- SM-3: Identification of applicability
- SM-5: Process scoping
- SM-12: Process verification
- SR-1: Product security context
- SR-2: Threat model

5.3.1.3 Evaluation activity EA-1

The evaluator shall check if secure product development processes as described in accordance with IEC 62443-4-1 were applied to the component under evaluation.

5.3.1.4 Evaluation activity EA-2

The evaluator shall examine the relevant artefacts as required by the IEC 62443-4-1 practices.

5.3.2 Security context and artefacts

5.3.2.1 General

The product security context includes a description of minimum requirements and assumptions about the environment. A specific format for this description is not defined by IEC 62443-4-1. The contents of the description, however, are required for an effective evaluation, e.g. a security context needs to be defined and a threat model needs to be completed for the component under evaluation.

The information needs to be provided in the form of a descriptive document or based on one or more artefacts. The content of the component specification is given in Annex A. The component specification can be used as a structure for the descriptive document or as a checklist for artefacts.

5.3.2.2 Reference

Referenced requirements:

- CCSC 1: Support of essential functions
- CCSC 2: Compensating countermeasures
- CCSC 4: Software development process
- SR-1: Product security context
- SR-2: Threat model
- SR-4: Product security requirements content

5.3.2.3 Evaluation activity EA-3

The evaluator shall check if the provided artefacts include all the information from Annex A in this document.

5.3.2.4 Evaluation activity EA-4

The evaluator shall check if a threat model is available and if the threat model provides the content defined in SR-2.

5.3.2.5 Evaluation activity EA-5

The evaluator shall examine if the provided artefacts describe system essential functions and related specific constraints implemented on the component under evaluation.

NOTE 1 For system essential functions, see 4.2.2.

NOTE 2 A list of common constraints is given in IEC 62443-3-3:2013, 4.2.

5.3.2.6 Evaluation activity EA-6

If constraints according to EA-5 exist, the evaluator shall examine that those have been considered in the risk assessment and that the component under evaluation does not adversely affect these system or component essential functions.

5.3.2.7 Evaluation activity EA-7

The evaluator shall examine if the provided documents specify which security capabilities external to the component are identified to be implemented as compensating countermeasures.

NOTE Each security capability is implemented as a built-in security capability or by a compensating countermeasure, see 4.2.3.

5.3.2.8 Evaluation activity EA-8

The evaluator shall examine that the description of the compensating countermeasures is accurate.

5.3.2.9 Evaluation activity EA-9

The evaluator shall examine if the security context, the threat model and the selected component requirements are aligned.