Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IEC 62443-4-2 Use Case

Industrial Firewall

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 Industrial IT GmbH
Schmierer, Marc - ads-tec Industrial 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 2

1.1 General Introduction 2

1.2 Intended Operational Environment 3

1.3 Introduction of Use-Case Security-Level Capability 4

1.4 Disclaimers 4

2 System Architecture 5

2.1 Architecture 5

2.2 Operational Modes/Lifecycle Phases 7

3 Component Definition 8

3.1 Component Scope Definition 8

3.2 Component Type 8

3.3 Component Security Assumptions 8

3.4 Component Threats 9

4 Security Requirements 10

4.1 Definition of Use-Case Security-Level Capability 10

4.2 Mapping of Component Requirements to Use-Case Security-Levels Capability 10

4.2.1 Rationale for Non-Selected Component Requirements 12

4.2.2 Rationale for Modified Component Requirements 13

4.3 Additional Requirements 14

5 Evaluation Specification 15

5.1 Required Test Environment 15

5.2 Required Test Interfaces 15

5.3 Acceptance Criteria 16

5.3.1 Acceptance Criteria for IEC 62443 4-2 Component Requirements 16

5.3.2 Acceptance Criteria for Additional Requirements 16

5.4 Test Case Considerations 16

5.4.1 Packet Filter 16

5.4.2 Configuration Web Interface or API 16

5.4.3 Test Case De-/activate interfaces 17

6 List of Abbreviations 18

7 Definitions 18

8 Bibliography 18

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.

The Use-Case Industrial Firewall defines the widely-used automation or IACS component-type Industrial Firewall as part of an OT network.

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

One of the key challenges in an OT network is the segmentation of operation cells from each other to avoid IP address conflicts. Additionally, communication traffic disturbance or integration issues should be avoided by network segmentation.

The term OT network is equivalent to shop-floor network, production network, machine network, automation network, or industrial ethernet.

In this case, the Industrial Firewall helps to segment those networks. With the help of communication rulesets, it manages traffic between cells and other components, e.g. workstations.

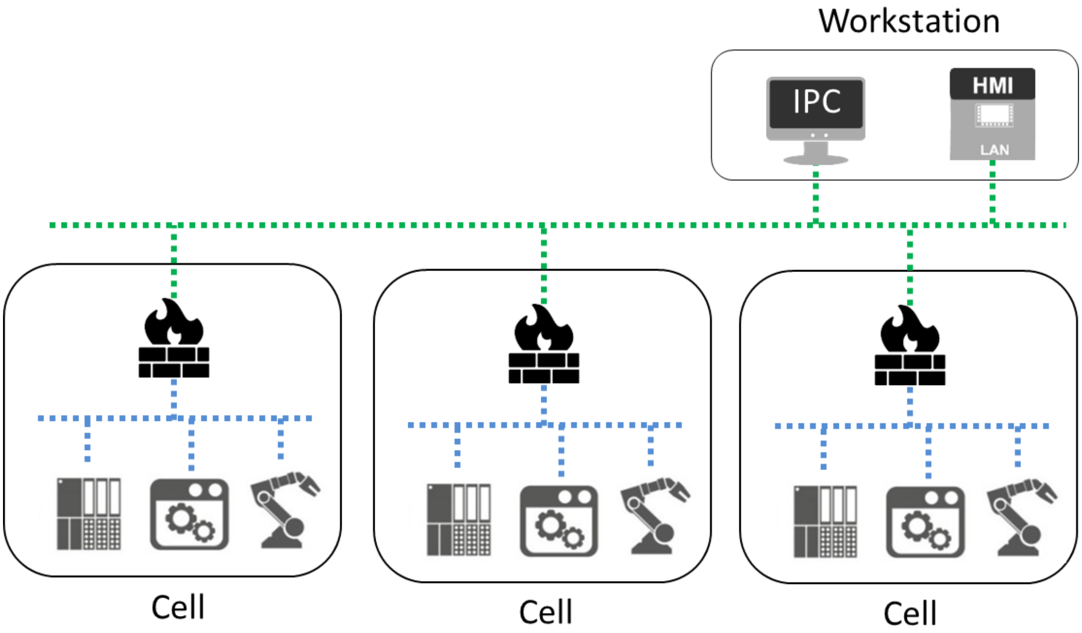

Figure 1 – OT Network

1.3 Introduction of Use-Case Security-Level Capability

In this use-case, the levels *Basic* and *Extended* are defined as Use-Case Security-Level Capabilities. In the following table we summarise the risk and impact for the two levels.

