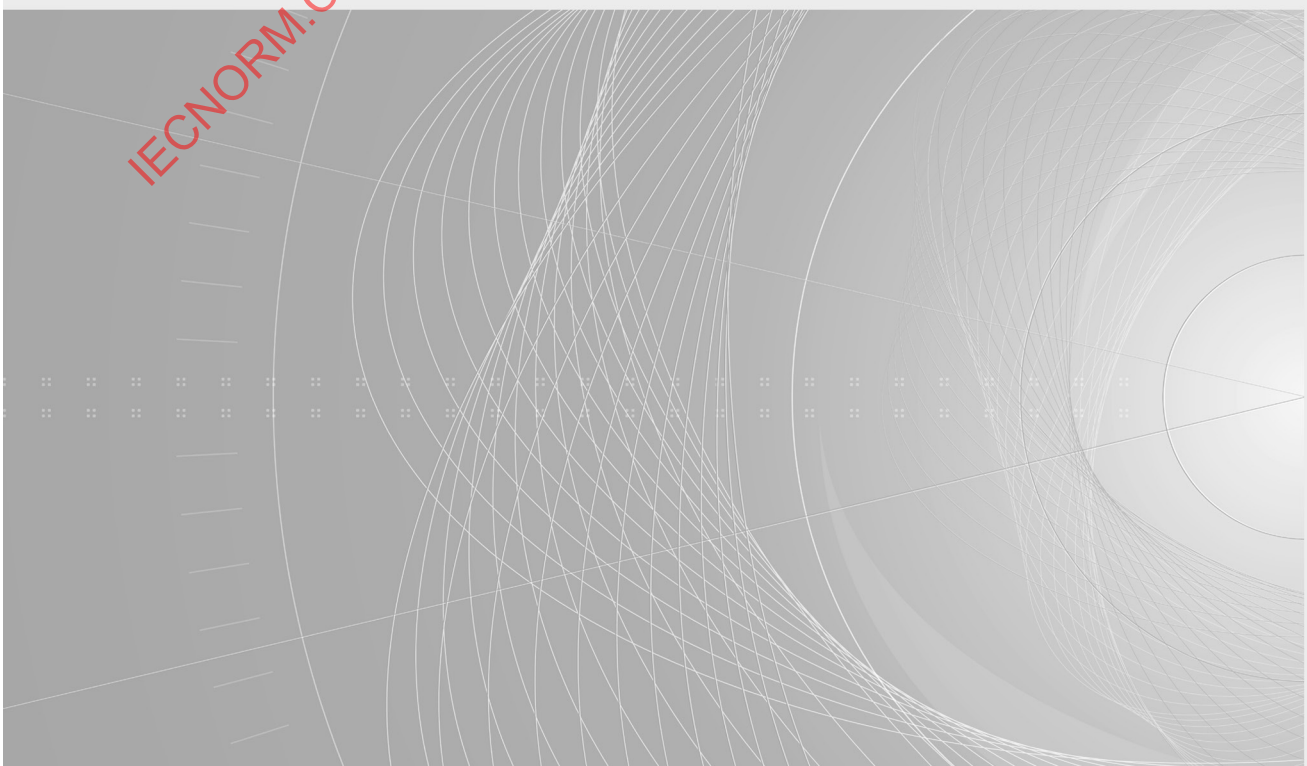
IEC TS 62443-6-2

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 It also gives information on projects, replaced and withdrawn publications.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.

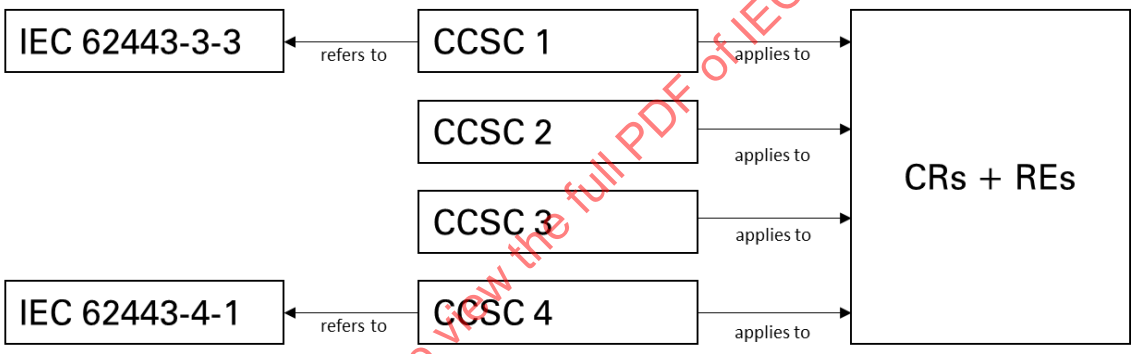


Figure 1 – Relationship between CCSCs and parts of the series or requirements

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.

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.

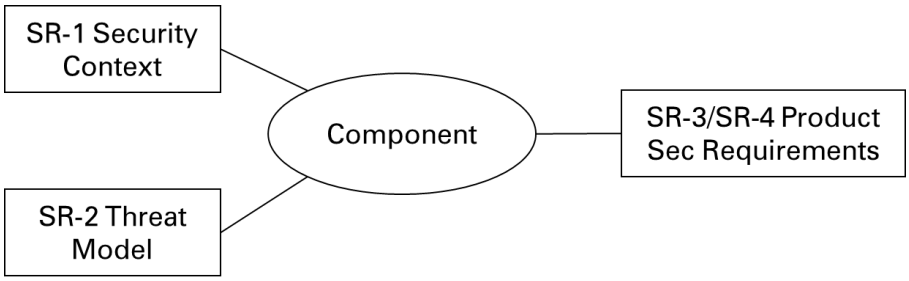


Figure 2 – Component security requirements selection evaluation (Step 1)

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.

