Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IEC 62443-4-2 Use Case

Industrial Remote Access Device

2023

Danksagung

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

Projektleitung

Steffen Heyde, secunet Security Networks AG
Leiter der TeleTrusT-AG "Smart Grids / Industrial Security"

Autoren und mitwirkende Experten

Fritsch, Sebastian - secuvera GmbH
Fuß, Andreas - Phoenix Contact Electronics GmbH
Güntner, Josef - TÜV SÜD Industrie Service GmbH
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried - MB connect line 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 2023-02-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.

The Use case Industrial Remote Access Device defines the widely-used automation or IACS component-type Industrial Remote Access Device as part of an infrastructure to remotely access 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 required by the use case complemented by additional requirements. Additionally, the use case includes an evaluation specification for 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

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

Many of the machines and production lines used in industrial manufacturing are now connected and use remote access functionality over a public network.

The target systems (Cell) are typically connected to the internet via routers (Red Box) to allow remote maintenance. These connections are used to establish a VPN connection to what is called an “RENDEZVOUS SERVER". This intermediate point is the link between the target system and the remote user/workstation which has likewise established a VPN connection to the RENDEZVOUS SERVER. Since both locations have their own connection each participant is able to terminate it at any time. The task of the RENDEZVOUS SERVER in this process is to allow only approved remote users to connect to the approved target system via a REMOTE WORKSTATION. (Quelle: TeleTrusT-Stand der Technik, Fernwartung)

