IT Security Association Germany

TeleTrusT Evaluation Method for IEC 62443-4-2

Security for Industrial Automation and Control Systems

2019-05

TeleTrusT Working Group "Smart Grids / Industrial Security"

Co-ordination and contact:

Sebastian Fritsch, secuvera GmbH

Tobias Glemser, secuvera GmbH
Steffen Heyde, secunet Security Networks AG
Dr. Holger Muehlbauer, IT Security Association Germany (TeleTrusT)

Imprint

Publisher:

IT Security Association Germany (TeleTrusT)
Chausseestrasse 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

TeleTrusT Evaluation Method for IEC 62443-4-2

2019-05

Security for Industrial Automation and Control Systems

IEC 62443 Security for Industrial Automation and Control Systems -
Part 4-2: Technical Security Requirements for IACS Components (IEC 62443-4-2:2019)

Inhaltsverzeichnis

Inhalt

1 Introduction

1.1 Scope

The relatively young and partly unfinished standard IEC 62443 aims at viewing the topic of cyber security in the industrial field (primarily in automation technology) in its entirety, focusing on the roles of asset owner, integrator, and component manufacturer.

This evaluation method focuses on the IEC 62443-4-2 (IEC 62443-4-2:2019), which poses requirements on the technical security properties of industrial components. In addition, IEC 62443-4-1, which directly addresses component manufacturers, contains requirements pertaining to a secure development process. The requirements on technical security properties of comprehensive industrial systems (facilities) is covered in IEC 62443-3-3.

The standard IEC 62443 consists in all parts of process models and requirements for the design and operation of secure industrial systems. However, there are no requirements given pertaining to a third party verifying the correct and effective implementation of the standard. This is especially relevant in a certification context, because manufacturers holding certificates are generally expected to provide comparable evaluation results.

This document is a proposal for an evaluation approach to verify the fulfilment of the requirements of IEC 62443-4-2.

The evaluation method primarily pertains to the technical qualities of a component while also assuming that the development of that component was based on a development process according to the IEC 62443-4-1. However, by applying the evaluation method, no conclusion can be drawn as to the state of maturation of said development process.

This means that the evaluation method postulates, according to the standard, that the development of a component was based on the processes defined by the IEC 62443-4-1, i.e., there are results (deliverables) of the development process available, which can be resorted to during the evaluation of the component. Any references made in this evaluation method pertain to these deliverables, not the evaluation of the state of maturation of the development process per se.

The evaluation method is not meant to be a certification scheme, but a basis for a conformity assessment. Aspects relevant to a certification, such as the definition of participating roles, application procedures, approval and monitoring of certified components, and more, will need to be defined accordingly by evaluation scheme operators or certification authorities, which is not part of this document.

The evaluation method perceives itself in terms of the IECEE system document [OD-2061] as the implementation of a product certification according to the IEC 62443-4-2 and scenario 1. However, the evaluation method does not consider the existence of an IEC 62443-4-1 certification as sufficient. As described above, only the deliverables of an IEC 62443-4-1-conformant development process are taken into consideration, i.e., the evaluation is performed based on evidence and not on existing certificates.

The evaluation method can be used for combined certifications according to IEC 62443-4-2 with regard to a development process according to IEC 62443-4-1. This would be a third-party evaluation. Another typical application of the evaluation method is a conformity assessment of a manufacturer's own components, i.e. first-party evaluation.

The desired result of an evaluation according to this scheme, referring to a specific component, is a verification of the correct and robust implementation of the requirements of IEC 62443-4-2 or of a lack thereof. Additionally, the evaluation answers the question whether or not the component is resistant according to the level of a defined attacker (the security level, see Chapter 1.3). The evaluation result always pertains to the version of the component under consideration and takes into account the vulnerabilities and attack methods known at that time.

1.2 Overview of IEC 62443-4-2

Industrial components according to IEC 62443-4-2 are divided into four device type categories:

- embedded devices, e.g. PLC, sensors, SIS (Safety Instrumented Systems) controllers, DCS (Distributed Control System) controllers;
- host devices, e.g. notebooks, PCs, workstations;
- network devices, e.g. industrial routers;
- applications, e.g. configuration software, historiography software.

These are components used in industrial automation systems. Among other things, these are COTS (commercial off-the-shelf) components which are being made available to a larger group of users. However, the norm part may also be used by a system manufacturer/integrator aiming for the mitigation of the risks accompanying the design phase of a facility, who wants to develop a specific component with selected security properties.

The standard part sorts the individual requirements into so-called Foundational Requirements (FR), which may also be understood as subject categorisation. Among those are Component Requirements (CR), which constitute the technical detail requirements.

1.3 Application of the Standard

For the evaluation according to IEC 62443-4-2, two approaches can be derived from the definition given in the standard part as well as the whole IEC 62443:

1. Selection of a Security Level (SL) in connection with requirements (CR) and resistance level.
2. Targeted selection of requirements (CR) of a defined resistance level.

The first model assumes a component manufacturer’s perspective who wants to perform an evaluation of the security properties of the various operation modes of his components. The manufacturer uses the security level to define the target level of his security properties, which in turn is derived from, e.g., the analysis of the usual operational environment of his component or customer surveys.

The second model assumes the facility design perspective. To this end, a risk analysis according to the procedure model given in the standard part IEC 62443-3-2 is performed, and, on the basis of the determined risks, a system design is created. In order to mitigate the determined risks, the necessary requirements on the components can be derived. This set of requirements can be specifically defined via a selection of requirements (CR).

Irrespective of both procedure models, a component manufacturer has to meet the requirements of the IEC 62443-4-1 in the development process of his component. One important result of this process is, e.g., the definition of the component’s intended use or context. This and other information offer valuable insights into the component’s expected behaviour to the user as well as the evaluator.

The definition of the term “Security Level”, more precisely SL-C as in SL Capability, according to IEC 62443-4-2 consists of two components, the selection of requirements (CR) and a defined attacker type. An attempt was made to combine these two in a sensible and universally valid way according to the IEC 62443-4-2. However, a risk analysis may result in having to adjust both the requirement set and the attacker type definition. Component manufacturers often face the problem that their customers’ exact application scenarios are not sufficiently known or differ greatly from one another. It is therefore sensible and effective for component manufacturers to resort to the pre-defined security levels in order to simplify their approach. When selecting a security level, the component’s intended use should be taken into account.

Concerning attack resistance, the security level defines the following abstract attack types:

Security Level	Attack Type
SL-1	Protection against casual or coincidental violation.
SL-2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation.
SL-3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.
SL-4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation.

Table 1

1.4 Security Level Differentiation

This evaluation method is based on the requirements of the security levels SL-1 to SL-3. SL-4 is not taken into consideration, because for the time being, this document addresses evaluations in the medium/substantial assurance range in order to firstly gain some experience in handling the standard.

Security Level SL-4 assumes an attacker with high potential, high motivation, and high resources. It is recommended to develop specific security concepts for this case, i.e. based on standard part IEC 62443-3-2.