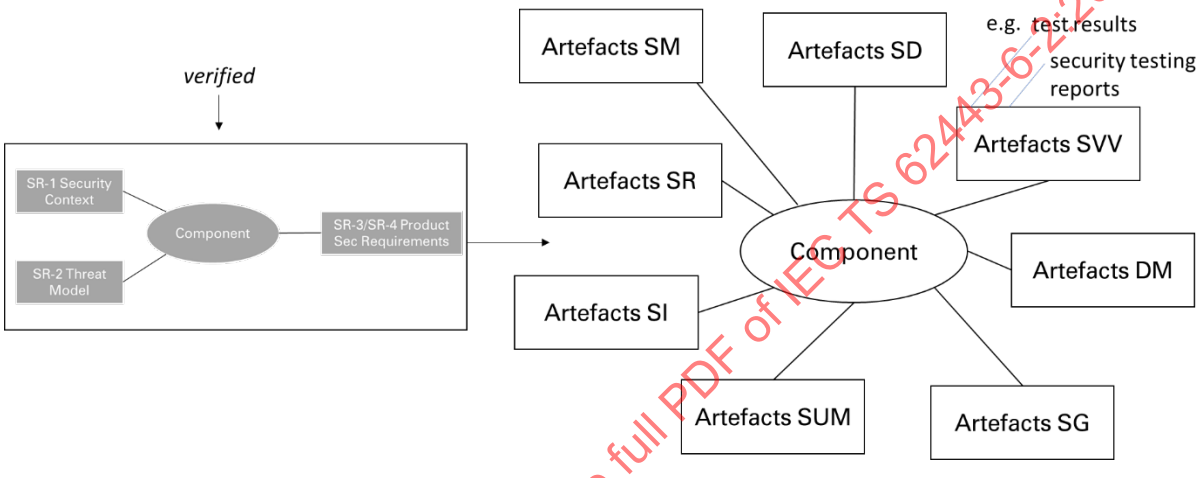


Figure 3 – Component security artefacts evaluation (Step 2)

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.

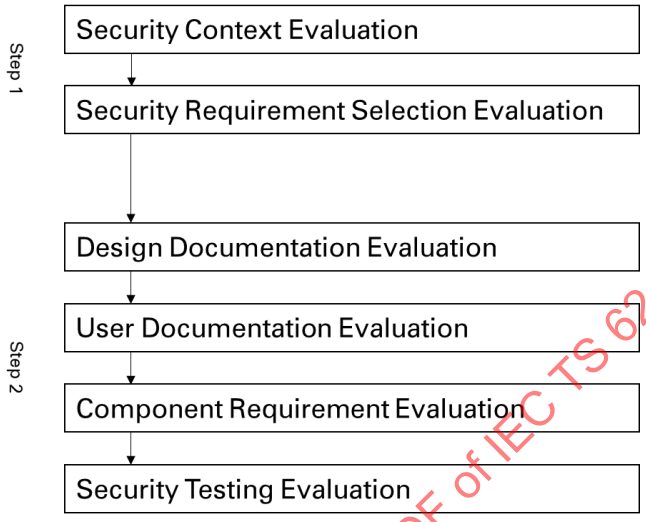


Figure 4 – Evaluation process

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.

5.4 Security requirement selection evaluation

5.4.1 General

This methodology assumes a set of component requirements (CR) and requirement enhancements (RE) are selected by the product supplier. These are referred to as the selected security requirements. Additionally, the product supplier needs to follow the process defined in its own product development process. This step is used to examine if the internal process was followed.

The selected requirements shall be consistent with the threat model and the documented security context.

5.4.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SR-2: Threat model
– SR-3: Product security requirements
– SR-4: Product security requirements content
– SM-5: Process scoping

5.4.3 Evaluation activity EA-10

The evaluator shall examine if the selected component requirements were selected as defined in the product supplier's development process.

5.4.4 Evaluation activity EA-11

The evaluator shall examine that the component requirements which are not in scope of the evaluation have a sound rationale for exclusion.

NOTE This requirement refers to both a) component requirements which are technically not applicable for the component, and b) component requirements outside the requirements selection outlined in 5.4.1.

5.5 Design documentation evaluation

5.5.1 Component design

5.5.1.1 General

For each component requirement the evaluator examines provided artefacts how the requirements are fulfilled. Additionally, artefacts need to be referenced to support the statement of conformity.

5.5.1.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SR-2: Threat model
– SD-1: Secure design principles
– SD-2: Defense in depth design
– SD-3: Security design review
– SD-4: Secure design best practices

5.5.1.3 Evaluation activity EA-12

The evaluator shall examine that the provided threat model addresses all interfaces and the component's secure design.

5.5.1.4 Evaluation activity EA-13

The evaluator shall check the artefacts and verify if these contain all the required design documentation.

NOTE Clause A.5 specifies the content of the required design documentation.

5.5.1.5 Evaluation activity EA-14

The evaluator shall examine the consistency of the component's artefacts to the defense in depth design and the threat model.

5.5.2 Externally provided and custom developed components

5.5.2.1 General

Component development often utilizes externally developed sub-components which might not be able to follow the requirements from the development process.

5.5.2.2 Reference

Referenced requirements:

– SM-9: Security requirements for externally provided components
– SM-10: Custom development components from 3rd -party suppliers
– SD-1: Secure design principles
– SD-2: Defense in depth design

5.5.2.3 Evaluation activity EA-15

The evaluator shall examine if externally provided and custom developed components from 3rd -party components fulfill the requirements from SM-9 or SM-10 and the relevant artefacts are available.

NOTE Clause D.1 includes guidelines for the required content.

5.6 Security guideline evaluation

5.6.1 General

The security guideline for the component under evaluation is based on required content specified in IEC 62443-4-1:2018, 12.2 (SG-1) to 12.6 (SG-6).

5.6.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SUM-2: Security update documentation
– SUM-3: Dependent component or operating system security update documentation
– SG-1: Product defense-in-depth
– SG-2: Defense-in-depth measures expected in the environment
– SG-3: Security hardening guidelines
– SG-4: Secure disposal guidelines
– SG-5: Secure operation guidelines
– SG-6: Account management guidelines

5.6.3 Evaluation activity EA-16

The evaluator shall examine whether the information provided in the security guideline is complete and consistent. In particular the security guideline shall be consistent with the security context and the assumptions about the environment. The security guideline shall be complete, i.e. include the content required in IEC 62443-4-1 Practice 8 (security guidelines).

