Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IEC 62443-4-2 Use Case

Security Gateway

based on DIN SPEC 27070

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

Content

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 IDS Security Gateway (or Connector) defines the corresponding automation or IACS component as part of an International Data Spaces (IDS) system.

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 backgrounds and different levels of experience in 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 Introduction

A Security Gateway in the context of IDS makes a virtual cross-company data and service space possible. Based on the principles of data sovereignty, the Security Gateway facilitates the secure exchange of data and allows for providing and using trustworthy data services.

The Security Gateway is available in three different variants, corresponding to different levels of security and protection. It is suited for being used by companies from industry segments such as finance, healthcare, IT, telecommunications, logistics, or industry 4.0 (Industrial Internet).

Figure 1 shows how different exchange architectures are facilitated by a secure gateway.

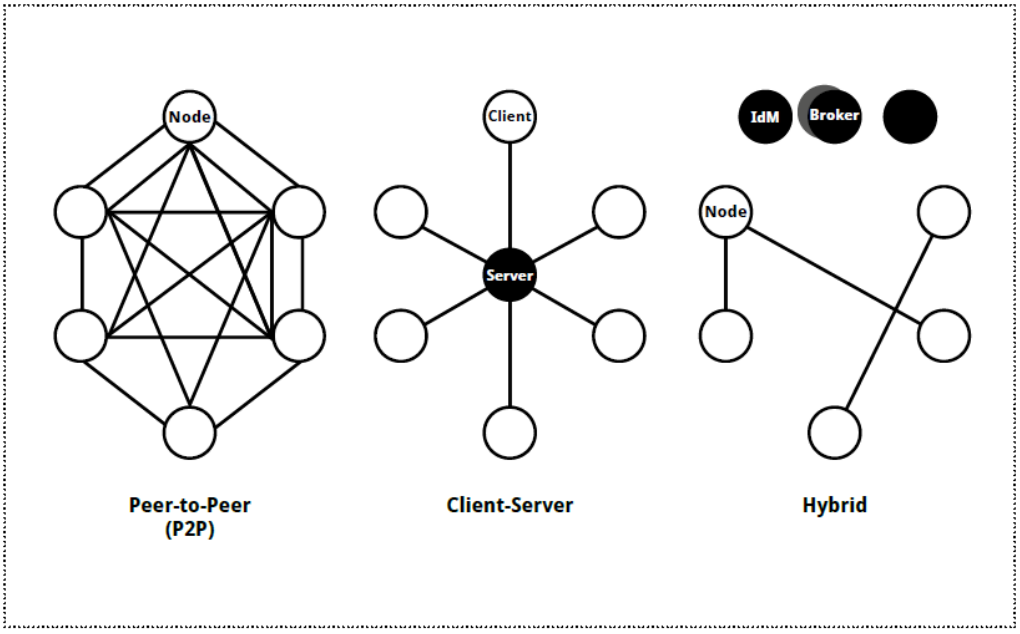

Figure 1 — Data Exchange Architectures

The focus of this use-case is the gateway as depicted in Figure 2. The figure displays two Security Gateways exchanging data with each other (in this case: machine parameters and sensor data) with corresponding supporting components like Identity Provider, Broker, and App Store as defined in the IDS.

The preconditions for this infrastructure are detailed in Chapter 4.2 “Data Exchange Architectures” in [DIN SPEC 27070].

1.3 Copyright

1.4 Objectives

The Security Gateway serves as a platform for operating data services via apps and making data endpoints available. To ensure data exchange, the following objectives must be fulfilled by the Security Gateway:

- The Security Gateway must provide metadata (i.e. a self-description) in order to inform other Security Gateways about its data endpoints and other features it offers (e.g. supported security features).
- The Security Gateway must prove its own identity.
- The Security Gateway must provide access control regarding data sources offered.
- The Security Gateway must support executable data services.
- The Security Gateway must control interaction of such data services.
- The Security Gateway must control access to internal networks and data sources.

These objectives are formulated as security requirements for the component in Chapter 4 in this document. For a full list of requirements, see Chapter 6 “Security Gateway Requirements” in [DIN-SPEC-27070].