In the future, an update of this evaluation method in order to incorporate SL-4 will be possible.

1.5 Target Audience

The primary target audience of this evaluation method are assessors, testing laboratories, and internal QA and IT testing departments. Certification authorities can apply this evaluation method. Additionally, this document is for component manufacturers who want to prepare an evaluation of their components, i.e. development departments.

1.6 Normative Terminology

In the following text, the key words SHALL, SHOULD, CAN, and MAY will be used according to their normative meaning und will be written in capital letters. Thereby, SHALL is a strict requirement, SHOULD is used as a recommendation, CAN is a possibility, and MAY is a permission for a potential application.

1.7 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 62443-3-3, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels* [IEC62443-3-3]
IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Product development requirements* [IEC62442-4-1]
IEC 62443-4-2, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components* [IEC62442-4-2]

1.8 Terms and Definitions

Term	Definition
Acceptance Criteria	Criteria for the evaluator for assessing whether an implementation has been executed in an acceptable manner according to the requirement
Attack Resistance	A component's ability to remain resistant (cf. security level) against an attack
Resistance Level	Categories for the description of the expected attack resistance according to respective attack potential (definition of security levels)
Robustness	Maintaining correct functionality in case of invalid input or unfavourable environmental conditions, i.e. special characters in per se regular user input

Table 2

2 Concept of the Evaluation Method

2.1 General Concept

The evaluation of a component related to compliance with the standard part IEC 62443-4-2 SHALL be carried out according to the following steps:

1. Intended Use Verification
2. Documentation (Design)
3. Documentation (User)
4. Conformity Assessment
5. Vulnerability Analysis

The first step is based on two principles; one is the normative requirement of the component development being processed according to the standard part IEC 62443-4-1. To this end, a security context and a threat model SHALL be established. Two: The to some extent very abstract descriptions of the requirements of the IEC 62443-4-2 entail that the component-specific parameters SHALL be taken into account for the evaluation, which in turn means that the component's intended use SHALL be specified.

In order to be able to evaluate a component's security properties, the manufacturer is required, depending on the evaluation concept and security level, to provide details on the component. In established IT product evaluation standards, it is common practice to convey an increasing resistance by using a higher security level (SL), e.g., accompanied by a more intense evaluation and therefore growing assurance. In principle it is also applied in this evaluation concept in such a way that with a higher security level, a manufacturer SHALL provide more detailed developer or designer documents.

In the following step, the user documentation SHALL be examined for completeness and correctness in regard to security properties. The minimum requirement of topics to be covered can be derived from the processes given in the IEC 62443-4-1, an overview of which can be found in Chapter 2.4 of this document.

The next and more substantial evaluation step is an evaluation of the implementation in regard to the previously defined requirements according to the chosen security level. In order to assist the evaluator during the evaluation, acceptance criteria are defined in this document. Proof of compliance with these criteria SHALL be established via one or more tests. If this is not possible, i.e. if the functionality cannot be tested over an interface, then a proof CAN be established via a design document evaluation.

The following step is a vulnerability check in order to identify whether the expected attack resistance was sufficient. In this step, a reference to the assumed attack resistance SHALL be made, which is also defined by a chosen security level. If the security requirements are not defined by a security level, the correct attacker type SHALL be chosen explicitly.

At least two instances of the component SHOULD be available to the evaluation team; this optional requirement aims to provide an evaluation process free from interferences. The component SHALL conform to a normal serial model. If the component is still undergoing development, it SHALL be ensured that the evaluated component specifics conform with those of the subsequent serial model.

The previously mentioned points define the extent of the information to be provided by the manufacturer for the evaluation according to IEC 62443-4-2. In the following, a more in-depth description is given about the specific details pertaining to the respective steps.

2.2 Intended Use Verification

The intended use defines the component's operational and security requirements. These CAN for example be described as assumptions about the operational environment. A specific format for this description is not defined in the IEC 62443. The contents of the description, however, are required for an effective evaluation.

The contents can be deduced from the processes given in the IEC 62443-4-1 and will partly be specified in this document. A security context (SR-1) SHALL be defined and a threat model (SR-2) SHALL be established for the component.

According to this evaluation method, the information SHALL be given in the form of a descriptive document. The content of the component specification is given in Appendix A of this document which SHOULD be used to represent all required information. The component specification CAN be used as a structure for the descriptive document or as a checklist for referenced documents.

The evaluator SHALL analyse the provided information regarding completeness and correctness.

2.3 Documentation (Design)

Established evaluation standards make use of the concept of incremental assurance levels. In addition, a direct reference is made between the attack resistance and the absence of vulnerabilities. The underlying idea is that transparency in the technical details offers the evaluators an effective way to evaluate the component design. This also allows for the identification of design flaws in this analysis step.

This evaluation method takes on this concept and assigns the following postulated design documentation to the aforementioned levels SL-1 to SL-3 (resistance level).

The technical implementation SHALL be adequate to the chosen security level (resistance), which is to be represented by the design documentation. This requirement results from the definitions of the seven Foundational Requirements (FR) given at the beginning of each chapter (Chapters 5 to 11) of the [IEC62442-4-2].

This means, for instance, that in regards to the requirement CR 4.1 Information Confidentiality, it must be shown why the chosen implementation at SL-2 complies with the level required in FR 4 Data Confidentiality: „Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.“

The final assessment on whether the technical implementation corresponds with the required security level takes place in step 5 Vulnerability Analysis.

Security Level	Postulated Design Documentation	Annotation
SL-1	Description of all external interfaces, i.e.: all cable-bound and wireless communication interfaces, electrical interfaces, debugging interfaces including a description of their functionality and configuration options, e.g. an interface for component configuration including a technical description of the protocol (or the protocol stack) and all configuration parameters, furthermore a communication matrix (source, target, and purpose).	

	Information about cryptographic algorithms in use, also a reference to the recommending authority and a reason for the choice of algorithm. Information about software in use, including 3rd-party libraries and exact version. Information for the protection of the component's integrity, i.e. firmware file integrity (term from [IEC62442-4-1]: product integrity verification mechanisms).	
SL-2	See SL-1.	
SL-3	Additionally, internal design, i.e.: mention of subsystems and modules with functionality and external configuration options, also a description of the security architecture. Listing all of the component's current users. These must also be listed in the documentation.	
SL-4	Not defined	Not relevant for this version of the evaluation method.

Table 3

The evaluator SHALL perform a test of comprehensibility and comprehensiveness. The information SHALL be referred to in the conformity assessment and vulnerability analysis. The previously performed Threat Modelling (SR-2) SHALL be taken into account during the evaluation of design decisions and SHALL be checked for conclusiveness.

2.4 Documentation (User)

The component's development process SHALL adhere to the processes given in IEC 62443-4-1, therefore, the following contents of the user documentation are required. The corresponding process from the standard part IEC 62443-4-1 is given in brackets:

- installing security updates for the component (SUM-2) and additional independent components or underlying operating systems (SUM-3);
- rolling out security updates (SUM-4);
- describing the component's defense-in-depth strategy (SG-1);
- requirements of the defense-in-depth strategy on the operational environment;
- performing security hardening via component configuration (SG-3), e.g. how to configure a hardened minimum configuration (CR 7.7 least functionality);
- secure decommissioning/disposal (SG-4);
- secure operation (SG-5);
- account management (SG-6).