5.7 Component requirement evaluation

5.7.1 Component requirement verification existence

5.7.1.1 General

Security requirements are documented for the security capabilities related to installation, operation, maintenance and decommissioning. The component requirements (CR) from IEC 62443-4-2 are, in part, already specifically defined, in other parts described in a technology-independent manner. The fulfilment of the requirements for the component under evaluation needs to be verified. The verification can be conducted by either test documentation review or design documentation review.

NOTE Component requirements (CRs as defined in IEC 62443-4-2) could be part of the full set of security requirements for a component. Requirements not defined in IEC 62443-4-2 are out of scope of the component evaluation process and not considered during the evaluation process. The evaluation process can be facilitated with requirement mappings to the CRs from IEC 62443-4-2.

The component requirements for the component under evaluation need to be associated with a component requirement verification, e.g. by a test case or other verification activity.

5.7.1.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SR-3: Product security requirements
– SVV-1: Security requirements testing
– SD-1: Secure design principles
– SD-2: Defense in depth design
– all CRs and REs

5.7.1.3 Evaluation activity EA-17

The evaluator shall check if for each applicable component requirement, a component requirement verification was performed.

5.7.2 Component requirement verification results

5.7.2.1 General

In Clause 6 of this document, acceptance criteria are specified for all component requirements given in IEC 62443-4-2 to support evaluators during the evaluation activities.

The component requirements have to be verified by appropriate and traceable means, e.g. by the definition of test cases. In some cases, because requirements could pertain to more than one interface or component function, several tests will be necessary.

The model for linking CRs to requirement verification (e.g. test cases) is composed in the following order:

1) Requirements of the standard parts (CR and RE from IEC 62443-4-2, sorted by FR)
2) Evaluation criteria (given in this document, Clause 6)
3) Requirement verification, e.g. test cases (component-specific, not defined in this document)

For an example on how to apply the evaluation criteria for a test case, see Clause 6.

5.7.2.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SR-3: Product security requirements
– SVV-1: Security requirements testing
– all CRs and REs

5.7.2.3 Evaluation activity EA-18

The evaluator shall examine the results of the requirement verification, using the related acceptance criteria defined in Clause 6. The examination shall verify traceability of requirements to design and tests.

5.7.2.4 Evaluation activity EA-19

The evaluator shall check if all applicable component requirements are met by component or met by system integration.

5.7.3 Component requirement by testing

5.7.3.1 General

If security testing (as defined in SVV-1) is used for component requirement verification the following applies.

Testing is an expected and accepted method for requirements verification, see SVV-1 Security requirements testing. For defining test cases, at least the following test characteristics have to be met:

- test description with test expectation, test preparation, and testing steps;
- test result;
- evaluation (pass or fail).

The test expectation is the expected test result, which will occur if the component functions correctly. The test expectation results from the component's intended behavior and the evaluation criteria. The test result is the actually detected behavior of the component during the testing steps.

The choice of technical implementation needs to be appropriate for the chosen security level. The choice of technical implementation is shown in the design documentation, see 5.5 documentation (design).

During testing, it needs to be examined whether the chosen technical implementation has been performed correctly to verify that the component meets the respective IEC 62443-4-2 component requirements. The test description needs to reflect details of the technical implementation adequately.

If the test result corresponds with the test expectation, the evaluation will be positive (pass). If the test result deviates, the evaluation will be negative (fail).

5.7.3.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SR-3: Product security requirements
– SVV-1: Security requirements testing
– SVV-5: Independence of testers
– all CRs and REs

5.7.3.3 Evaluation activity EA-20

The evaluator shall check if all test documentation meets the given test characteristics.

5.7.3.4 Evaluation activity EA-21

The evaluator shall check the test results to confirm all tests passed and shall provide a description why evaluated tests failed.

5.7.4 Component requirement verification completeness

5.7.4.1 General

If no test case was specified for a specific CR, e.g. if one interface is not testable via an external interface, an alternative verification has to be given.

An evaluation of the pertaining design documentation focusing on the respective CR and regarding the evaluation criteria is an alternative validation method. The evaluator is asked to give a well-founded opinion on the fulfilment with the evaluation criteria.

5.7.4.2 Reference

Referenced requirement:

– CCSC 4: Software development process
– SR-3: Product security requirements
– SR-5: Security requirements review
– SD-1: Secure design principles
– SD-2: Defense in depth design

5.7.4.3 Evaluation activity EA-22

The evaluator shall examine all requirement verification results for requirements that are not testable for whether the component requirements are sufficiently fulfilled by the product supplier evidence.

5.8 Security testing evaluation

5.8.1 Security test reports

5.8.1.1 General

Security testing is the term used for a broad set of activities required in the component development process to discover security vulnerabilities, i.e. threat mitigation testing, vulnerability testing and penetration testing. Security testing is performed at the component level including all parts and functionality of the component.

Security testing should consider the product security context. Before testing starts the guidelines for hardening the product (according IEC 62443-4-1 SG-3) should be applied appropriately.

The results of security testing are documented in test reports. The format of these test reports is not mandated but clear references to the software development process requirements are recommended.

Penetration testing reports are sometimes confidential. If these reports are not available to the evaluator a summary of the results shall be provided to the evaluator.

5.8.1.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SI-1: Security implementation review
– SVV-1: Security requirements testing
– SVV-2: Threat mitigation testing
– SVV-3: Vulnerability testing
– SVV-4: Penetration testing

5.8.1.3 Evaluation activity EA-23

The evaluator shall examine the security testing reports for the component under evaluation for completeness.

5.8.2 Independence of activities

5.8.2.1 General

The security testing is expected to adhere to the necessary independence as defined in IEC 62443-4-1:2018, SVV-5, Table 3 "Required level independence of testers from developers".

5.8.2.2 Reference

Referenced requirement:

– CCSC 4: Software development process
– SVV-5: Independence of testers

5.8.2.3 Evaluation activity EA-24

The evaluator shall check if the security testing meets the required independence of testers.