Level	Basic	Extended
Hard Facts to select the level (Must)	No dedicated criteria	• Critical infrastructure • Safety relevant
Soft Facts to select the level (Scenario considerations)	No dedicated criteria	Impact of damage: • High costs • Loss of intellectual property • Loss of reputation

The typical scenario for level Basic is the protected cell of a machine or equipment in production environment and it is not used in a critical infrastructure purpose. For level Basic, also no safety component like Safety Guard System or Safety-PLC is connected to OCTL (OT-Communication-Layer).

The level Extended is defined for critical infrastructure and/or for safety-relevant scenarios. This level might also be relevant for operators with high-cost or high-risk scenarios.

The Extended level is defined for scenarios where safety systems are protected by the firewall or where the whole application is part of a critical infrastructure purpose. In addition, the extended scenario should be used depending on the amount of damage to be expected from an event. Examples of such damages are a danger to life and limb, environmental damage, the loss of intellectual property, the loss of major investments, or the loss of reputation.

Definition of safety-relevant:
If a safety component is connected through OCTL to some cell component, then it is safety-relevant.

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

In an OT environment, a cell consists of IACS components like PLC, HMI, IPC, or motion controller. These components are connected inside a machine network (cell network).

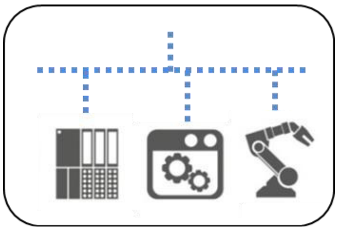

Figure 2 – Cell

Other Components in such an OT network are workstations. Typically, these are HMI, SCADA, MES, BDE, operator interface, industrial PC (IPC), or engineering workstations.

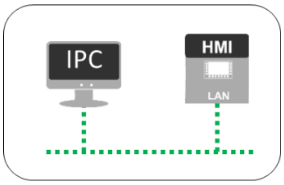

Figure 3 – Workstation

In these environments, the following communication protocols and layers are used. We call those OT-Communication-Layer (OTCL):

- TCP/IP;
- Layer 2 (MAC filter);
- IP network/port.

For this use-case we consider the following items to be out of scope:

- fieldbuses, like EtherNet/IP or PROFINET;
- connectivity to or from a DMZ, other IT networks or from cloud systems.

All those components together give a realistic picture on the design of today’s OT networks.

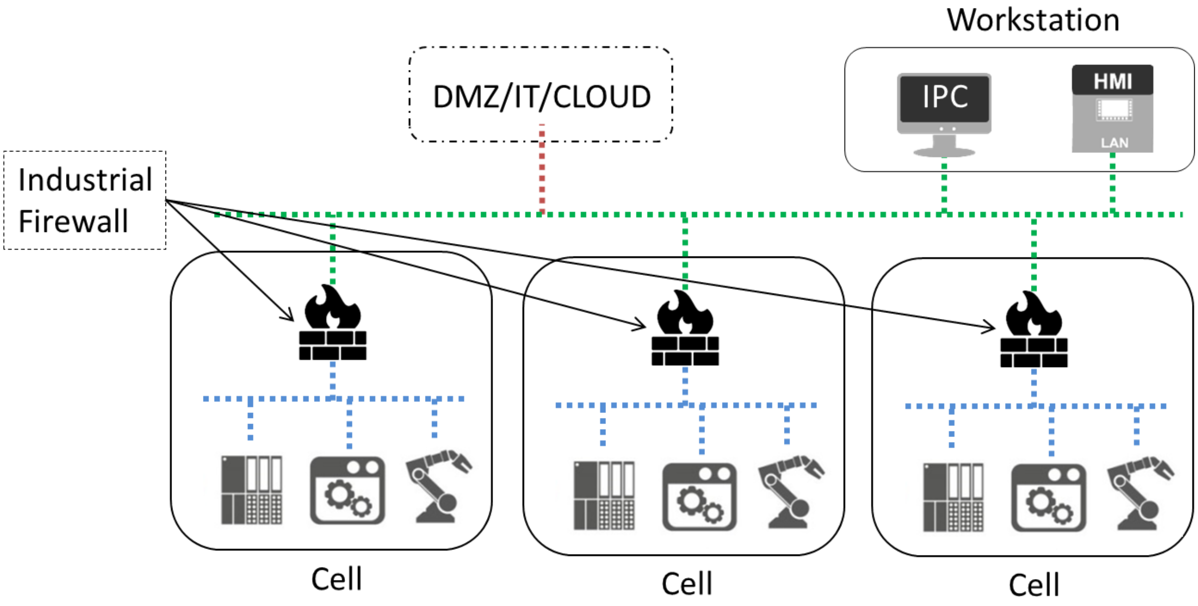

Figure 4 – Typical OT Network

All these components are intended to communicate with each other. For the communication, the described protocols and layers are used.