The evaluator SHALL assess whether the information provided in the user documentation is adequate and complete and does not contain any discrepancies.

2.5 Conformity Assessment

The standard part IEC 62443-4-2 poses requirements (Component Requirements, CR) that are, in part, already specifically defined, in other parts described in a technology-independent manner. The requirements for a specific component SHALL be substantiated by the evaluator within a test case.

As an intermediate step, acceptance criteria are defined which are then used as a guideline for the expected results for the test case. The evaluation method derives the acceptance criteria from the standard requirements and also, if possible, offers examples for non-acceptance.

The acceptance criteria, unlike the standard, can be specified technologically, i.e. it is possible to specifically name recommended technologies.

The process model for transferring requirements to test cases is composed in the following order (step 3 is to be mentioned in the evaluation documentation):

1. Requirements of the standard parts (CR from IEC 62443-4-2, sorted by FR)
2. Acceptance criteria (of this evaluation method, Appendix C)
3. Test cases (component-specific, not defined in this document)

For each requirement of the standard, at least one test case SHALL be referenced. In many cases, several tests SHOULD be referenced, because requirements could pertain to more than one interface or component function.

A test case SHALL be described with at least the following characteristics:

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

The test expectation is the expected test result, which will occur if the component functions correctly. The test expectation SHALL result from the component’s intended behaviour and the acceptance criteria. The test result is the actually detected behaviour of the component during the testing steps. The choice of technical implementation SHALL be appropriate for the chosen security level (resistance) which has to be shown in the design documentation, see step Documentation (Design) in Chapter 2.3. During conformity assessment it SHALL be examined whether the chosen technical implementation has been performed correctly. The test description SHALL reflect details of the technical implementation adequately. The final evaluation of whether the technical implementation conforms with the required level is performed in step 5 Vulnerability Analysis.

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).

If no test case can be specified for a CR, e.g. if one implementation detail cannot be addressed via an external interface, an alternative proof of correct implementation SHALL be given. To this end, an evaluation of the pertaining design documentation focusing on the respective CR and regarding the acceptance criteria CAN be performed. The level of detail in the design documentation SHALL be appropriately high. The evaluator SHALL give a well-founded opinion on the compliance with the acceptance criteria.

The following example pertaining to CR 3.1. Communication Integrity aims to illustrate the previously described process model:

	Level		**Specific Example**
1	IEC 62443-4-2	CR 3.1: Communication Integrity	The component shall provide the capability to protect the integrity of transmitted information.
2	Evaluation method	Acceptance criteria	Accept: - capability to protect integrity of transmitted information; - use of CRC (protection against casual or coincidental manipulation); - use of standardised cryptographic protocol; - use of recommended protocols (e.g. BSI TR-02102), see CR4.3.
3	Component-specific, evaluation documentation	Test cases for assumed communication protocols HTTPS and FTP with a fictional component	Test description: Connections for 1) Test HTTPS against recommended protocols, 2) Test FTP. Test expectation: No manipulation due to man-in-the-middle attack is successful.

			Test conditions: ARP spoofing for diverting local network traffic to man-in-the-middle attacker. Test steps: a. Establish connection. b. Manipulate network packets. c. Observe if data is still transmitted, received, and processed. Test results: 1. HTTPS → Manipulation is not possible, but analysis of available cipher suites showed that non-recommended ciphers were active (not accepted). 2. FTP → Manipulation is possible (not accepted). Assessment: If all cases are accepted → pass, otherwise → fail; in this example all cases were not accepted, therefore the test failed.

Table 4

2.6 Vulnerability Analysis

The vulnerability analysis aims to determine whether a component has known or exploitable vulnerabilities. Additionally, it determines whether security properties have been implemented using mechanisms with sufficient resistance against an assumed attacker type (defined by the security level). Sufficient resistance means that only such attacks can be described that operate above the asserted resistance. The according assessment method is described in the following.

The identification of vulnerabilities CAN be integrated into several phases of the component's development, using the following methods of the IEC 62443-4-1:

- threat model (SR-2);
- threat mitigation testing (SVV-2);
- vulnerability testing (SVV-3);
- penetration testing (SVV-4).

During the evaluation process and the evaluation of the results, an evaluator SHALL adopt the necessary independence according to the respective role (first-, second-, third-party) (SVV-5).

Additionally, the previously described step "Conformity Assessment" can be utilised to find potential vulnerabilities. The analysis also examines all orthogonal threats to the requirements (CR), e.g.:

- vulnerabilities in 3rd-party software;
- vulnerabilities in the operating system;
- manipulation of the hardware, firmware, or the BIOS;
- missing integrity assurance for data exports.

Irrespective of phase and method, the goal of identifying and evaluating all known and exploitable vulnerabilities SHALL be reached.

The evaluation of the vulnerabilities SHALL lead to the conclusion that at the time of completion, no vulnerabilities are known that can be exploited successfully by the assumed attacker type.

The analysis will yield a list of identified vulnerabilities which will then be assessed according to their relevance and criticality for the component in question. In this context the intended use must be considered.

The evaluation SHALL take into account the attacker type definition. The attacker type is defined in the IEC 62443 by the security level, e.g. SL-3 defines an attacker with a medium attack potential. A component claiming to conform with SL-3 has to be resistant against such an attacker.

In consequence, an evaluation model has to take into account all relevant factors for such an attacker. The present evaluation method does not predefine a specific vulnerability assessment metric.

The used model for the vulnerability assessment SHALL fill the subsequently listed requirements. To give the users of this evaluation method more details, Appendix D defines and illustrates a model for vulnerability assessments based on the [CEM] methodology.

The evaluation requires that not one particular vulnerability is considered, but the whole attack vector SHALL be outlined. This is how the component's intended use can be reflected in the vulnerability analysis. An attack CAN include a sub-step which has not yet been described practically, but only theoretically, in which case the technical experts must be able to argue for the realistic feasibility of this step in the future.

The chosen assessment method SHALL ensure that an outlined attack and attack vector is distinctively above the threshold of the resistance level, hence above SL-1 to SL-3. This CAN take place by choosing a quantification or by using categories. For this, standardised methods SHOULD be used in order to support comparability of the evaluation results.

The technical attack vector evaluation SHOULD be performed with the help of the design documentation. For the evaluation of possible countermeasures, the security architecture SHOULD be considered (SD-2).

The following list of evaluation criteria SHALL be used for the chosen evaluation methodology for a complete attack, at least indirectly:

- time needed (both for the design and for the execution of the attack);
- expertise;
- knowledge of the component (e.g. is it accessible by the public or only by the development team);
- window of opportunity;
- attacker's equipment.

An example for the application based on the suggested [CEM] methodology can be found in Appendix D.