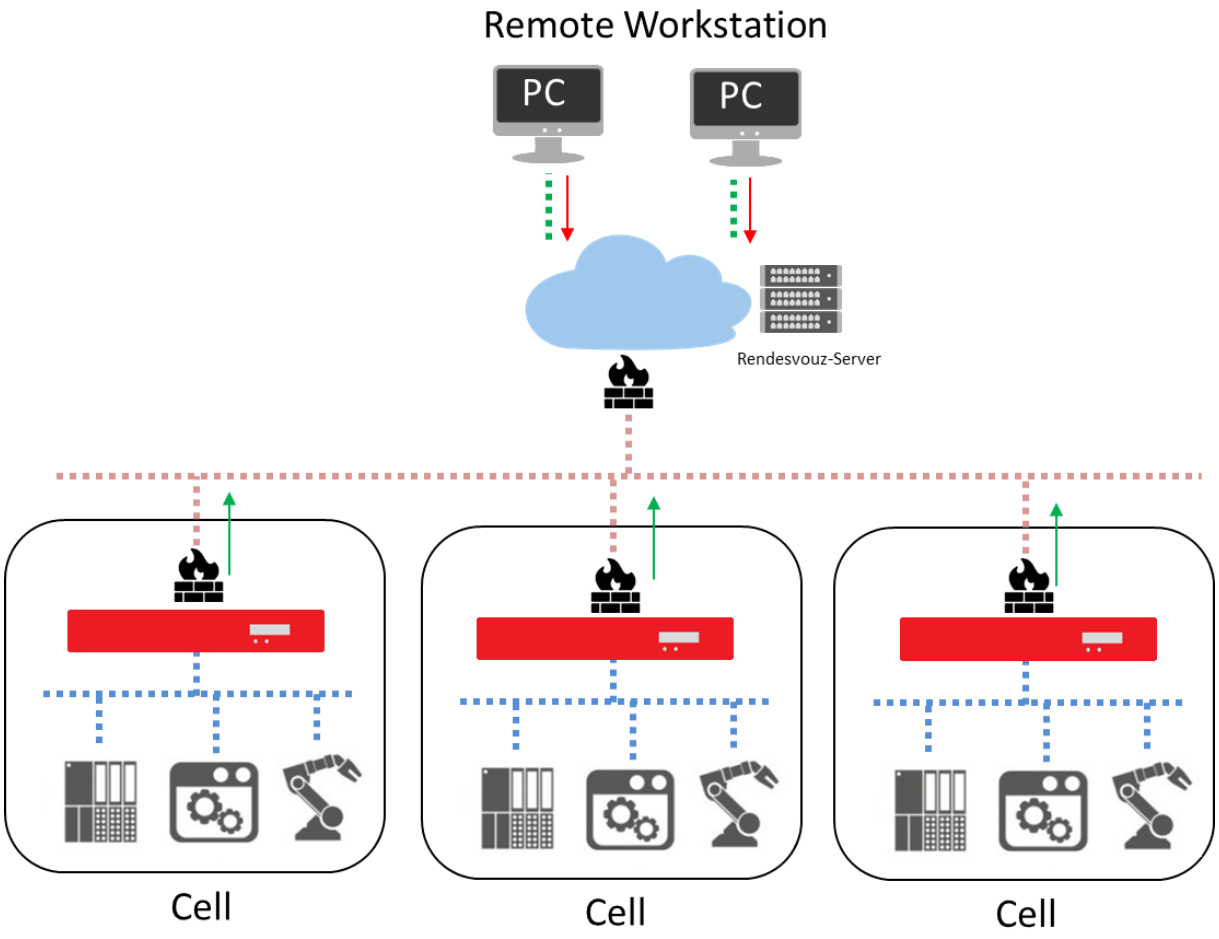

Figure 1: Remote Access to OT Network

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, 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 for 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). The Industrial REMOTE ACCESS DEVICE (red box) is also part of the cell network. For remote access the device should be able to route traffic from the VPN into the cell network. The Industrial Remote Access should also be used as a cell network firewall, see Figure 3.

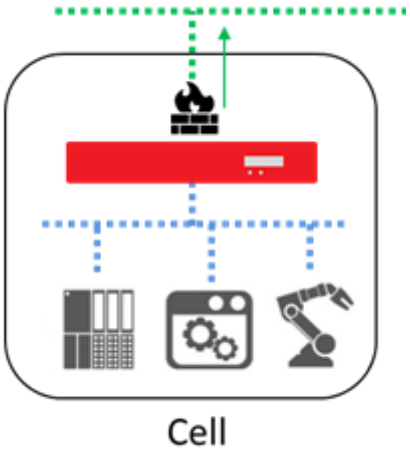

Figure 2 – Cell network with Industrial Remote Access Devices in Firewall Mode

To access the Industrial REMOTE ACCESS DEVICE a PC with an integrated VPN Client should be used. The REMOTE WORKSTATION connects over the internet to the RENDEZVOUS SERVER where a User and Rights management allows to connect to the Industrial REMOTE ACCESS DEVICE and/or the cell network, see Figure 4.

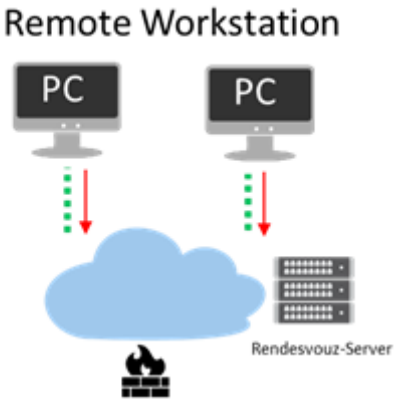

Figure 4 – Remote Workstations connect to the Rendezvous-Server

In these environments, the following communication protocols and layers are used typically:

- TCP
- IP network/port
- IPSec
- UDP
- DNS
- TLS
- HTTPS

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

- fieldbuses, like EtherNet/IP or PROFINET;
- connectivity to or from other IT/OT networks

All those components together give a realistic picture on the design of today's remote access networks, see Figure 5.