5.8.3 Examination of test results

5.8.3.1 General

The primary aim of security testing is the identification of security vulnerabilities and fulfillment of security requirements. For example, vulnerability testing has to consider the following types of vulnerabilities:

– vulnerabilities in 3rd-party software;
– vulnerabilities in the operating system;
– hardware vulnerabilities;
– lack of integrity or authenticity of firmware;
– missing integrity assurance for data exports;
– shared static credentials located in software;
– weak protection of data in transit or data at rest.

The aim of the vulnerability testing is to identify publicly known and unknown security vulnerabilities in the component under evaluation.

The security testing of attack vectors has to be performed with the help of the available design documentation especially the defense in depth design.

5.8.3.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SM-11: Assessing and addressing security-related issues
– SD-2: Defense in depth design
– SI-1: Security implementation review
– SVV-2: Threat mitigation testing
– SVV-3: Vulnerability testing
– SVV-4: Penetration testing

5.8.3.3 Evaluation activity EA-25

The evaluator shall examine that all the security requirements have been met as given in the referenced requirements (i.e. IEC 62443-4-1 SI-1, SVV-1, SVV-2, SVV-3 and SVV-4).

5.8.4 Vulnerability assessment metric

5.8.4.1 General

Security testing can lead to a list of discovered vulnerabilities. A discovered vulnerability can be exploitable (i.e. the attack can be executed directly) or can be described in principle (e.g. weak cryptographic algorithm with a related attack path).

These discovered security vulnerabilities have to be rated with a consistent scoring metric which is called vulnerability assessment metric in this document.

The present evaluation methodology does not predefine a specific vulnerability assessment metric. The vulnerability assessment metric needs to be defined as part of the software development process. Typically, the security context of the component under evaluation is an environmental parameter in such a vulnerability assessment metric.

NOTE 1 An example of a standardized metric is the CVSS (common vulnerability scoring system). An example of a standardized vulnerability assessment method is the CEM-AVA-Method defined in Common Criteria, see CEM and ISO 18045.

For the component under evaluation a vulnerability assessment metric has to be defined. As part of this metric corresponding thresholds are specified according to the security context.

The discovered vulnerabilities, for which the estimated value in the metric is above this threshold, are expected to be mitigated. The vulnerabilities, for which the estimated value is below this threshold, are recommended to be analyzed and mitigated or accepted.

NOTE 2 When automated tools (e.g. known vulnerability scanning tools, web server vulnerability assessment tools) are used for vulnerability testing, false positive results will be identified in many cases. Results identified as false positives need a further investigation of the issue.

5.8.4.2 Reference

Referenced requirements:

– CCSC 4: Software development process
– SM-11: Assessing and addressing security-related issues
– SR-2: Threat model
– SR-4: Product security requirements content
– DM-3: Assessing security-related issues
– DM-4: Addressing security-related issues
– SI-1: Security implementation review
– SVV-2: Threat mitigation testing
– SVV-3: Vulnerability testing
– SVV-4: Penetration testing

5.8.4.3 Evaluation activity EA-26

The evaluator shall check if a vulnerability assessment metric was chosen and is adequately described.

NOTE This vulnerability assessment metric can be a simple qualitative rating (for example, low, medium and high), or a more quantitative method based on likelihood and consequence, or a standardized method such as the CVSS.

5.8.4.4 Evaluation activity EA-27

The evaluator shall examine if the selected vulnerability assessment metric is industry-recognized and based on a commonly recognized methodology.

5.8.4.5 Evaluation activity EA-28

The evaluator shall check if a vulnerability assessment metric was specified and applied.

5.8.4.6 Evaluation activity EA-29

The evaluator shall examine if all publicly known vulnerabilities as identifiable by vulnerability testing (i.e. IEC 62443-4-1 SVV-3) were detected and addressed during the security testing for the component under evaluation.

5.8.4.7 Evaluation activity EA-30

The evaluator shall examine if all discovered vulnerabilities during the security testing were assessed and addressed for the component under evaluation.

NOTE The terms assessing and addressing is used as in IEC 62443-4-1 SM-11.

5.8.4.8 Evaluation activity EA-31

The evaluator shall examine if the security testing reports take the vulnerability assessment metric into account.

5.8.4.9 Evaluation activity EA-32

The evaluator shall examine that all security-related issues in the component under evaluation which are higher than the threshold for the required SL-C have been addressed and tracked to closure. Additionally, all security-related issues in the component under evaluation which are below the threshold have been addressed and the corresponding action is tracked to closure.

NOTE 1 Publicly known vulnerabilities and security-related issues refer to all known security-related issues at the time the component is being tested.

NOTE 2 The threshold is expected to express the acceptable residual risk within the product security context as specified in IEC 62443-4-1 SM-11.

NOTE 3 Acceptable options for "tracked to closure" are given in IEC 62443-4-1 DM-4.

6 Evaluation criteria

6.1 Preliminary note

In the following the evaluation criteria for the component requirements are defined. These criteria are used in the evaluation step component requirement verification, see 5.7.

The evaluation criteria are normative and clarify the component requirements verification to ensure these are verifiable. The first two columns (ID and Requirement Title) in the tables in 6.2 to 6.8 are taken from IEC 62443-4-2.

The evaluation criteria are primarily formulated in positive terms to describe what is acceptable. Criteria marked by "not sufficient" are an explicit exclusion of an implementation. Conditions are marked by "applicable" or "not applicable".

The requirements in the table shall be interpreted based on the interpretation of security level in the product supplier's development process.

Clause D.2 gives an example on how evaluation criteria are applied.

6.2 FR-1: Identification and authentication control

Table 1 shows the FR-1: Identification and authentication control.