In addition, a vulnerability assessment according to CVSS can be performed. This approach, however, neither takes the whole attack vector nor the component's intended purpose into consideration as described before and thus can only offer the classification of a found vulnerability. This assessment can in turn be helpful for providing identified vulnerabilities with a criticality rating for the component's future development process. CVSS provides a metric to assess the severity of found vulnerabilities.

3 Evaluation Process

3.1 Conformity Assessment

A conformity assessment within the scope of a certification SHALL be performed by specialised testing labs with expertise in IT security. The evaluation facility should orientate their own testing methods by the DIN EN ISO/IEC 17025. This corresponds with the [DAkkS] accreditation requirements for the IEC 62443. Because of the existing expertise, the activities performed by inspection bodies in the context of the IEC 62443 can only be applied to later inspections, such as whether a component with a certain set of technical capacities in a certain site complies with legal requirements.

The evaluators' qualification based on expertise SHALL orientate itself by the chosen security level (attack resistance).

The evaluators' independence SHALL conform with the requirements of the [IEC62442-4-1] (SVV-5: Independency of testers).

The requirements which are posed in documents such as application documents or templates SHOULD be provided by certification authorities. The content requirements posed on manufacturer documents which are needed for this evaluation method can be found in Appendix A "Component Specification".

This document explicitly only offers complete acceptance criteria for the evaluation process. Conclusions such as "not applicable" CAN, where necessary, be allowed as part of a conformity assessment; this, however, lies outside the scope of this evaluation method. Physical security properties, for example, CAN be excluded from an assumed threat scenario with logical attacks. This document addresses the complete technical evaluation.

The result of a positive conformity assessment is the verification of a component's aptitude, that is SL-C or the targeted selection of requirements (CR).

3.2 Certification

In case of a certification (outside IECEE) according to the standard part IEC 62443-4-2, this evaluation method SHOULD be used.

(Prospective) In case of an IECEE certification, this evaluation method SHALL be applied compulsively.

In certifications the competence of the evaluation team SHALL be consistent with the requirements from ISO/IEC 17025.

3.3 Other Testing Methods

The evaluation method CAN be used for other testing methods, such as:

- technical assessments in supplier-agent relationships (second-party evaluation);
- internal testing of a component's technical aptitude and resistance by an in-house QA department (first-party evaluation).

3.4 Testing Procedure

Before the testing, a timetable SHOULD be constructed which should contain submission dates for the test objects as well as time periods and completion dates for the steps listed in Chapter 2.

The competence of all experts of the evaluator team SHALL be proven. This SHALL be done prior to the start of an evaluation.

4 Appendix A (Normative) – Component Specification

4.1 Preliminary Note

In the following, the requirements with regard to the content of the manufacturer's documents, which are to be used in this evaluation method, are described. Requirements derived from the Secure Development Process (according to standard part IEC 62443-4-1) will be labelled with the abbreviation for the respective process, e.g. "(SM-6)". The verification of these specifications takes place during the step "Intended Use Verification", see Chapter 2.2.

4.2 Component Description/Declaration of Conformity

- Short component description;
- component identification;
- component label,
- version;
- identification during operation, installation and updates;
- proof of component integrity, primarily software (SM-6);
- component category

o according to IEC 62443-4-2: software application, embedded component, host component, or network component;

- excluded parts of the component;
- component functionalities which are not considered:

o deactivated by default;

o only activated for special cases and not the focal point of the conformity assessment;

- declaration of security requirements

o by stating a security level: SL-1, SL-2, SL-3, or SL-4

or

o by listing individual requirements, including possible requirement enhancements;

- specification of the assumed attacker type (resistance level)

o by stating a security level: SL-1, SL-2, SL-3, or SL-4 (analogous to the declaration of conformity or divergent, but generally higher)

or

o by describing the attacker (based on the definition given in the IEC 62443).

4.3 Intended Use

- Intended use (SR-1);
- use cases;
- threat model (SR-2);
- operational environment (mandatory and optional);
- security functionality (SR-3, SR-4);
- implementation mechanisms for security properties;
- information on whether PKI techniques are supported.

4.4 Documentation

User documentation:

- depending on the intended use, information on secure operation, e.g. in an

o end customer documentation;

o integrator documentation;

- mandatory content requirements:

o source and implementation of component updates and underlying components/operating systems (SUM-4);

o information on the update extent (SUM-2);

o information on update dependencies (SUM-3);

o contact point for security problems (DM-1);

o defense-in-depth measures of the component (SG-1);

o defense-in-depth measures of the operational environment (SG-2);

- information on security hardening (SG-3);
- information for secure decommissioning (SG-4);
- information for secure operation (SG-5);
- information on account management (SG-6).

Design documentation:

- For SL-1 to SL-3:
  - description of all external interfaces,
    - all cable-bound and wireless communication interfaces, electrical interfaces and debugging interfaces including a description of their functionality and configuration options, e.g. an interface for component configuration including a technical description of the protocol (or the protocol stack) and all configuration parameters, furthermore a communication matrix (source, target, and purpose);
  - information about cryptographic algorithms in use, also a reference to the recommending authority and a reason for the choice of algorithm;
  - information about software in use, including 3rd-party libraries and exact version;
  - information for the protection of the component's integrity, i.e. firmware file integrity (term from [IEC62442-4-1]: product integrity verification mechanisms).

- For SL-3 additionally:
  - listing of subsystems and modules with functionality and external configuration options;
  - description of the security architecture;
  - listing all of the component's system accounts.

5 Appendix B (Normative) – Evaluation Report Requirements

5.1 Preliminary Note

In the following, the requirements with regard to content of the evaluation report according to this scheme are described. The use of similar reports makes it possible to compare results between evaluators and between evaluated components.

However, only the basic framework is offered; the contents SHOULD reappear in the evaluators' reports. The exact structure of the individual documents is not provided here.

5.2 Evaluation Summary

- Reviewing component specification with regards to completeness and correctness;
- configuration(s) of the tested component;
- test setup;
- untested functionalities (out of scope).

5.3 Design Documentation

- Results of the design documentation evaluation.

5.4 User Documentation

- Results of the user documentation evaluation.

5.5 Results of the Conformity Assessment

- Detailed test results;
- summary of the test results.

5.6 Vulnerability Analysis

- Identified vulnerabilities;
- vulnerability assessment;
- description of the remaining vulnerabilities.

5.7 Overall Assessment

- Summary of the test results;
- evaluation facilities verdict, i.e. a summary of compliance with all requirements;
- evaluation facilities recommendations (i.e. pertaining to vulnerabilities).

6 Appendix C (Normative) – Acceptance Criteria

6.1 Preliminary Note

The acceptance criteria are primarily worded in a positive way (“accept”). In some cases, however, an explicit exclusion of an implementation is sensible for accentuation. These criteria are specified under “not accept”.