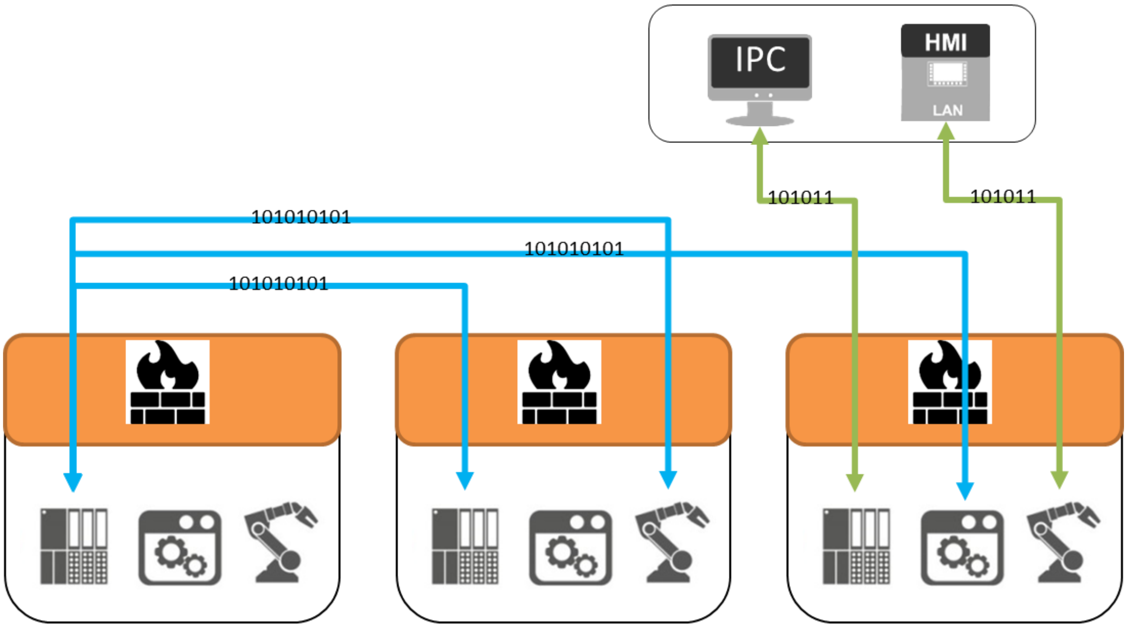

Figure 5 – Communication Structure

There are several scenarios where all these assets need to exchange information via OTCL. In these scenarios TCP/IP-based protocols are used. Such protocols can be filtered with a common packet filter and are routable.

1. Inter-cell communication (Cell-to-cell communication):

In this scenario it is very common that the cells are part of a production line. The purpose for this inter-cell communication is to send data and signals to up-/downstream machines for production coordination. These are a few examples:

- PLCs from different cells communicate with each other to push and poll data from their memory or send/receive commands. Those PLCs use proprietary protocols from the PLC manufacturer. We assume only TCP/IP-based protocols are used.

- A PLC communicates with a robot control system to push and poll data from the memory or send/receive commands. Proprietary protocols from the PLC or robot manufacturer are used. We assume only TCP/IP-based protocols are used.
- A PLC communicates with IPC/HMI to push and poll data from their memory or send/receive commands. Proprietary protocols from the PLC or IPC/HMI manufacturer are used. We assume only TCP/IP-based protocols are used.

2. Communication between cell and workstation:

In this scenario it is very common that the cell is a substation of a larger control system or that the cell is maintained from an engineering station. The purpose is to poll and push data for/back to a BDE/MES system or to diagnose the ICS. Here are a few examples:

- A PLC sends its production data to a BDE/MES system. The PLC uses proprietary protocols from the PLC manufacturer. We assume only TCP/IP-based protocols are used.
- MES/BDE polls data from a PLC. Such a system uses proprietary protocols from the PLC manufacturer. We assume only TCP/IP-based protocols are used.
- An engineering workstation establishes a diagnostic communication channel to one or more of the ICS for maintenance, e.g. program updates, loggings, or remote desktop session via VNC/RDP.