1.5 Intended Operational Environment

As the Security Gateway connects the company’s internal infrastructure with its external environment, the Gateway is typically located at a company‘s logical border. This means that a Gateway can physically be implemented both at the company’s premises and at the premises of a service provider.
The infrastructure of the Security Gateway depicted in Figure 1 should consist of the following additional components:

- an Identity Provider issuing identities to Security Gateways and participants;

- an App Store providing services to be used by Security Gateways;
- a Broker acting as a kind of service registry and referring to Security Gateways offering these services;
- a Clearing Entity logging all data transactions (if required).

For successful integration and operation of these additional components, a business layer should be defined, this makes use of the gateway's functional requirements. For the operation of the Security Gateway, the following roles are involved:

- Participant: data consumer or data provider within a data exchange scenario.
- User: Participant using the Security Gateway as a service (appliance). This presupposes that Security Gateway Providers are responsible for Security Gateway integration and operation.
- Security Gateway Provider: Developer of Security Gateways providing components that meet the requirements specified with regard to secure integration and operation.
- Service Provider: Part of the organisational and technical environment in which the Security Gateway is to be embedded.

1.6 Introduction of Use-Case Security-Level Capability

In the following chapters, three variants of the Security Gateway will be defined:
- Base (basic protection);
- Trust (proven protection);
- Trusted Plus (enhanced protection).

From a business perspective, the data provider can decide which Security Gateway type entrusts the control and manipulation of the data.

Base Connectors are designed to make a low barrier starting point possible. Ideally these should be employed for experimental and test environments. In a mature IDS environment, the Base Connectors are not to be expected to be operated.

For mission-critical or otherwise highly sensitive data, Base Connectors might only be allowed in private security domains.

In case of critical infrastructure, the data provider can restrict the data flow by policy. This can be enforced by making use of Trusted Plus Gateways.

See table 1 below for a description and a comparison between the defined levels and the Security Levels (SL-C) defined in IEC 62443 4-2 (see [IEC62442-4-2]).

1.7 Disclaimers

Compensating Countermeasures
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.

Security Gateways according to [DIN-SPEC-27070] have to be designed to implement all defined requirements as listed in Chapter 4.

2 System Architecture

2.1 Architecture

Figure 2 shows an example of how the Security Gateway can be embedded in a communication infrastructure composed of multiple IDS components.

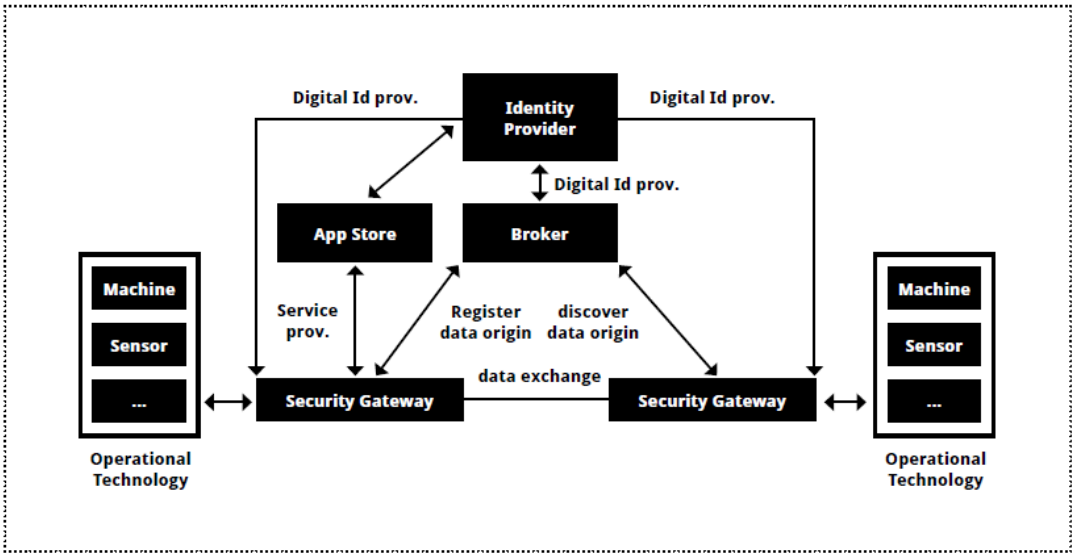

Figure 2 — Infrastructure for the Security Gateway in a Complete Ecosystem

2.2 Interfaces

The logical interfaces of a gateway vary with the implementation. Which protocol is used for the data provision depends on the scenario and can be taken from the self-description. The Connector self-description is the collection of Connector information, such as the catalogue of provided resources.