6.2 FR-1: Identification and Authentication Control

ID	Requirement	SL-1	SL-2	SL-3
CR 1.1	Human user identification and authentication	Accept: - authentication of human users on all interfaces with human access	Accept: - unique authentication for every human user on all interfaces, for example with username and password	Accept: - capability to employ multifactor authentication for all human user access to the component
CR 1.2	Software process and device identification and authentication	no requirements	Accept: - the component identifies itself and authenticates to any other component using passwords, tokens or location (physical or logical) - authentication mechanism is capable to prevent attacks like man-in-the-middle or message spoofing	Accept: - uniquely identify and authenticate itself to any other component Not accept: - unencrypted authentication and identification - no recommended encryption (e.g. BSI TR-02102)

CR 1.3	Account management	Not relevant if only one fixed administrative account is implemented on the component. Accept: - capability to integrate into a higher level account management system - account management capability (only by authorized users, including adding, activating, modifying, disabling and removing accounts) - the core functionality of the component is not affected by an availability problem of the higher-level system Not accept: - no capability to enable/disable accounts	no additional requirements	no additional requirements
CR 1.4	Identifier management	Not relevant if only one fixed administrative account is implemented on the component. Accept: - capability to integrate into a system that supports management of identifiers - provide the capability to support the management of identifiers by user, group, role or control system interface	no additional requirements	no additional requirements

CR 1.5	Authenticator management	Accept: - support of (initial) authenticator content (tokens, symmetric keys, private keys, biometrics, passwords, key cards) - enforced change of default authenticators after installation or recognition of unchanged default authenticator (combined with warning message) - periodic change of authenticators - protection of unauthorized disclosure or modification of authenticators (when stored, used, transmitted) Not accept: - transmission of cleartext passwords	no additional requirements	Accept: - authenticators are protected via hardware mechanisms (e.g. Password protected memory, OTP memory, hardware data integrity checks, and device security boot mechanism) Not accept: - no hardware protection mechanism
CR 1.6	Wireless access management	Network Component Requirement Accept: - capability to identify and authenticate all users (human, software processes and devices) engaged in wireless communication	Accept: - capability to uniquely identify and authenticate all users (human, software processes and devices) engaged in wireless communication	no additional requirements

CR 1.7	Strength of password-based authentication	Accept: - enforce configurable password strength based on minimum length and variety of character types - configurable password strength according to internationally recognized and proven password guidelines, e.g. NIST SP800-63-2, BSI TR-02102 - external authentication	no additional requirements	Accept: - 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 accept: - no configurable options for reusing passwords, i.e. password reuse cannot be prevented - no minimum and maximum lifetime restrictions for human user passwords
CR 1.8	Public key infrastructure certificates	no requirements	Relevant if PKI or public keys are in use. Accept: - 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")	no additional requirements

CR 1.9	Strength of public key authentication	no requirements	Relevant if PKI or public keys are in use. Accept: - 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 - algorithms and keys comply with CR 4.3	Accept: - protect the relevant private keys via hardware mechanisms (e.g. smart cards) Not accept: - no additional protection mechanisms
CR 1.10	Authenticator feedback	Accept: - sensitive data concerning the authentication process is obscured Not accept: - feedback not distinguish between wrong password or wrong username - no timing differences for error and no error response - displaying password, wireless key, SSH token in input field instead of asterisks - usage of WEP	no additional requirements	no additional requirements

CR 1.11	Unsuccessful login attempts	Accept: - capability to enforce, for each user type (human, software, device), a configurable limit of consecutive invalid access attempts performed in a configurable time period - capability to deny access for a specified period of time or until unlocked, when limit reached	no additional requirements	no additional requirements
CR 1.12	System use notification	Accept: - capability to display a system use notification message before authenticating to the local user interface - capability as an authorized user to configure the message	no additional requirements	no additional requirements
CR 1.13	Access via untrusted networks	Network Component Requirement Accept: - monitor and control all methods of access to the network device via untrusted networks (dial-up, office network, remote access) Not accept: - access to the network device cannot be monitored / controlled - untrusted network is missing in monitoring or cannot be	no additional requirements	Accept: - 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
CR 1.14	Strength of symmetric key-based authentication	no requirements	Relevant if symmetric key authentication (e.g. pre-shared-secrets) is used. Accept: - validate shared secret to establish the mutual trust - authentication is valid as long as shared secret remains a secret, i.e. secrets are stored securely - restrict access to the shared secret	Accept: - control system provides the capability to protect the relevant shared keys via hardware mechanisms

			- ensure that the algorithms and keys used comply with CR 4.3 (Use of cryptography)	

6.3 FR-2: Use Control

ID	Requirement	SL-1	SL-2	SL-3
CR 2.1	Authorization enforcement	Accept: - authorization mechanism is enforced on all interfaces which can accessed by human users based on their responsibilities, as dictated by the least privilege principle Not accept: - interface without authorization mechanism (e.g. HMI, web interface, console)	Accept: - 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 Not accept: - interface without authorization mechanism (e.g. HMI, web interface, console) - user with access to HMI can log in via console or SSH	Accept: - capability to configure a time or sequence of events during supervisor override without closing the current session Not accept: - no possibility to configure supervisor override
CR 2.2	Wireless use control	Accept: - capability to deny critical action via wireless connection (i.e. only use wired) - monitor devices	no additional requirements	no additional requirements
CR 2.3	Use control for portable and mobile devices	no requirements	no additional requirements	no additional requirements

CR 2.4	Mobile code	Only relevant if components allows to execute mobile code. Accept: - capability to enforce a security policy for the usage of mobile code - control execution of mobile code - define which users are allowed to transfer mobile code to/from device	Accept: - provides the capability to verify the integrity of the mobile code before execution is allowed Not accept: - execution is allowed without verifying the integrity of the mobile code	no additional requirements
		Embedded Component Requirements - only upload to device - perform integrity checks on the code prior to code execution - perform authenticity checks to verify origin prior to code execution		
CR 2.5	Session lock	Accept: - for HMI (local or via network): - Session Lock after configurable time period of inactivity - option to explicitly disable Session Lock (e.g. in control room scenarios) - manual session lock - access to session only possible using authentication procedures - comply with session locks requested by the underlying infrastructure (operating system, control system)	no additional requirements	no additional requirements
CR 2.6	Remote session termination	no requirements	Remote session is interpreted as logical network session. Accept: - remote session terminated by user who initiated session (minimum requirement) - remote session manually terminated by a local authority/user	no additional requirements

			- remote session terminated after configurable inactive period of time	
CR 2.7	Concurrent session control	no requirements	No requirements	Accept: - ability to limit the number of session per interface for any user Not accept: - Sessions cannot be limited per interface - Sessions cannot be limited per user
CR 2.8	Auditable events	Accept: - 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 - audit records include at least the following information: timestamp, source, category, type, event ID, event result	no additional requirements	no additional requirements
CR 2.9	Audit storage capacity	Accept: - capability to allocate audit record storage Not accept: - failure of audit functionality when a threshold is reached or the storage capacity is exceeded	no additional requirements	Accept: - a warning message informs when a configurable threshold is reached Not accept: - no warning is produced if the used storage capacity reaches the threshold - the threshold is not configurable
CR 2.10	Response to audit processing failures	Accept: - no loss of essential services or functions during an audit processing failure	no additional requirements	no additional requirements