2.2 Operational Modes/Lifecycle Phases

In this use-case we consider two types of cells. The first is called Single Cell. Such a cell is not part of an integrated production line. Those cells are either independent or stand-alone.

The second type of cell is called Multiple Cells. Those cells are part of a production line, which means every cell is communicating with each other.

The main differences of the two cell types are in the design or planning phase. It is obvious that a production line needs planning in advance and therefore the network and communication structure has to be defined before the roll-out or commissioning phase.

Lifecycle phase	Single Cell (Stand-alone/Independent)	Multiple Cells (Production Line)
Design or planning	No knowledge about structure of the cell. Zero trust	Define network structure Define communication rules
Rollout or commissioning	Update to latest version Setup configuration	
In operation	Patching Monitoring Re-configuration	
Decommissioning	Delete configuration Factory reset	

3 Component Definition

3.1 Component Scope Definition

To ensure the reliable functionality described in the previous chapter, the Industrial Firewall also has to provide a set of security functionalities. The following lists the relevant security functions:

- Layer 3 packet filter, IP/port/protocol;
- Stateful Inspection;
- Layer 2 MAC filter;
- Authentication for configuration management;
- Role-based-access for configuration, monitoring, or patching;
- Authentication for configuration API;
- Update capability;
- Integrity of protected firmware and boot-process;
- Security hardening, e.g. disabled interfaces, functions, or configuration interfaces.

These security functions are expressed in terms of IEC 62443-4-2, i.e. component requirements (CR), in Chapter 4.2.

Additional security functions like application level gateway (ALG) or deep package inspection are not mandatory in this use-case. Nevertheless, a component that complies with this use-case can also offer more security functions.

3.2 Component Type

The component type according to IEC 62443-4-2 is a Network Component.

3.3 Component Security Assumptions

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

Physical assumptions
The Industrial Firewall is installed at least in a control cabinet with minimum locking capability. High-resistance protection might be necessary but may depend on a case-by-case analysis, i.e. as a result of a risk assessment. Additional physical access control of the component should be considered if level Extended applies.

Additional physical assumptions might result from the component's intended use, especially based on environmental and electrical conditions.

Assumptions on integrators
The default factory configuration might not follow the principle of security-by-default, i.e. a deny/deny ruleset is not the default configuration. The administrator carefully reads the guidance documents on this aspect.

The Industrial Firewall receives a valid time from an NTP server.

The component should not have any wireless interfaces (e.g. WiFi, Bluetooth). If wireless interfaces are available, those are disabled by configuration.

The component should not have any mobile code functionality (see CR 2.4, e.g. Script-Code or Container-Hosting). If mobile code functionality is available, this is disabled by configuration.

Assumptions on supplier
The component supplier protects private keys for code signing from unauthorised access, modifications, or theft with procedural and technical controls.

3.4 Component Threats

The configuration management interface and configuration APIs are the main attack threat vectors of the Industrial Firewall. If an attacker is able to get access to these interfaces, the configuration of the component is threatened. If the integrity of the configuration is harmed, the correct function of the Industrial Firewall cannot be guaranteed.

The functionality of the Industrial Firewall is limited to ISO/OSI layer 4, but the IP stack has to be robust. Not correctly formatted IP packets might be a direct threat for the IP stack.

The integrity of the Industrial Firewall but also of the processed data is threatened in general. This might lead to integrity violations of the boot process, the firmware (e.g. caused by the update function), configuration, and event log.