Table 1 – Evaluation criteria for FR-1: Identification and authentication control

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 1.1	Human user identification and authentication	- The component implements an identification and authentication mechanism of human users on each accessible interface, or - the component is capable to integrate into a system-level authentication Examples: identifier and password-based authentication, pre-shared key, or USB token, shared account Not sufficient: - only static authenticator, e.g. hard-coded password	Additional to SL-1: RE (1) - The component requires unique authentication of human users on each accessible interface. Examples: unique identifiers and password-based authentication for each human user, or PKI-based certificate for each human user stored in a smartcard Not sufficient: - The component implements only one identity.	Additional to SL-2: RE (2) - The component requires unique authentication of human users on each accessible interface using a multi-factor authentication mechanism. Examples: - physical token with PIN, or - certificate with password, or - biometric identification with passphrase Not sufficient: - The component implements only a single authentication mechanism. - The two factors depend on each other.	No additional requirements in addition to those of SL-3
CR 1.2	Software process and device identification and authentication	No requirements	- The component identifies itself, and authenticates to any other component, and - authentication mechanism is capable to prevent attacks like man-in-the-middle or message spoofing. Examples: certification-based authentication, challenge and response mechanisms, tokens (e.g. password, location) Essential functions: - identification and authorization do not prevent the initiation of a safety function unless supported by a risk assessment Not sufficient: - unprotected authentication and identification	Additional to SL-2: RE (1) - uniquely identify and authenticate itself to any other component	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 1.3	Account management	Not applicable if only a single fixed administrative account is implemented on the component. - capability to integrate into a higher-level account management system, or - account management capability (only by authorized users, including adding, activating, modifying, disabling and removing accounts) Essential functions: - component is not affected by an availability problem of the higher-level system - accounts used for essential functions shall not be locked out, even temporarily (see IEC 62443-3-3, 4.2) Examples for higher level account management: component connected to LDAP, Active Directory, or host (e.g. operator workstation) Not sufficient: - no capability to enable/disable accounts	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 1.4	Identifier management	- capability to integrate into a system that supports management of identifiers, or - provide the capability to support the management of identifiers by user, group, role or control system interface Essential functions: - accounts used for essential functions shall not be locked out, even temporarily (see IEC 62443-3-3:2013, 4.2) Examples: account names, UNIX user IDs, Microsoft Windows account globally unique identifiers (GUID), X.509 certificates	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 1.5	Authenticator management	- Support of (initial) authenticator content, and - enforced change of default authenticators after installation, or recognition of unchanged default authenticator (combined with warning message), and - periodic change of authenticators, and - protection of unauthorized disclosure or modification of authenticators (when stored, used, transmitted) Examples: tokens, symmetric keys, private keys, biometrics, passwords, key cards Not sufficient: - plain text authenticators at rest - cached authenticators without limited lifetime - static identifier or authenticator, e.g. hard-coded password	No additional requirements in addition to those of SL-1	Additional to SL-2: RE (1) - authenticators are protected via hardware mechanisms Not sufficient: - no hardware protection mechanism NOTE For hardware-based protection also refer to the requirement CR 1.9 RE(1) or CR 1.14 RE(1).	No additional requirements in addition to those of SL-3
CR 1.6	Wireless access management	Applicable for network device Not applicable if the component does not have a wireless interface. - capability to identify and authenticate all users (human, software processes and devices) engaged in wireless communication Examples: WiFi password authentication, wireless LAN (802.11) with 802.1X, WirelessHART with configured join keys, Bluetooth with pairing	Additional to SL-1: RE (1) - capability to uniquely identify and authenticate all users (human, software processes and devices) engaged in wireless communication Example: Wireless LAN (802.11) with 802.1X EAP TLS, WirelessHART with configured unique join keys, eUICC-based authentication, Bluetooth with out of band (OOB) pairing	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 1.7	Strength of password-based authentication	IF cryptography means are used then CR 4.3 shall be applicable. - enforce configurable password strength based on minimum length and variety of character types, and - configurable password strength according to internationally recognized and proven password guidelines, and - system providing strong and configurable external authentication (by integration into a system)	No additional requirements in addition to those of SL-1	Additional to SL-2: RE (1) - prevent any human user account from reusing a password for a configurable number of generations - enforce password minimum and maximum lifetime restrictions for human users - external authentication Not sufficient: - no configurable options for reusing passwords, i.e. password reuse cannot be prevented - no minimum and maximum lifetime restrictions for human user passwords	Additional to SL-3: RE (2) - Enforce password minimum and maximum lifetime restrictions for all users (human, software process, or device) Not sufficient: - no minimum and maximum lifetime restrictions for all users.
CR 1.8	Public key infrastructure certificates	No requirements	Applicable if PKI is in use. - interaction and operation within the scope of the PKI according to 62443-3-3 SR 1.8 ("operate a PKI according to commonly accepted best practices (see IETF RFC 3647) or obtain a public key certificate from an existing PKI") Essential functions: - certificate verification mechanisms do not interrupt essential functions Examples: - X.509-based PKI	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 1.9	Strength of public key authentication	No requirements	Applicable if PKI or public keys are in use. If applicable then CR 4.3 shall be applied, too. Additional to SL-1 - provide directly or integrate into a system that provides, the capability to: - validating signature of a given certificate - validate certificate chain - in case of self-signed certificates, leaf certificates should be deployed to all hosts that communicate with the subject to which the certificate is issued - validate certification revocations status - establish user (software, human or device) control of the corresponding private key - map authenticated identity to a user by checking either the subject name, common name or distinguished name against the destination	Additional to SL-2: RE (1) - protect the relevant private keys via hardware protection mechanism Examples: Trusted Platform Module (TPM), Secure Elements, Hardware Security Module (HSM) conform to FIPS PUB 140-2 / ISO/IEC 19790 Not sufficient: - no additional hardware protection mechanism	No additional requirements in addition to those of SL-3
CR 1.10	Authenticator feedback	- Sensitive data concerning the authentication process is obscured Not sufficient: - feedback distinguishes between wrong password and wrong username - displays password, wireless key, token as plain text instead of asterisks or other symbol	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 1.11	Unsuccessful login attempts	- Capability to enforce, for each user type (human, software, device), a configurable limit of consecutive invalid access attempts performed in a configurable time period, and - capability to deny access for a specified period of time or until unlocked, when limit reached Essential functions: - accounts used for essential functions shall not be locked out, even temporarily (see IEC 62443-3-3:2013, 4.2)	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 1.12	System use notification	- Capability to display a system use notification message before authenticating to the local user interface, and - capability as an authorized user to configure the message	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 1.13	Access via untrusted networks	Applicable for network device Applicable if the security product context allows the component to be used for the connection between different zones. - monitor and control all methods of access to the network device via untrusted networks (dial-up, office network, remote access) Not sufficient: - access to the network device cannot be monitored / controlled - untrusted network is missing in monitoring or cannot be Examples: ACL-based layer 3 firewall capability	No additional requirements in addition to those of SL-1	Additional to SL-2: RE (1) - deny access requests via untrusted networks unless approved by an assigned role - for each connection a device-internal or external physical key is used to authorize the connection Examples: Deny by default, system administrator is expected to define specific rules and to approve request attempts (on-demand).	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 1.14	Strength of symmetric key-based authentication	No requirements	Applicable if symmetric key authentication (e.g. pre-shared-secrets) is used. CR 4.3 shall be applicable. - validate shared secret to establish the mutual trust, and - authentication is valid as long as shared secret remains a secret, i.e. secrets are stored securely, and - restrict access to the shared secret Examples: AES algorithm, challenge response mechanism, key derivation function	Additional to SL-2: RE (1) - control system provides the capability to protect the relevant shared keys via hardware mechanisms Examples: Trusted Platform Module (TPM), Secure Elements, Hardware Security Module (HSM) conform to FIPS PUB 140-2 / ISO/IEC 19790	No additional requirements in addition to those of SL-3

