Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IEC 62443-4-2 Use Case

Template

2021

Danksagung

TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung an dieser Handreichung.

Projektleitung

Sebastian Fritsch, secuvera GmbH

Autoren und mitwirkende Experten

Fritsch, Sebastian - secuvera GmbH
Fuß, Andreas - Phoenix COntact Electronics GmbH
Güntner, Josef - TÜV SÜD Industrie Service GmbH
Jänicke, Lutz - Phoenix Contact GmbH & Co. KG
Menge, Stefan - AchtWerk GmbH & Co. KG
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried - MB connect line GmbH
Negrea, Dan-Mihai - SICK AG
Pfendtner, Steffen - ads-tec IT GmbH
Schmierer, Marc - ads-tec IT GmbH

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Desweiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

V 2021-02 EN

Table of Contents

1 Scope

A use-case describes a component starting from its intended use and ending up with the acceptance criteria. Although the information presented here may be found in other documents, the added value is represented by the perspective from which the component is described. The result may be a mapping of the IEC 62443-4-2 Component Requirements (CRs) and / or the definition and reasoning of new requirements.

1.1 General Introduction

The main aspect defined in the use-case is the intended use of the component specified in the system context. The component is introduced and specified based on system architectural and functional aspects.

The component includes the scope, product type (according to IEC 62443-4-2), assumptions, threats, and security functionalities. The security requirements are selected based on CRs (component requirements from IEC 62443-4-2) and, if necessary in the use-case, complemented by additional requirements. Additionally, the use-case includes an evaluation specification of the component.

There are different motivations to define use-cases for automation components based on IEC 62443-4-2. One of the most relevant aspects is the drawback of the pre-defined set of four security levels. Those levels, called SL-1 to SL-4, are not specific enough to be easily understood and applicable by different types of users. In this context it is important to realise that there is a wide field of users with different background and experience of the standard or similar concepts.

Especially SL-1 is not accepted by a wide range of users because this security level does not address lowest resistance against attackers.

Another aspect is the non-expandability of the IEC 62443-4-2 component requirements (CRs). The static catalogue of the CRs does not allow for selecting additional component requirements. Additional requirements are introduced in the use-case concept.

1.2 Intended Operational Environment

1.3 Introduction of Use-case Security-Level Capability

In this use-case the following Security-Level are defined:

- Basic
- Extended

1.4 Disclaimers

The IEC 62443 series defines the concept of system and components. System requirements are the security requirements for the whole system (or of one zone of the system). These (technical) system requirements are mapped to component requirements.

Compensating Countermeasures

There might be scenarios where components are not able to fulfil necessary component requirements. For example, in those scenarios a set of security requirements (see Chapter 4) for the component might be required. If a dedicated component does not have the capability to implement all requirements during the implementation, then additional compensating countermeasures have to be defined. Those countermeasures are not part of the component itself. Therefore, these are not part of the use-case definition in this document.

In a second situation, if some necessary security requirement is not mapped to the component defined in the use-case but has to be implemented in the environment of the component, then such an additional

requirement is defined as part of the system architecture and not as compensating countermeasure. One example could be a logging service for a network component which is in general not capable of implementing such a service by itself. In this case the requirement for the environment can be part of the use-case.

2 System Architecture

2.1 Architecture

2.2 Operational Modes/Lifecycle Phases

3 Component Definition

3.1 Component Scope Definition

3.2 Component type

The component type according to IEC 62443-4-2 is Application Component, Embedded Component Host Component or Network Component.

3.3 Component Security Assumptions

The use-case has typical constraints or assumptions which are described in the next paragraphs.

Physical assumptions
e.g. security of operational environment

Logical assumptions
e.g. administrative concepts

Assumptions on integrators
e.g. installation or operational guidelines

Assumptions on supplier
e.g. delivery process

3.4 Component Threats

4 Security Requirements

4.1 Definition of Use-Case Security-Level Capability

The introduction of the Use-Case Security-Level Capability definition is given in Chapter 1.2. The following shows the mapping of level Basic and Extended to the IEC 62443-4-2 security levels.

Table 1 Mapping of Use-Case Security-Level Capability to default IEC 62443 Security Levels

	SL-1	**SL-2**	**SL-3**	**SL-4**
Basic				
Extended				

4.2 Mapping of Component Requirements to Use-Case Security Levels Capability

The following table contains a mapping of the Component Requirements from IEC 62443-4-2 to the defined Use-Case Security-Level Capability in this document.

Table 2 Mapping to IEC 62443-4-2 Component Requirements

	Basic	**Extended**
EXAMPLE		
FR 1 - Identification and authentication control (IAC)		
CR 1.1 - Human user identification and authentication	x	x
CR 1.1 (1) - Unique identification and authentication	x	x
CR 1.1 (2) - Multifactor authentication for all interfaces		x
…		

4.2.1 Rationale/adjustment for not-selected Component Requirements

For all CRs that are not mapped to the standard SLs as defined in IEC 62443-4-2, a rationale is given in the following table.

CR	**Basic**	**Extended**	**Rationale**

4.2.2 Rationale/adjustment for modified Component Requirements

For all CRs that were modified mapped to the standard SLs as defined in IEC 62443-4-2, a rationale is given in the following table.

CR	**Modification**	**Rationale**

4.3 Additional Requirements

The TEMPLATE use-case supports XXX

The additional requirements are listed in Table 4.

Table 3 Additional Requirements Specific for Secure Gateway

Requirement	Basic	Extended
CATEGORY		

5 Evaluation Specification

Comparable evaluation results of components are crucial for buyers of components. To support first-party (self-assessment) and third-party (certification) evaluations, TeleTrusT published the document “Evaluation Method for IEC 62443-4-2" in 2019-05[1]. This document contains guidance for evaluation teams.

The following sections list derivations of the given evaluation methodology or additional guidance for the application.

In this document no guidance for performing penetration tests are given. These have to performed state-of-the-art and in accordance to IEC 62443-4-1 requirements.

5.1 Required Test Environment

5.2 Required Test Interfaces

5.3 Acceptance Criteria

5.3.1 Acceptance Criteria for IEC 62443 4-2 Component Requirements

For the requirements defined in IEC 62443 (see table 4), the corresponding test cases defined in “Appendix C (Normative) – Acceptance Criteria" [TeleTrusT-4-2] apply.

5.3.2 Acceptance Criteria for Additional Requirements

Requirement	Acceptance Criteria
CATEGORY	
	Accept: • XXX Not accept: • XXX

5.4 Test Case Considerations

The following information should be taken into consideration when designing the test cases.

[1] TeleTrusT stopped the maintenance of the document after the first major update in 2019-05. Successor versions of this document will be published by IECEE or IEC in the future.

6 List of Abbreviations

Abbreviation	Meaning

7 Definitions

Term	Definition
Component specification	Instance of use-case for the specific product
Use-Case Security-Level-Capability	Derived Security Level which are specifically applicable for one defined use-case. The specific use-case should be mapped to standard IEC 62443 or at least to Component Requirements (CR) defined in IEC 62443-4-2.

Table 1

8 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

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.