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
Basic	x	x	
Extended			x

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

Requirement	Basic	Extended
FR 1 — Identification and Authentication Control (IAC)		
CR 1.01 Human user identification and authentication	x	x
CR 1.01 RE(1) Unique identification and authentication	x	x
CR 1.01 RE(2) Multifactor authentication for all interfaces		
CR 1.02 RE(1) Unique identification and authentication		x
CR 1.03 Account management	x	x
CR 1.04 Identifier management	x	x
CR 1.05 Authenticator management	x	x
CR 1.05 RE(1) Hardware security for authenticators		x
CR 1.06 Wireless access management		
CR 1.07 Strength of password-based authentication	x	x
CR 1.07 RE(1) Password generation and lifetime restrictions for human users		x
CR 1.07 RE(2) Password lifetime restrictions for all users (human, software process, or device)		
CR 1.08 Public key infrastructure certificates		x
CR 1.09 Strength of public key-based authentication	x	x
CR 1.09 RE(1) Hardware security for public key-based authentication		x
CR 1.10 Authenticator feedback	x	x
CR 1.11 Unsuccessful login attempts	x	x
CR 1.12 System use notification	x	x
CR 1.13 Access via untrusted networks	x	x
NDR 1.13 Access via untrusted networks	x	x
NDR 1.13 RE(1) Explicit access request approval		x
CR 1.14 Strength of symmetric key-based authentication		
CR 1.14 RE(1) Hardware security for symmetric key-based authentication		
FR 2 — Use Control (UC)		
CR 2.01 Authorization enforcement	x	x

CR 2.01 RE(1) Authorization enforcement for all users (humans, software processes and devices)	x	x
CR 2.01 RE(2) Permission mapping to roles	x	x
CR 2.01 RE(3) Supervisor override		x
CR 2.01 RE(4) Dual approval		
CR 2.02 Wireless use control		
CR 2.03 Use control for portable and mobile devices		
CR 2.04 Mobile code		
CR 2.05 Session lock	x	x
CR 2.06 Remote session termination	x	x
CR 2.07 Concurrent session control		x
CR 2.08 Auditable events	x	x
CR 2.09 Audit storage capacity	x	x
CR 2.09 RE(1) Warn when audit record storage capacity threshold reached	x	x
CR 2.10 Response to audit processing failures	x	x
CR 2.11 Timestamps	x	x
CR 2.11 RE(1) Time synchronization	x	x
CR 2.11 RE(2) Protection of time source integrity		
CR 2.12 Non-repudiation	x	x
CR 2.12 RE(1) Non-repudiation for all users		
NDR 2.13 Use of physical diagnostic and test interfaces		
NDR 2.13 RE(1) Active monitoring		
FR 3 — System Integrity (SI)		
CR 3.1 Communication integrity	x	x
NDR 3.2 Protection from malicious code		
CR 3.3 Security functionality verification	x	x
CR 3.3 RE(1) Security functionality verification during normal operation		
CR 3.4 Software and information integrity	x	x
CR 3.4 RE(1) Authenticity of software and information	x	x
CR 3.4 RE(2) Automated notification of integrity violations		x
CR 3.5 Input validation	x	x
CR 3.6 Deterministic output		
CR 3.7 Error handling	x	x
CR 3.8 Session integrity	x	x
CR 3.9 Protection of audit information	x	x
CR 3.9 RE(1) Audit records on write-once media		
NDR 3.10 Support for updates	x	x
NDR 3.10 (1) Update authenticity and integrity	x	x
NDR 3.11 Physical tamper resistance and detection	x	x
NDR 3.11 (1) Notification of a tampering attempt		
NDR 3.12 Provisioning product supplier roots of trust	x	x
NDR 3.13 Provisioning asset owner roots of trust	x	x
NDR 3.14 Integrity of the boot process	x	x
NDR 3.14 (1) Authenticity of the boot process	x	x
FR 4 — Data Confidentiality (DC)		
CR 4.1 Information confidentiality	x	x

CR 4.2 Information persistence	x	x
CR 4.2 RE(1) Erase shared memory resources		
CR 4.2 RE(2) Erase verification		x
CR 4.3 Use of cryptography	x	x
CR 5.1 Network segmentation	x	x
FR 5 — Restricted Data Flow (RDF)		
NDR 5.2 Zone boundary protection	x	x
NDR 5.2 (1) Deny all, permit by exception	x	x
NDR 5.2 (2) Island mode		
NDR 5.2 (3) Fail close		
NDR 5.3 General-purpose person-to-person communication restrictions	x	x
FR 6 — Timely Response to Events (TRE)		
CR 6.1 Audit log accessibility	x	x
CR 6.1 RE(1) Programmatic access to audit logs		x
CR 6.2 Continuous monitoring		x
FR 7 — Resource Availability (RA)		
CR 7.1 Denial of service protection	x	x
CR 7.1 RE(1) Manage communication load from component	x	x
CR 7.2 Resource Management	x	x
CR 7.3 Control System backup	x	x
CR 7.3 RE(1) Backup integrity verification	x	x
CR 7.4 Control system recovery and reconstitution	x	x
CR 7.6 Network and security configuration settings	x	x
CR 7.6 RE(1) Machine-readable reporting of current security settings		x
CR 7.7 Least functionality	x	x
CR 7.8 Control system component inventory	x	x