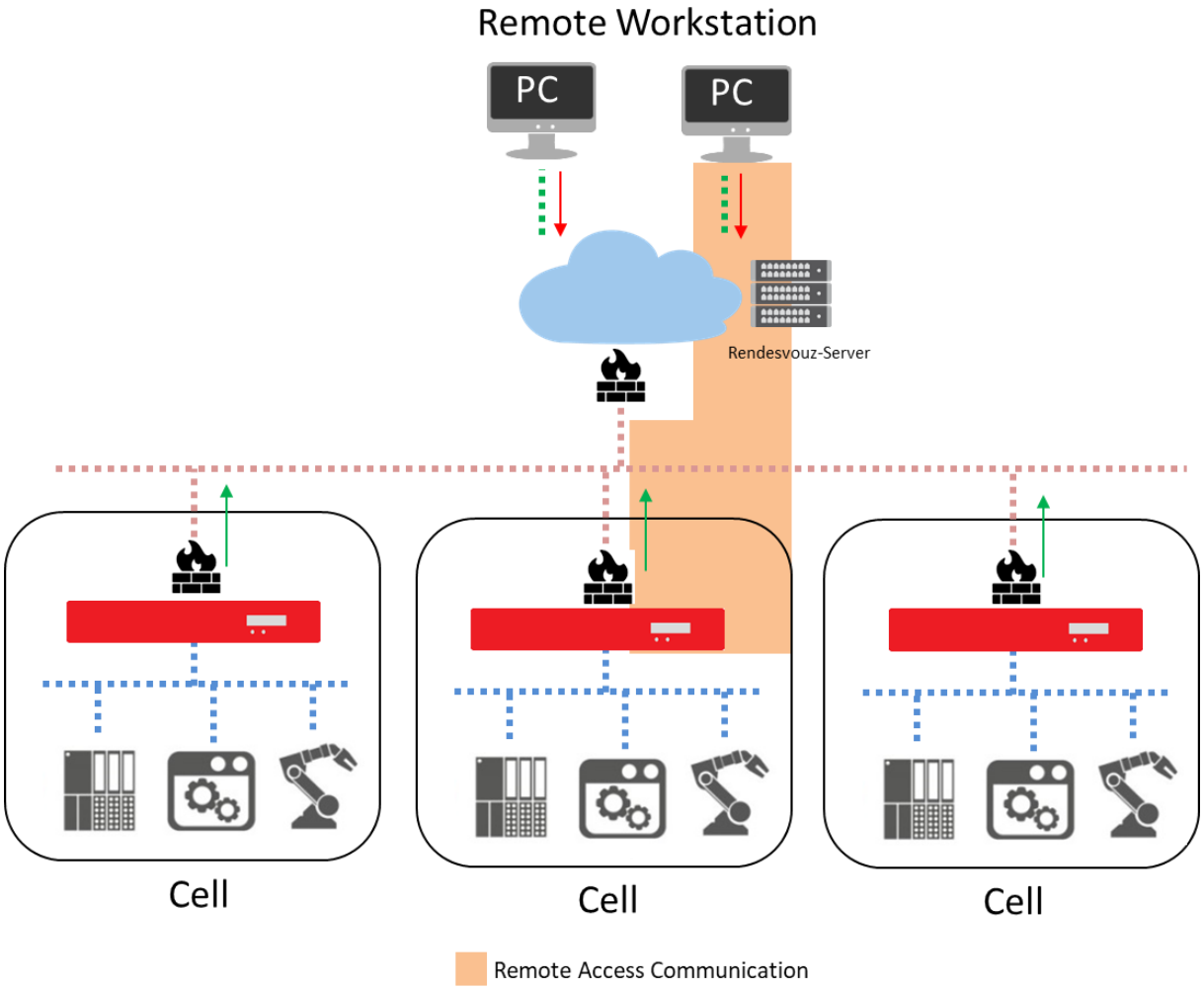

Figure 5: Typical remote access structure

The main remote access scenario is the so-called RENDEZVOUS SERVER scenario. In this scenario the connections are only outgoing connections from the REMOTE ACCESS DEVICE and the REMOTE WORKSTATION via WAN to the RENDEZVOUS SERVER. In this scenario TCP/IP, DNS and VPN protocols will be used.

- Remote Access communication

1. In this scenario the initial connection will be started from the REMOTE ACCESS DEVICE with a (external) trigger for activating the connection to the RENDEZVOUS SERVER. This trigger can be physical (e.g. key-switch) as well as over an API on the REMOTE ACCESS DEVICE
2. For remote access, the same procedure must be done from the REMOTE WORKSTATION. The connection will be initialised by the REMOTE WORKSTATION to the RENDEZVOUS SERVER. The communication via VPN must be secured by state-of-the-art security mechanism.
3. A publicly available RENDEZVOUS SERVER is needed to establish a VPN tunnel from the REMOTE ACCESS DEVICE and REMOTE WORKSTATION.

4. The RENDEZVOUS SERVER now can connect the two VPN tunnels, one from the Remote Access Device and one from the REMOTE WORKSTATION to the RENDEZVOUS SERVER, so that the Remote Workstation has access to the REMOTE ACCESS DEVICE which can route the traffic from the VPN tunnel into the cell network for remote access.

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 REMOTE ACCESS DEVICE also has to provide a set of security functionalities. The following lists the relevant security functions:

- state of the art VPN;
- state of the art Encryption;
- state of the art Authentication for remote access and for configuration management;
- state of the art Role-based-access for configuration;
- state of the art Remote Update capability;
- state of the art Integrity of protected firmware and boot-process;
- state of the art Security hardening, e.g. disabled interfaces, functions, or configuration interfaces.

These security functions are expressed in terms of IEC 62443-4-2:2019, i.e. component requirements (CR), in Chapter 4.2. State of the art of security functionality and mechanism are defined in “TeleTrusT Guideline State of the art in IT security” in the recent version[1].

The user authentication from the REMOTE WORKSTATION to the RENDEZVOUS SERVER is not part of this Use Case “Remote Access Device”.

Additionally, Stateful Inspection and Layer 3 Firewall including application level gateway (ALG) or deep package inspection to WAN is described in the Use Case “Industrial Firewall” and is not part of this Use Case “Remote Access Device”.