		- optional support of appropriate actions in response to an audit processing failure - e.g. alerting personnel could be an appropriate action		
CR 2.11	Timestamps	Accept: - ability to generate timestamps for audit records (see CR 2.8) - timestamps include date and time	Accept: - synchronized timestamps - e.g. external source like NTP server	no additional requirements
CR 2.12	Non-repudiation	Relevant if HMI is used. Accept: - possibility to determine which human user took a particular action - logging user id in audit trail	no additional requirements	no additional requirements
CR 2.13	Use of physical diagnostic and test interfaces	No requirements	Exempt are 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 standard. Accept: - prevent unauthorized use of the physical factory diagnostic and test interfaces, e.g. JTAG - disabled diagnostic and test interface based on removed external connectors Not accept: - any diagnostic and test interface without authorization	Accept: - provides active monitoring of the device's diagnostic and test interfaces - generate log entry when attempts to access these interfaces are detected Not accept: - disabled diagnostic and test interface based on removed external connectors

Table 7

6.4 FR-3: System Integrity

ID	Requirement	SL-1	SL-2	SL-3
CR 3.1	Communication integrity	Accept: - capability to protect integrity of transmitted information - use of CRC (protection against casual or coincidental manipulation) - use of standardized cryptographic protocol - use of recommended protocols (e.g. BSI TR-02102), see CR4.3	Accept: - capability to authenticate information during communication Not accept: - use of error detection codes, weak hashing or weak signature functions - authentication of information is not possible - fallback to not recommended protocols	no additional requirements
CR 3.2	Protection from malicious code	Software Application Component Accept: - list at least one compatible security component which implements the protection functionality (user documentation requirement)	no additional requirements	no additional requirements
		Embedded Component Accept: - capability to protect from installation and execution of unauthorized software - environment is allowed to provide malicious code protection mechanism, has to be required by component intended -use description (user documentation requirement) - allowed detection techniques: binary integrity, attributes monitoring, hashing, signature techniques - allowed prevention techniques (e.g. removable media control, sandbox techniques, specific computing platforms mechanisms (e.g. restricted firmware	no additional requirements	no additional requirements

		update), No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection. mandatory access controls) Not accept: - reference to IACS capabilities which are not implemented by the component itself		
		Host Component Accept: - need to support the use of malicious code protection (design documentation requirement)	Accept: - able to automatically report version of the malicious code protection which is actually in use	no additional requirements
		Network Component Accept: - provided by the network device directly - allowed to use compensating control	no additional requirements	no additional requirements
CR 3.3	Security functionality verification	Accept: - definition of (manual) verification procedures for verifying the security functionality - guidance on how to test security functionality (documentation requirement) - documented side effects if these verification procedures are running during normal operation Not accept: - no possibility to test security functionality, e.g. no log message, no notification	no additional requirements	no additional requirements

CR 3.4	Software and information integrity	Accept: - integrity check of data at rest (e.g. software, configuration) - capability to be integrated into a system that can perform or support integrity checks Not accept: - no recording of results of checks	Accept: - authenticity check of data at rest (e.g. software, configuration)	Accept: - unauthorized change is reported to a configurable entity upon discovery of the attempt
CR 3.5	Input validation Note: Not-accept-criteria give guidance which insufficient input validation methods are most relevant for the SL levels to plan test cases with reasonable effort.	Accept: - every input, that directly impacts the action of the application or device is validated for syntax and content Not accept: - out-of-range values for a defined field type - invalid characters in data fields - missing or incomplete data and buffer overflow	Not accept: - SQL injection attacks - cross-site scripting - commonly known malformed packets	Not accept: - malformed packets as commonly generated by protocol fuzzers
CR 3.6	Deterministic output	Applicable if device directly controls a process. Accept: - the deterministic output needs to be documented (documentation requirement) - in case of failsafe, allowed to demonstrate by described process	no additional requirements	no additional requirements
CR 3.7	Error handling	Accept: - error conditions are identified and handled - no unintended information is leaked - no security relevant information is visible	no additional requirements	no additional requirements

CR 3.8	Session integrity	no requirements	Accept: - use of mechanisms to protect the integrity of communication sessions - sessions are invalidated after termination - sessions are invalidated after reboot - use of unique session IDs Not accept: - session hijacking - man in the middle attack - insertion of false information into a session - replay attacks	no additional requirements
CR 3.9	Protection of audit information	no requirements	Accept: - protect audit information and audit tools (if present) Not accept: - unauthorized access, modification or deletion of audit information	no additional requirements
CR 3.10	Support for updates	Accept: - capability to be updated and upgraded once commissioned - if component supports or executes essential functions, needs for mechanism to support patching and updating without impacting the essential function	Accept: - the authenticity and integrity of any update is validated prior installation	no additional requirements
CR 3.11	Physical tamper resistance and detection	no requirements	Not relevant in case of software applications. Relevant if intended use does not offer physical protection of component according to threat modelling. Accept: - anti-tamper resistance: specialized materials to make tampering difficult; e.g.: hardened enclosures, locks, encapsulation, security screws - detection mecha-	Accept: - capability to automatically notify upon discovery of an attempt to make an unauthorized physical access

			nisms for unauthorized physical access into the device, e.g. seal	
CR 3.12	Provisioning product supplier roots of trust	no requirements	Not relevant in case of software applications. Accept: - provision of product supplier keys and roots of trust during device manufacturing - e.g. cryptographic hashes or public key used for verification Fail: - keys or root of trust can be manipulated or leaked	no additional requirements
CR 3.13	Provisioning asset owner roots of trust	no requirements	Not relevant in case of software applications. Relevant if CR 2.4 Mobile Code is selected. Accept: - capability to provision asset owner roots of trust - 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
CR 3.14	Integrity of the boot process	Not relevant in case of software applications. Accept: - integrity verification of boot process relevant firmware, software and configuration data prior to the use	Accept: - authentication verification of boot process relevant firmware, software and configuration data prior to the use - use of product suppliers roots of trust for verification	no additional requirements

Table 8

6.5 FR-4: Data Confidentiality

ID	Requirement	SL-1	SL-2	SL-3
CR 4.1	Information confidentiality	Accept: - capability to protect against unauthorized disclosure of information via **eavesdropping or casual exposure** - capability to protect the confidentiality of information at rest for which explicit read authorization is supported - protection of the confidentiality of information in transit - (wireless) use of encryption Not accept: - outdated or deprecated encryption protocols - use of cleartext protocols (e.g. FTP)	Accept: - capability to protect against unauthorized disclosure of information caused by an attacker actively searching for vulnerabilities with **low resources, generic skills and low motivation**	Accept: - 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**
CR 4.2	Information persistence	no requirements	Accept: - capability to purge component - capability to erase all information with explicit read authorization Not accept: - existence of data after component was decommissioned	Accept: - capability to protect against unauthorized and unintended information transfer via volatile shared memory resources - capability to verify that the erasure of information occurred effectively
CR 4.3	Use of cryptography	If cryptography is required by CR 1.14, CR 3.1 and CR 4.1. Accept: - use of standardized cryptographic protocol - use of recommended protocols (e.g. BSI TR-02102), see CR4.3 - used according to proven practic-	no additional requirements	no additional requirements

		es or documentation		

Table 9

6.6 FR-5: Restricted Data Flow

ID	Requirement	SL-1	SL-2	SL-3
CR 5.1	Network segmentation	Network Component Requirement Accept: - support of network segmentation, e.g. multiple network cards, VLANs - network configuration with routing and router capability	no additional requirements	no additional requirements
		Non-Network Component Requirement Not Accept: - component opens or requires network connections that make a network segmentation non-feasible or hard to maintain		