Two protocols are defined to exchange data between Security Gateways, namely HTTP (WS) and IDSCP (see [IDS-Comm]).

In different scenarios the gateway can act as both client as well as server. In the following, the different scenarios for a Gateway are listed:

a) Data Consumer
   - The Security Gateway receives data from a partner Security Gateway. Data is directed towards the apps for implementing the business logic.

b) Data Provider
   - Data obtained from its operation technology segment is processed and made available to a partner Security Gateway.

c) App Consumer
   - The Security Gateway is a client, pulling app from another Security Gateway or App Store. There are three app exchange scenarios possible, depending on the (eco)system configuration:
     1) No mediation: The Security Gateway uses the direct and trusted relationship with another Security Gateway, which provides the metadata of the apps available for downloading and the apps themselves.
     2) Metadata mediation: A Metadata Broker server holds as intermediary, the apps are stored by other Gateways listed in the metadata.
     3) Resource (Data App) provision: An App Store is entrusted the role of storing metadata and the apps.

d) App Provider
   - The Security Gateway is a server. In the “No mediation” and “Metadata mediation” scenario, the Security Gateway serves metadata and/or apps to the client Security Gateway.

e) Client of a Clearing House
   The Security Gateway acts as a client to the logging services of a Clearing House.

2.3 Operational Modes/Lifecycle Phases

Roll-out
The IDS certification[1] is required for the participant as well as the employed security gateway. In the latter case, the certification refers to the technical capabilities. A digital certificate for the security gateway is a precondition for a valid participant.

In the roll-out phase, a certification authority provides a certificate for the security gateway, once the technical capabilities have been certified by an evaluation facility.

Commissioning
The participant registers the security gateway at the Dynamic Attribute Provisioning Service after successfully deploying the digital certificate. The security gateway registers itself to a metadata broker.

In Operation
The security gateway participates in the IDS ecosystem as a certified gateway.

Decommissioning
The certificate is removed from the gateway. The apps and the data stored in apps are purged. Additionally, the configuration is restored to the factory default.

[1] https://www.internationaldataspaces.org/the-ids-certification-scheme/

3 Component Definition

3.1 Component Scope Definition

The component defined in this use-case is a Security Gateway. The term “Gateway” refers to the ability of the device and its software to control the messages that are passed through its interface. This differs from the mode of operation of a router. A router even in conjunction with a firewall does not inspect the content of the packets beyond a certain OSI layer in order to make security and functional decisions. The router will pass the packets from one segment to the other according to the routing table and optionally filters the traffic by the firewall. The source and destination address, ports, and, in case of stateful firewalls, the direction are the decisive factors.

The gateway does not only route the traffic based on port, state, and addressing information, but also serves as a server and client regarding the specific communication flow. Allowed data flows through the gateway are defined using a whitelist approach by denying non-defined traffic. Authentication of the communication parties is a must and a secure transport should be enforced when the channel is considered less trustworthy.

3.2 Component Type

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

3.3 Component Security Constraints/Assumptions

Physical Assumptions
Organisation certification requires baseline IT security practices be in place, like protections from unauthorised individuals.

Logical Assumptions
Information should not flow among the two interface networks (being external or internal) unless it passes through the gateway.

The environment has to provide at least one NTP server that is able to provide a reliable time source.

Requirements for Integrators
The integrator should use only IDS-certified components and apps from a certified App Store.

The communication with other components shall be carried out only with IDS-certified members.

3.4 Component Threats

Most component threats are derived from the environment. On the IDS side, the Metadata Broker, the App Store, the Identity Provider can be spoofed or corrupted. On the other hand, the communication channels are not guaranteed to run over private or secure networks.