6.3 FR-2: Use control

Table 2 shows the FR-2: Use control.

Table 2 – Evaluation criteria for FR-2: Use control

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 2.1	Authorization enforcement	- Authorization mechanism is enforced on all interfaces which can be accessed by human users based on their responsibilities, as dictated by the least privilege principle, and - least privilege can be applied for the authorization enforcement mechanism Essential functions - authorization enforcement do not prevent the initiation of a safety function unless supported by a risk assessment Not sufficient: - interface without authorization mechanism (e.g. HMI, web interface, console)	Additional to SL-1: RE (1) + RE (2) - authorization mechanism on all interfaces which are exposed, independent of user type (additionally technical users) - management of roles and permissions (definition and modification, only by privileged role) - management of users mapped to roles Examples: - a component with at least two roles configured	Additional to SL-2: RE (3) - capability to configure a time or sequence of events during supervisor override without closing the current session Not sufficient: - no possibility to configure supervisor override	Additional to SL-3: RE (4) - dual approval is provided by an interface of the component Not sufficient: - dual approval can be skipped by the user of the component

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 2.2	Wireless use control	- capability to deny critical action via wireless connection (i.e. only use wired), and - monitor devices	No additional requirements	No additional requirements	No additional requirements
CR 2.3	Use control for portable and mobile devices	No requirements	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 2.4	Mobile code	Applicable if components allow to execute mobile code. - capability to enforce a security policy for the usage of mobile code, and - control execution of mobile code, and - define which users are allowed to transfer mobile code to/from device, and - only upload to device, and - perform integrity checks on the code prior to code execution, and - perform integrity checks to verify origin prior to code execution	Additional to SL-1: RE (1) - provides the capability to verify the authenticity of the mobile code before execution is allowed Not sufficient: - execution is allowed without verifying the authenticity of the mobile code	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 2.5	Session lock	For any human user interface (local or via network): - Session Lock after configurable time period of inactivity, or - option to explicitly disable Session Lock (e.g. in control room scenarios), or - manual session lock, or - access to session only possible using authentication procedures, or - comply with session locks requested by the underlying infrastructure (operating system, control system) Essential functions: - Session lock do not prevent the initiation of a safety function unless supported by a risk assessment - accounts used for essential functions shall not be locked out, even temporarily (see IEC 62443-3-3:2013, 4.2)	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 2.6	Remote session termination	No requirements	Remote session is interpreted as logical network session. - remote session terminated by user who initiated session (minimum requirement), or - remote session manually terminated by a local authority/user, or - remote session terminated after configurable inactive period of time	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 2.7	Concurrent session control	No requirements	No requirements in addition to those of SL-1	- ability to limit the number of sessions per interface for any user Not sufficient: - Sessions cannot be limited per interface - Sessions cannot be limited per user	No additional requirements in addition to those of SL-3
CR 2.8	Auditable events	- audit records for following security relevant cases are generated: access control, request errors, control system events, backup and restore events, configuration changes, audit log events, and - audit records include at least the following information: timestamp, source, category, type, event ID, event result Essential functions: Audit events do not adversely affect essential functions.	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 2.9	Audit storage capacity	- capability to allocate audit record storage Examples: - log rotation mechanism ensures that audit storage capacity is never exceeded Not sufficient: - failure of audit functionality when a threshold is reached or the storage capacity is exceeded	No additional requirements in addition to those of SL-1	Additional to SL-2: RE (1) - a warning message informs when a configurable threshold is reached Not sufficient: - no warning is produced if the used storage capacity reaches the threshold - the threshold is not configurable	No additional requirements in addition to those of SL-3

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 2.10	Response to audit processing failures	- no loss of essential services or functions during an audit processing failure, or - optional support of appropriate actions in response to an audit processing failure Examples: - alerting personnel could be an appropriate action	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 2.11	Timestamps	- ability to generate timestamps for audit records (see CR 2.8) - timestamps include date and time	Additional to SL-1: RE (1) - synchronized timestamps - e.g. external source like NTP server	No additional requirements in addition to those of SL-2	Additional to SL-3: RE (2) - Ability to detect unauthorized alteration of time source identity, Example: - compare against a second time source over a protected channel"
CR 2.12	Non-repudiation	Applicable if HMI is used. - possibility to determine which human user took a particular action, and - logging of user id in the audit trail Essential functions: Non-repudiation does not add significant delay to essential functions.	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	Additional to SL-3: RE (1) - possibility to determine which user (human, software process or device) took a particular action, and - logging of all identities in the audit trail
CR 2.13	Use of physical diagnostic and test interfaces	No requirements	No SAR for software applications. In case factory diagnostic and test interfaces use network communication, the interfaces are to be subjected to all of the requirements of this document. - prevent unauthorized use of the physical factory diagnostic and test interfaces, e.g. JTAG Not sufficient: - any diagnostic and test interface without authorization	Additional to SL-2: RE (1) - provides active monitoring of the device's diagnostic and test interfaces, and - generate log entry when attempts to access these interfaces are detected	No additional requirements in addition to those of SL-3

6.4 FR-3: System integrity

Table 3 shows the FR-3: System integrity.