CR 5.2	Zone boundary protection	Network Component Requirement Accept: - capability to monitor and control communication at zone boundaries to enforce compartmentalization defined in risk-based zones and conduits model Not accept: - demonstrate insufficient boundary protection	Accept: - capability to deny network traffic by default - allow network traffic by exception	Accept: - capability to prevent any communication through the control system boundary (island mode) - 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)
CR 5.3	General purpose person-to-person communication restrictions	Accept: - 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) - e.g. filtering traffic with packet filters or application-level gateways Not accepted: - no/insufficient traffic inspection	no additional requirements	no additional requirements

Table 10

6.7 FR-6: Timely Response to Events

ID	Requirement	SL-1	SL-2	SL-3
CR 6.1	Audit log accessibility	Accept: - capability for authorized humans or tools to access audit logs on a read only basis - web interface (audit perspective) - console tools (separate information system for audit access) Not accepted: - audit logs are accessible to unauthorized users	no additional requirements	Accept: - programmatic access to audit records by either using an application programming interface (API), or - capability to send the audit logs to a centralized system
CR 6.2	Continuous monitoring	no requirements	Accept: - capability to provide an active interface for continuous monitoring, or - capability to send continuous monitoring information to a centralized system	no additional requirements

Table 11

6.8 FR-7: Resource Availability

ID	Requirement	SL-1	SL-2	SL-3
CR 7.1	Denial of service protection	Accept: - capability to operate in a degraded mode (essential functions) during a DoS event	Accept: - Manage communication load from application or device to mitigate effects of DoS events - e.g. limit network capacity of interfaces	no additional requirements

CR 7.2	Resource management	Accept: - capability to limit the use of resources by (active running) security functions to prevent resource exhaustion - e.g. software process prioritization, network traffic rate limiting	no additional requirements	no additional requirements
CR 7.3	Control system backup	Accept: - shall provide backup abilities to safeguard application/device state (user- and system-level information) - Backup Process does not affect normal operation Not accept: - no / insufficient backup abilities - normal operation is affected by control system backup	Accept: - capability to verify the reliability of backup mechanism - e.g. verify backup data mechanism, integrity of backed up information is validated prior to restoring it	no additional requirements
CR 7.4	Control system recovery and reconstitution	Accept: - capability to recovery and reconstitute to a known secure state after disruption or failure - system parameters (either default or configurable) are set to secure values - security-critical patches are reinstalled - security-related configuration settings are re-established - system documentation and operating procedures are available - components are reinstalled and configured with established set-	no additional requirements	no additional requirements

		tings - recovery uses a backup selected explicitly by an authorized person or the recovery uses an internal authentic backup source		
CR 7.5	Emergency power	no requirements	no additional requirements	no additional requirements
CR 7.6	Network and security configuration settings	Accept: - network and security configurations can be configured (as described in guidelines provided by the control system supplier) - component provides an interface to the deployed network and security configuration settings Not accept: - missing related guideline - insufficient description of configurations	no additional requirements	Accept: - capability to generate a report listing the currently deployed security settings in a machine-readable format
CR 7.7	Least functionality	Accept: - capability to restrict the use of unnecessary functions, ports, protocols and/or services (security-by-configuration) - functions beyond a baseline configuration should be able to be deactivated	no additional requirements	no additional requirements
CR 7.8	Control system component inventory	no requirements	Accept: - capability to support a control system component inventory - e.g. vendor-specific management-system or standard-based inventory systems (e.g. with SNMP support) - capable to monitor device ID and status	no additional requirements

Table 12

7 Appendix D (Informative) – Vulnerability Assessment Methods

7.1 Introduction

The evaluation step "Vulnerability Analysis" involves the assessment of possible attacks in regards to the chosen security level (attack resistance). No mandatory assessment model is provided in this evaluation method. The requirements of the assessment model can be found in Chapter 2.6.
In the following, the assessment model according to the [CEM] methodology is explained which complies with all requirements for a vulnerability assessment.

7.2 AVA/CEM Assessment

As an assessment model, the "Vulnerability Assessment (AVA)" methodology from the Common Evaluation Methodology [CEM] or the ISO/IEC 18045 [ISO18045] has proven of worth. When used in the context of the IEC 62443, an adapted version must be used in order to utilise the defined security levels. This adapted version is described in the following.
The method does not aim to identify vulnerabilities or attacks, only to assess describable attack vectors.

In order to apply the methodology to the IEC 62443, the security levels must be adapted to the numerical values of the [CEM]. This is done in the following table:

Security Level	Sufficient Resistance Threshold	Annotation
SL-1	> 0	The assumed attack potential only applies to non-targeted attacks; this, on the other hand, means that found vulnerabilities have to violate an explicit requirement (CR) in order to be rated SL-1.
SL-2	> 4	A low attack potential essentially means that time is the deciding factor, the assumed threshold is less than 1 month of attack time for design and execution combined. One month is valued with 4 points, see [CEM] Appendix B.
SL-3	> 14	The assumed medium attack potential has a minimum value of 14 points, this results from an attack time of two months (7 points), either further expertise (3 points) or access to restricted data (also 3 points), plus specialised equipment (4 points). This adds up to 14 points, see [CEM] Appendix B.
SL-4	-	Not relevant for this version of the evaluation method.

Table 5

The following characteristics are used as a basis for a complete attack:

- time needed (both for the design and for the execution of the attack);
- expertise;
- knowledge of the component (e.g. is it accessible by the public or only by the development team);
- window of opportunity;
- attacker's equipment.

The column "Sufficient Resistance Threshold" is to be understood insofar as that a describable attack SHALL lie above said threshold in order for the component with a certain SL level to be identified as sufficiently resistant.

Each assessment criterion rating is valued with a number of points, which are then summed up and compared with a reference value. These points are explained in detail in Appendix B of the [CEM].

7.3 Assessment Example according to AVA/CEM

As an example, the following scenario is considered. The component interface is SSH (Secure Shell) with a password authentication. A password with at least four characters is chosen (no further restrictions), the number of possible authentication attempts is not limited. On the basis of this scenario, an attack can be designed by trying to guess the password of a user account with an SSH-brute-forcing tool, e.g. Hydra. In a LAN environment, for example, 180 SSH authentication attempts per minute are possible, such or similar values can be determined in lab situations.