3.2 Component Type

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

3.3 Component Security Assumptions

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

Physical assumptions
The REMOTE ACCESS DEVICE 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 REMOTE ACCESS DEVICE receives a valid time from an NTP server.

[1] https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

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.

The private keys for authentication of the remote access infrastructure must be protected from unauthorised access, modification, or theft with procedural and technical controls.

Key management is part of configuration management and therefore the integrator must maintain the key infrastructure for the remote access over the complete lifecycle of the REMOTE ACCESS DEVICE.

There should be one unique (client) certificate for each REMOTE ACCESS DEVICE to authenticate at the remote access infrastructure.

The encryption of the keys (cipher, size and art of encryption) must be state of the art.

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

One attack vector is the remote connection and the (initial) configuration, it must be robust of wiretapping, hijacking or man in the middle attacks.

The configuration management interface and configuration APIs are another attack threat vectors of the Industrial REMOTE ACCESS DEVICE. If an attacker can 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 REMOTE ACCESS DEVICE cannot be guaranteed.

Because the remote connection is initiated from the Industrial REMOTE ACCESS DEVICE, it can be assumed that the device is closed for incoming connections. However, the IP stack must be robust. Not correctly formatted IP packets might be a direct threat for the IP stack.

The integrity of the Industrial REMOTE ACCESS DEVICE and the integrity 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 1.1 Human user identification and authentication Note: This CR is relevant for configuration management interface	x	x
CR 1.1 RE(1) Unique identification and authentication	x	x
CR 1.1 RE(2) Multifactor authentication for all interfaces Note: only applicable if accessible from external reachable interfaces (i.e. Internet)		x
CR 1.2 Software Process and Device Identification and Authentication Note: This CR is relevant for remote access interface	x	x
CR 1.2 RE(1) Unique identification and authentication	x	x
CR 1.3 Account management	x	x
CR 1.4 Identifier management	x	x
CR 1.5 Authenticator management	x	x
CR 1.5 RE(1) Hardware security for authenticators		x
CR 1.6 Wireless access management	x	x
CR 1.7 Strength of password-based authentication	x	x
CR 1.7 RE(1) Password generation and lifetime restrictions for human users	x	x
CR 1.7 RE(2) Password lifetime restrictions for all users (human, software process, or device)		x
CR 1.8 Public key infrastructure certificates	x	x
CR 1.9 Strength of public key-based authentication	x	x
CR 1.9 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		
CR 1.14 Strength of symmetric key-based authentication	x	x
CR 1.14 RE(1) Hardware security for symmetric key-based authentication		x
FR 2 — Use Control (UC)		
CR 2.1 Authorization enforcement	x	x
CR 2.1 RE(1) Authorization enforcement for all users (humans, software processes and devices)	x	x
CR 2.1 RE(2) Permission mapping to roles	x	x
CR 2.1 RE(3) Supervisor override		
CR 2.1 RE(4) Dual approval		
CR 2.2 Wireless use control	x	x
CR 2.3 Use control for portable and mobile devices		
CR 2.4 Mobile code		
CR 2.5 Session lock	x	x
CR 2.6 Remote session termination	x	x
CR 2.7 Concurrent session control		x
CR 2.8 Auditable events	x	x
CR 2.9 Audit storage capacity	x	x
CR 2.9 RE(1) Warn when audit record storage capacity threshold reached		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		x
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
FR 5 — Restricted Data Flow (RDF)		
CR 5.1 Network segmentation		
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		x
NDR 5.2 (3) Fail close		x
NDR 5.3 General-purpose person-to-person communication restrictions		
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
NDR 1.13 RE(1) Explicit access request approval	N/A	N/A	Not relevant, non-trusted network access in the OT environment will be established via Firewall Use Case

CR 2.1 RE(3) Supervisor override	N/A	N/A	This control isn’t existing and not allowed in this use case
CR 2.3 Use control for portable and mobile devices	N/A	N/A	Portable and mobile devices are out of scope in this use case.
CR 2.4 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	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.
CR 5.1 Network segmentation			Not relevant, network segmentation will be established via Firewall Use Case
NDR 5.3 General-purpose person-to-person communication restrictions			Not relevant, network segmentation will be established via Firewall 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. Physical access to the component is restricted in this use case, see Chapter 3.3.	Modifications of the components could be identified by a broken tamper seal. The seal supports the secure delivery process. Integrators can verify the seal status after unboxing and before commissioning.

4.3 Additional Requirements

The REMOTE ACCESS DEVICE 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 allows administrator access only during the initially configuration. The administrator has to set a new password after the initial access. The factory reset configuration does not contain any activate remote access user account or pre-configured authentication key.	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[2]. 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 REMOTE ACCESS DEVICE 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 REMOTE ACCESS DEVICE, the required components and a possible high-level architecture for the setup are presented in Figure 3.