Table 3 – Evaluation criteria for FR-3: System integrity

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 3.1	Communication integrity	- capability to protect integrity of transmitted information, and - use of error detection codes, e.g. CRC (protection against casual or coincidental manipulation), or - use of standardized cryptographic protocol, or - use of recommended protocols (e.g. BSI TR-02102), see CR4.3 In case protocols are not capable to provide integrity, compensating countermeasures shall be applied. Compensating countermeasures may include physical security of the cable or network. Compare to Evaluation activity EA-7 and EA-8.	Additional to SL-1: RE (1) - capability to verify authenticity of information during communication Not sufficient: - use of error detection codes, weak hashing or weak signature functions - authentication of information is not possible - fallback to not recommended protocols In case protocols are not capable to provide authentication integrity, compensating countermeasures shall be applied. Compensating countermeasures may include physical security of the cable or network. Compare to Evaluation activity EA-7 and EA-8.	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 3.2	Protection from malicious code	Software Application Component - list at least one compatible security mechanism which implements the protection functionality (user documentation requirement)	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
		Embedded Component - capability to protect from installation and execution of unauthorized software, or - in case the environment is capable of providing malicious code protection as a compensating countermeasure, this shall be applied. Compare to Evaluation activity EA-7 and EA-8. or - use description (is available, or - allowed detection techniques: binary integrity, attributes monitoring, hashing, signature techniques, or - allowed prevention techniques include removable media control, sandbox techniques, specific computing platforms mechanisms (e.g. restricted firmware update), No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection. mandatory access controls, process whitelisting and comparable mechanisms	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
		Host Component - need to document any special configuration requirements related to protection from malicious code"	Additional to SL-1: RE (1) - able to automatically report version of the malicious code protection which is actually in use	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
		Network Component - provided by the network device directly - allowed to use compensating control	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 3.3	Security functionality verification	- definition of (manual) verification procedures for verifying the security functionality, and - guidance on how to test security functionality (documentation requirement) Not sufficient: - no possibility to test security functionality, e.g. no log message, no notification	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	Additional to SL-3: RE (1) - definition of (manual) verification procedures for verifying the security functionality during normal operation, and - guidance on how to test security functionality (documentation requirement) during normal operation, and - documented side effects if these verification procedures are running during normal operation
CR 3.4	Software and information integrity	- integrity check of data at rest (e.g. security configuration, software configuration, firmware configuration, and other information), or - capability to be integrated into a system that can perform or support integrity checks Not sufficient: - no recording of results of checks	Additional to SL-1: RE (1) - authenticity check of data at rest (e.g. security configuration, software configuration, firmware configuration, and other information)	Additional to SL-2: RE (2) - unauthorized change is reported to a configurable entity upon discovery of the attempt	No additional requirements in addition to those of SL-3

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 3.5	Input validation NOTE Not-accept-criteria are guidance on how insufficient input validation methods have to be considered for different SL levels to plan test cases with reasonable effort.	- every input, that directly impacts the action of the application or device is validated for syntax, length and content Not sufficient: - missing validation of out-of-range values for a defined field type - invalid characters in data fields - missing or incomplete data and buffer overflow - SQL injection attacks - cross-site scripting - malformed packets"	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 3.6	Deterministic output	Applicable if device directly controls a process. - the deterministic output needs to be documented (documentation requirement), and - in case of failsafe, it is allowed to demonstrate by described process	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 3.7	Error handling	- error conditions are identified and handled, and - no unintended information is leaked, and - no security relevant information is visible	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 3.8	Session integrity	No requirements	- use of mechanisms to protect the integrity of communication sessions, and - sessions are invalidated after termination, and - sessions are invalidated after reboot, and - use of unique session IDs and recognize only system-generated IDs Not sufficient: - possible to perform - session hijacking - man-in-the-middle attack - insertion of false information into a session - replay attacks	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 3.9	Protection of audit information	No requirements	- protect audit information and audit tools (if present) Not sufficient: - unauthorized access, modification or deletion of audit information and audit tools (if present)	No additional requirements in addition to those of SL-2	Additional to SL-3: RE (1) - Protect audit information by storing the audit records on a hardware-enforced write-once media, e.g. WORM (write once read many)
CR 3.10	Support for updates	- capability to be updated and upgraded once commissioned, and - if a component supports or executes essential functions, a mechanism exists to support patching and updating without impacting the essential function	Additional to SL-1: RE (1) - the authenticity and integrity of any update is validated prior installation	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-2

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 3.11	Physical tamper resistance and detection	No requirements	Not applicable in case of Software Applications. For Host Components - support anti-tamper resistance and detection mechanisms: capability to add specialized materials to make tampering difficult; e.g.: enclosure with sensor that detects volume intrusion, locks, encapsulation, security screws (non-standard head types), seal, and - detection mechanisms for unauthorized physical access into the device, e.g. seal For Embedded and Network Components - provide tamper resistance and detection mechanisms: specialized materials to make tampering difficult; e.g.: enclosure with sensor that detects volume intrusion, locks, encapsulation, security screws (non-standard head types), seal - detection mechanisms for unauthorized physical access into the device, e.g. seal	Additional to SL-2: RE (1) - capability to automatically notify upon discovery of an attempt to make an unauthorized physical access, and - capability to configure a set of recipients to inform about a tampering attempt and to integrate this into an overall system logging Examples: - electronic switches	No additional requirements in addition to those of SL-2

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 3.12	Provisioning product supplier roots of trust	No requirements	Not applicable in case of Software Applications. - provision of product supplier keys and roots of trust during device manufacturing, e.g. cryptographic hashes or public key used for verification, and - write-access to root of trust is restricted to authorized users only Not sufficient: - missing root of trust - keys or root of trust can be manipulated or leaked	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 3.13	Provisioning asset owner roots of trust	No requirements	Not applicable in case of Software Applications. Applicable if CR 2.4 Mobile Code is selected. - capability to provision asset owner roots of trust, and - protection of asset owner roots of trust Not accepted: - export of root of trust (private key) - leakage of root of trust security information	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 3.14	Integrity of the boot process	Not applicable in case of software applications. - integrity verification of boot process relevant firmware, software and configuration data prior to the use	RE (1) - authentication verification of boot process relevant firmware, software and configuration data prior to the use, and - use of product suppliers roots of trust for verification	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

6.5 FR-4: Data confidentiality

Table 4 shows the FR-4: Data confidentiality.