Further assuming that the password which is to be guessed indeed consists of four characters including lower-case and upper-case letters and numbers, 62^4 different passwords are possible. Given the previously mentioned brute-forcing rate, such an attack could be executable in under 23 hours, plus some effort for design and execution of the attack. This results in an overall time expenditure of little more than a day.

Estimating the basic attack parameters via the classification numbers from the [CEM] yields the following table:

Category	**Basis**	**Value According to [CEM]**	**Points According to [CEM]**
Time needed	More than a day, less than a week	<= one week	1
Expertise	Attack tools are publicly documented in many examples	Layman	0
Knowledge of the component	SSH is a protocol documented per RFC, an open port can be detected via a network portscan	Public	0
Window of opportunity	This depends largely on the intended use; if no restrictions have been defined, there are no limitations	Unnecessary/unlimited access	0
Equipment	The Hydra tool is publicly available and easily accessible	Standard	0

Table 6

This results in a total number of 1 point. In this example, the component’s resistance would not be sufficient for qualifying for SL-2, i.e. the vulnerability analysis would in this case yield a negative test result.

8 Appendix E (Informative) – Overview of Reuse of Deliverables from IEC 62443-4-1 Development Process

Practice 1	**Security Management**	**Evaluation Method Application**
SM-1	Development process	none[1]
SM-2	Identification of responsibilities	none
SM-3	Identification of applicability	none
SM-4	Security expertise	none
SM-5	Process scoping	none
SM-6	File integrity	Design documentation, see 2.3
SM-7	Development environment security	none
SM-8	Controls for private keys	none
SM-9	Security requirements for externally provided components	Design documentation, see 2.3
SM-10	Custom development components from third-party suppliers	Design documentation, see 2.3
SM-11	Assessing and addressing security-related issues	none
SM-12	Process verification	none
SM-13	Continuous improvement	none
Practice 2	**Specification of Security Requirements**	
SR-1	Product security context	Intended use verification, see 2.2
SR-2	Threat model	Intended use verification, see 2.2 Vulnerability analysis, see 2.6
SR-3	Product security requirements	Conformity assessment, see 2.5
SR-4	Product security requirements content	Intended use verification, see 2.2
SR-5	Security requirements review	Conformity assessment, see 2.5, role of tester
Practice 3	**Secure by Design**	
SD-1	Secure design principles	Implemented security properties on interfaces, concerning design documentation, see 2.3
SD-2	Defense-in-depth design	Vulnerability analysis, see 2.6
SD-3	Security design review	Implemented security properties (details required for SL-3 and higher), concerning design documentation, see 2.3
SD-4	Secure design best practices	Implemented security properties (details required for SL-3 and higher), concerning design documentation, see 2.3
Practice 4	**Secure Implementation**	
SI-1	Security implementation review	none
SI-2	Secure coding standards	none
Practice 5	**Security Verification and Validation Testing**	
SVV-1	Security requirements testing	Conformity assessment, see 2.5
SVV-2	Threat mitigation testing	Vulnerability analysis, see 2.6
SVV-3	Vulnerability testing	Vulnerability analysis, see 2.6
SVV-4	Penetration testing	Vulnerability analysis, see 2.6
SVV-5	Independence of testers	Vulnerability analysis, see 2.6

[1] “*none”* means that no direct deliverables can be gained from the product or the design documents.

		Conformity assessment, see 2.5
Practice 6	**Management of Security-Related Issues**	
DM-1	Receiving notifications of security-related issues	none
DM-2	Reviewing security-related issues	none
DM-3	Assessing security-related issues	none
DM-4	Addressing security-related issues	none
DM-5	Disclosing security-related issues	none
DM-6	Periodic review of security defect management practice	none
Practice 7	**Security Update Management**	
SUM-1	Security update qualification	none
SUM-2	Security update documentation	User documentation, see 2.4
SUM-3	Dependent component or operating system security update documentation	User documentation, see 2.4
SUM-4	Security update delivery	none
SUM-5	Timely delivery of security patches	none
Practice 8	**Security Guidelines**	
SG-1	Product defense-in-depth	User documentation, see 2.4
SG-2	Defense-in-depth measures expected in the environment	User documentation, see 2.4
SG-3	Security hardening guidelines	User documentation, see 2.4
SG-4	Secure disposal guidelines	User documentation, see 2.4
SG-5	Secure operation guidelines	User documentation, see 2.4
SG-6	Account management guidelines	User documentation, see 2.4
SG-7	Documentation review	User documentation, see 2.4

9 Appendix F (Informative) – Overview of Standard Amendments

In the long run, the evaluation method aims to make no additional requirements to those already defined in the standard.

For the evaluation itself, considering the current status of the standard parts IEC 62443-4-2 and IEC 62443-4-1, further details are needed in order to perform comparable evaluations. Therefore, specified requirements are defined in this document, which are listed below:

- component specification according to Appendix A;
- acceptance criteria according to Appendix C:
  - modified acceptance criteria compared to CR of the standard part IEC 62443-4-2:
    - CR 3.5: Complexity of the referenced methods in relation to security levels;
    - CR 4.1: Increasing mechanism strength of the used methods based on the security level (attack resistance);
    - CR 5.1: Differentiation between network component and other component types;
- requirements (CR) which have no graded requirements (i.e. RE, requirement enhancements) for the different security levels (attack resistance) need an appropriate implementation which is reflected in the acceptance criteria (e.g. CR 4.1), see Chapter 2.3.

10 List of Abbreviations

Abbreviation	Meaning
CVSS	Common Vulnerability Scoring System
EDR	Embedded Device Requirement
DM	Defect management (abbreviation from IEC 62443-4-1)
PKI	Public Key Infrastructure
SD	Security by design (abbreviation from IEC 62443-4-1)
SG	Security guidelines (abbreviation from IEC 62443-4-1)
SI	Security implementation (abbreviation from IEC 62443-4-1)
SM	Security management (abbreviation from IEC 62443-4-1)
SR	Security requirements (abbreviation from IEC 62443-4-1)
SUM	Security update management (abbreviation from IEC 62443-4-1)
SVV	Security verification and validation testing (abbreviation from IEC 62443-4-1)

11 Bibliography

[IEC62442-3-3] IEC 62443-3-3:2013

[IEC62442-4-1] IEC 62443-4-1:2018

[IEC62442-4-2] IEC 62443-4-2:2019

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004

[Dakks] Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443, 71 SD 2 019, Revision: 1.0, 05.03.2018

[ISO18045] ISO/IEC 18045:2008, Information technology - Security techniques - Methodology for IT security evaluation, 2014-01, Edition 2

[OD-2061] IECEE Industrial Cyber Security Program, OD-2061, Edition 1.1, 05.06.2018

IT Security Association Germany (TeleTrusT)

The IT Security Association Germany (TeleTrusT) is a widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users, researchers and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the IT expert certification schemes "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) and provides the trust seal "IT Security made in Germany". TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Contact:

IT Security Association Germany (TeleTrusT)
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.

TeleTrusT
Pioneers in IT security.