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

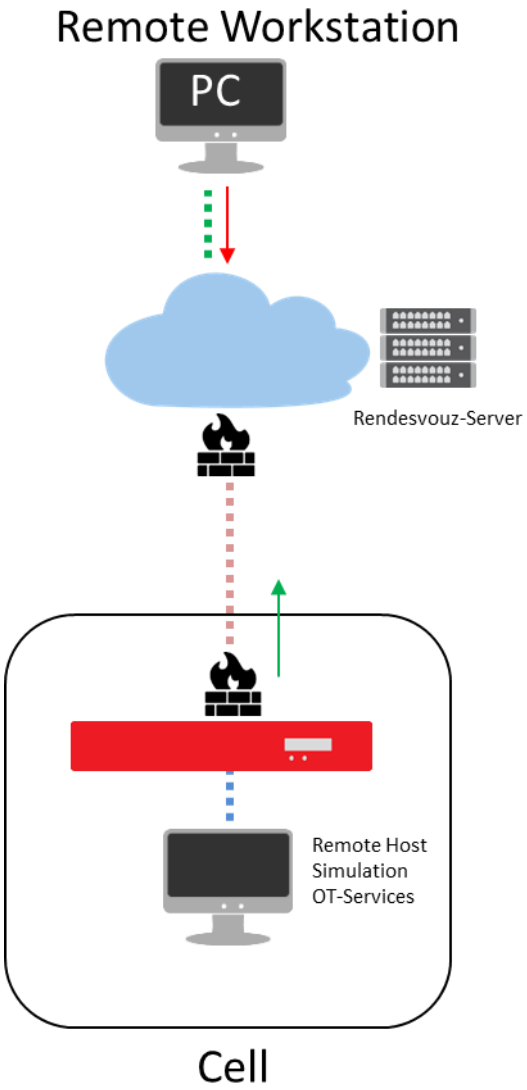

Figure 3 – Test setup with required test environment

5.2 Required Test Interfaces

The conformity testing should be focused on, at least,

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

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 no VPN connectivity.	Accept: • If all rules are flushed no VPN connections can be 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 VPN

The connection to the VPN Servers should be possible via pre-configured solutions for the evaluation or with the help of the integrator / supplier of the remote access infrastructure which can provide such a configuration.

After a successful connection is established a remote host (as a sample of a component in the OT environment) in the virtual VPN network should be reachable via ping, webserver or an application endpoint for passing the test case. The criteria which endpoint should be used can be defined with the integrator / supplier of the remote access infrastructure and the test lab.

5.4.2 Encryption

The encryption which is used for the connection to the remote access infrastructure should be state of the art. A connection log should be available with all important encryption parameters in the event log and/or the audit log of the REMOTE ACCESS DEVICE.

5.4.3 Authentication for remote access and for configuration management

This covers the component requirements from CR1.1 to CR1.7 and CR1.10 to NDR1.13:

Scenario 1:

Check using the device manual whether the use case security level capabilities are available in relation to the targeted security level (basic or extended).

Scenario 2:

After successful testing Scenario 1, continue testing of the implemented functionality regarding conformity with the use case security level capabilities on a device.

5.4.4 Role-based-access for configuration

This covers the component requirements from CR2.1 to CR2.2 and CR2.12:

Scenario 1:

Check using the device manual whether the use case security level capabilities are available in relation to the targeted security level (basic or extended).

Scenario 2:

After successful testing Scenario 1, continue testing of the implemented functionality regarding conformity with the use case security level capabilities on a device.

5.4.5 Remote Update capability

This covers the component requirement NDR 3.10:

Check using the device manual whether the device has the capabilities to update the firmware of the device from a central station initiated from:

- a user from remote

or

- from the device itself via periodic time trigger

5.4.6 Integrity of protected firmware and boot-process

This covers the component requirement NDR 3.14:

Check using the device manual whether the device has the capabilities to:

- Verify the originator of the firmware to ensure the integrity. (Signed Firmware)
- Verify the integrity of firmware, software and configuration data before using them at boot

5.4.7 Security hardening, e.g. disabled interfaces, functions, or configuration interfaces

Check using the device manual whether the device manufacturer provides a guideline for security hardening and follow these instructions. Alternative follow at least these recommendations:

- Disable unused physical interfaces like Ethernet-Ports, USB-Ports or similar.
- Disable unused functions and services
- Disable not necessary configuration interfaces, e.g. only one interface like WEB-GUI or console
- Change Factory Password

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, 2019-05

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.