Table 4 – Evaluation criteria for FR-4: Data confidentiality

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 4.1	Information confidentiality	- capability to protect against unauthorized disclosure of information via eavesdropping or casual exposure, and - capability to protect the confidentiality of information at rest for which explicit read authorization is supported, and - protection of the confidentiality of information in transit, and - (wireless) use of encryption Not sufficient: - outdated or deprecated protocols - use of cleartext protocols (e.g. FTP) without additional protection mechanisms (e.g. cryptographic signatures of payload)"	- capability to protect against unauthorized disclosure of information caused by an attacker actively searching for vulnerabilities with low resources, generic skills and low motivation Example: - use of cryptographic mechanisms (see CR 4.3)	- capability to protect against unauthorized disclosure of information caused by an attacker actively searching for vulnerabilities with moderate resources, IACS specific skills and moderate motivation	No additional requirements in addition to those of SL-3
CR 4.2	Information persistence	No requirements	- capability to purge component, or - capability to erase all information with explicit read authorization Not sufficient: - ability to retrieve or access information, for which explicit read authorization is supported, after component was decommissioned	Additional to SL-2: RE (1) + RE (2) - capability to protect against unauthorized and unintended information transfer via volatile shared memory resources, and - capability to verify that the erasure of information occurred effectively	No additional requirements in addition to those of SL-3

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 4.3	Use of cryptography	If cryptography is required by CR 1.14, CR 3.1 and CR 4.1. - use of standardized cryptographic algorithm, and - use of recommended protocols (e.g. BSI TR-02102, or other examples mentioned in IEC 62443-4-2 CR4.3), and - - used according to proven practices or documentation Not sufficient: - proprietary implementation of cryptographic algorithms which are not generally recognized	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

6.6 FR-5: Restricted data flow

Table 5 shows the FR-5: Restricted data flow.

Table 5 – Evaluation criteria for FR-5: Restricted data flow

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 5.1	Network segmentation	Network Component Requirement - support of network segmentation, e.g. multiple network cards, VLANs, or - network configuration with routing and router capability Non-Network Component Requirement Not sufficient: - component does not have a capability to support network segmentation, e.g. critical control systems and safety-related systems are not completely isolated from other networks	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 5.2	Zone boundary protection	Network Component Requirement - capability to monitor and control communication at zone boundaries to enforce compartmentalization defined in risk-based zones and conduits model Not sufficient: - demonstrate insufficient boundary protection, e.g. network component goes to "allow all" mode in high traffic situations, or network component with no error monitoring capability	Additional to SL-1: RE (1) - capability to deny network traffic by default, and - allow network traffic by exception	Additional to SL-2: RE (2) + RE (3) - capability to prevent any communication through the control system boundary (island mode), and - provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (fail close)	No additional requirements in addition to those of SL-3
CR 5.3	General purpose person-to-person communication restrictions	Network Component Requirement - capability to prevent general purpose, person-to-person messages from being received from users/systems to the control system (email, all forms of social media, message systems) Not sufficient: - no/insufficient traffic inspection, e.g. blocking of general purpose, person-to-person communications systems is not done properly Example: - filtering traffic with packet filters or application-level gateways	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

6.7 FR-6: Timely response to events

Table 6 the FR-6: Timely response to events.

Table 6 – Evaluation criteria for FR-6: Timely response to events

ID	Requirement Title	SL-1	SL-2	SL-3	SL-4
CR 6.1	Audit log accessibility	- capability for authorized humans or tools to access audit logs on a read only basis Not sufficient: - audit logs are accessible to unauthorized users Examples: - access via web interface (audit perspective), or - access via console tools (separate information system for audit access)	No additional requirements in addition to those of SL-1	Additional to SL-3: RE (1) - programmatic access to audit records by either using an application programming interface (API), or - capability to send the audit logs to a centralized or dedicated system for the handling of audit logs	No additional requirements in addition to those of SL-3
CR 6.2	Continuous monitoring	No requirements	- capability to provide an active interface for continuous monitoring, or - capability to send continuous monitoring information to a centralized system	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3

6.8 FR-7: Resource availability

Table 7 shows the FR-7: Resource availability.

Table 7 – Evaluation criteria for FR-7: Resource availability

ID	Requirement title	SL-1	SL-2	SL-3	SL-4
CR 7.1	Denial of service protection	- capability to operate in a degraded mode (essential functions) during a DoS event	Additional to SL-1: RE (1) - Manage communication load from application or device to mitigate effects of DoS events Essential functions: - component maintains essential functions while in a degraded mode unless supported by a risk assessment Example: - limit network capacity of interfaces	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 7.2	Resource management	- capability to limit the use of resources by (active running) security functions to prevent resource exhaustion Examples: - software process prioritization - network traffic rate limiting	No additional requirements in addition to those of SL-1	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3
CR 7.3	Control system backup	- provide backup abilities to safeguard application/device state (user- and system-level information), and - Backup Process does not affect normal operation Not sufficient: - no / insufficient backup abilities, e.g. the backup does not provide the necessary protection of the data at rest - normal operation is affected by control system backup	Additional to SL-1: RE (1) - capability to verify the reliability of backup mechanism Examples: - verify backup data mechanism, - integrity of backed up information is validated prior to restoring it	No additional requirements in addition to those of SL-2	No additional requirements in addition to those of SL-3