4.2.1 Rationale for Non-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**
CR 1.01 RE(2) Multifactor authentication for all interfaces	N/A	N/A	The component is not connected to the next level of connectivity like IT or Cloud, see definition and note in Chapter 2.1.
CR 1.06 Wireless access management	N/A	N/A	Wireless interfaces are out of scope in this use-case.
CR 1.14 Strength of symmetric key-based authentication	N/A	N/A	No interfaces with symmetric key-based authentication are used in this use-case.
CR 1.14 RE(1) Hardware security for symmetric key-based authentication	N/A	N/A	No interfaces with symmetric key-based authentication are used in this use-case.

CR 2.02 Wireless use control	N/A	N/A	Wireless interfaces are out of scope in this use-case.
CR 2.03 Use control for portable and mobile devices	N/A	N/A	Portable and mobile devices are out of scope in this use-case.
CR 2.04 Mobile code	N/A	N/A	Portable and mobile devices are out of scope in this use-case.
NDR 2.13 RE(1) Active monitoring		N/A	All device's diagnostic and test interfaces are not led to the outside. These interfaces are not used in the actual use-case. Additionally, according to Chapter 3.3, the component is protected at least in a locked control cabinet, therefore NDR 2.13 is considered to be sufficient.
NDR 3.2 Protection from malicious code	N/A	N/A	Mobile code is out of scope in this use-case.
CR 3.6 Deterministic output	N/A	N/A	All device's outputs are only used for outgoing signals. Those signals are not used in any process of the OT network.
CR 4.2 RE(1) Erase of shared memory resources		N/A	Decommission is realised (in most cases) by cutting off power. In this case the non-volatile memory is lost.
NDR 5.2 (2) Island mode	N/A	N/A	Island mode is only relevant for IT networks. This use-case is only focused on OT networks.
NDR 5.2 (3) Fail close	N/A	N/A	This requirement addresses too high demands for the level of security demanded in this use-case, e.g. a redundant implementation of a CPU or a network switch is out of scope in this use-case.

4.2.2 Rationale 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
NDR 2.13 Use of physical diagnostic and test interfaces	Changed from SL-2 to SL-3	According to Chapter 3.3, the component is protected at least in a locked control cabinet.
NDR 3.11 (1) Notification of a tampering attempt	The component shall be protected by a tamper seal.	Modifications of the components could be seen by a broken tamper seal.

	Physical access to the component is restricted in this use-case, see Chapter 3.3.	The seal supports the secure delivery process. Integrators can verify the seal status after unboxing and before commissioning.

4.3 Additional Requirements

The Industrial Firewall use-case supports security-by-default as much as possible. For successful commissioning and user acceptance, this principle may be weakened for the factory default configuration. If this is used, an empty ruleset has to enforce a deny/deny configuration.

The additional requirements are listed in Table 4.

Table 3 Additional Requirements Specific for Secure Gateway

Requirement	Basic	Extended
Ruleset		
RULE 01 – The factory default configuration may allow an allow(out)/deny(in) default ruleset. If no ruleset is configured, the component has to enforce a deny(out)/deny(in) configuration.	x	x

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

For verifying the fulfilment of the IEC 62443-4-2 Component Requirements no special test environment is required. The Industrial Firewall under test can be inspected with the help of two testing workstations configured in two separate networks.

For testing the additional requirements specific for the Industrial Firewall, the required components and a possible high-level architecture for the setup are presented in Figure 6.

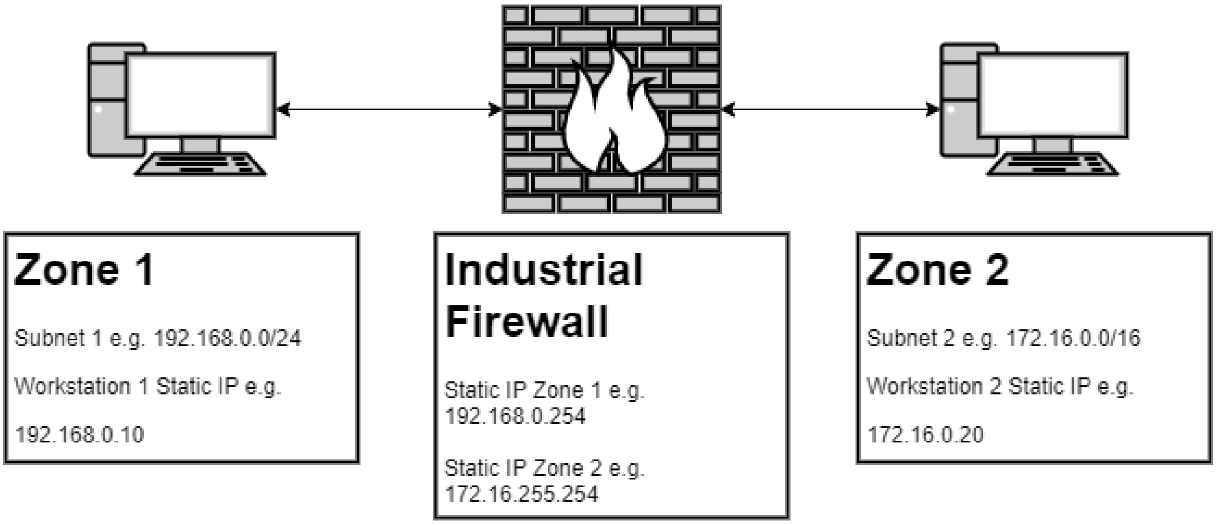
Zone 1
Subnet 1 e.g. 192.168.0.0/24
Workstation 1 Static IP e.g.
192.168.0.10
Industrial Firewall
Static IP Zone 1 e.g. 192.168.0.254
Static IP Zone 2 e.g. 172.16.255.254
Zone 2
Subnet 2 e.g. 172.16.0.0/16
Workstation 2 Static IP e.g.
172.16.0.20

Figure 6 – Test setup with required test environment

5.2 Required Test Interfaces

The conformity testing and the vulnerability analysis should be focused on, at least,

- network interfaces for data flows;
- configuration interfaces, e.g. web interface or API interface.

[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.

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
Communication integrity	
RULE 01 – The factory default configuration may allow an allow(out)/ deny(in) default ruleset. If no ruleset is configured, the component has to enforce a deny(out)/deny(in) configuration.	Accept: • If all rules were flushed, then no network connections router through the component is established. Not accept: • If the component is set to factory reset, then network connects are established between interfaces, except for one documented direction, i.e. only outbound.

5.4 Test Case Considerations

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

5.4.1 Packet Filter

Packet filter function can be checked with network sniffer software like Wireshark installed on the workstations.

If the Industrial Firewall supports Remote Capture Protocol (RPCAP) the traffic can be sniffed on the Industrial Firewall directly.

Scenario 1:

To test the packet filter data flow between zone 1 and zone 2 should be checked with active packet filter (data flow from zone 1 to zone 2 ACCEPT ANY).

Scenario 2:

To test the packet filter data flow between zone 1 and zone 2 should be denied or blocked with active packet filter (data flow from zone 1 to zone 2 DENY/BLOCK Target IP Workstation 2).

5.4.2 Configuration Web Interface or API

Scenario 1:

A Test user should be added in the user management of the Industrial Firewall and should check if the right management works effectively (role-based or individual right management).

Scenario 2:

With such a user the configuration API can be tested if restricted rights are enforced correctly (role-based or individual right management).

5.4.3 Test Case De-/activate interfaces

Scenario 1:

Deactivating the web interface or API for single interfaces and protocols should be tested (e.g. ACCESS only via https on eth2)

Scenario 2:

Deactivation single interfaces on Ethernet / Layer 2 and test physical links.

6 List of Abbreviations

Abbreviation	Description
CR	Component Requirement
IP	Internet Protocol
ICS	Industrial Control System
IACS	Industrial Automation and Control System
MAC	Media Access Control Address
SL	Security Level
OT	Operational Technology
OTCL	Operation-Technology-Communication-Layer

7 Definitions

Term	Definition
Component specification	Instance of use-case for the specific product
Use-Case Security-Level-Capability	Derived security levels 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.

8 Bibliography

[IEC62442-3-3] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

[IEC62442-4-1] IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

[IEC62442-4-2] IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

[TeleTrusT-4-2] TeleTrusT Evaluation Method for 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.