Spoofing IDS Components
A Security Gateway should be able to detect a spoofed IDS component. “Spoofed” refers to a malicious component that replicates the behaviour of the victim component. Even in the worst case of a compromise (software level), the attacker would not be able to extract the identity from the victim component. This means that a spoofing attack is only feasible after a high-profile attack involving software and hardware attacks on subsystems like TPM.

Compromised IDS Components
In this case an attacker is able to control an authentic IDS Component. For the Connector this means that at a certain point in time, one of its communication partners will become malicious. To defeat against this scenario, remote attestation was introduced.

Even without remote attestation, the following supplementary mitigations should be considered:

- The information delivered by a Metadata Broker must be double-checked against the information available in the described connector.
- In the case of potentially lost information by leaking it to a malicious Metadata Broker, the Security Gateway must deliver only the necessary data.

- Less trust is placed on the App Store itself than in the signature of the applications.

Threats on communication channels are well-known and documented. Applying well-accepted and standardised communication protocols or protocols that are based on such is the key to a secure communication channel.

Threats derived from the Security Gateway characteristics include malicious apps. A malicious app is an app that has obtained a valid signature through forgery or not. The intent is to cause harm by accessing the internal communications, by manipulating files, by starting or stopping processes, or by pivoting to obtain higher privileges. The threats in this case are of accessing or manipulating sensitive data and in performing denial-of-service attacks on internal subsystems or other apps. Part of the solution is the robustness of the framework, for example container isolation on Docker.

4 Security Requirements

4.1 Definition of Use-Case Security-Level Capability

Table 1 defines three variants of the Security Gateway, which differ with regard to the level of security and protection they offer.

Table 1 Overview of Security Gateway Variants

Variant	Description
Base	Security Gateway “Base” offers basic security features. It is typically issued in connection with Security Level 1 (according to IEC 62443-4-2) and used in scenarios that require a low level of security (to demonstrate testing operations, for example). Implementation and operation of the “Basis” variant is kept simple.
Trust	Security Gateway “Trust” is used in application scenarios in which protection of processed and exchanged data is critical. It is typically issued in connection with Security Level 3 (according to IEC 62443-4-2) and offers protection against inadvertent violation by administrators, e.g. by offering strict container isolation, integrity-protected logging, or encryption of persistent data.
Trust Plus	Building on the „Trust“ variant, Security Gateway „Trust Plus“ offers enhanced protection against violation by administrators applying technical measures. Like „Trust“ it is typically issued in connection with Security Level 3 (according to IEC 62443-4-2).

4.2 Mapping of 62443 4-2 Component Requirements to Use-Case Security-Level Capability

Table 2 contains the mapping of the Component Requirements from IEC 62443-4-2 to the defined Use-Case Security-Level Capability from Section 4.1.

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

Requirement	Basic	Trust	Trust Plus
FR 1 — Identification and Authentication Control (IAC)			
CR 1.1 — Human User Identification and Authentication	x	x	x
CR 1.1 (1) — Unique Identification and Authentication	x	x	x
CR 1.1 (2) — Multifactor Authentication for All Interfaces		x	x
CR 1.2 — Software Process and Device Identification and Authentication	x	x	x
CR 1.2 (1) — Unique Identification and Authentication	x	x	x
CR 1.3 — Account Management	x	x	x
CR 1.4 — Identifier Management	x	x	x
CR 1.5 — Authenticator Management	x	x	x
CR 1.5 (1) — Hardware Security for Authenticators		x	x
NDR 1.6 — Wireless Access Management	x	x	x
NDR 1.6 (1) — Unique Identification and Authentication		x	x
CR 1.7 — Strength of Password-Based Authentication	x	x	x

CR 1.7 (1) — Password Generation and Lifetime Restrictions for Human Users		x	x
CR 1.7 (2) — Password Lifetime Restrictions for All Users			
CR 1.8 — Public Key Infrastructure Certificates	x	x	x
CR 1.9 — Strength of Public Key-Based Authentication	x	x	x
CR 1.9 (1) — Hardware Security for Public Key-Based Authentication		x	x
CR 1.10 — Authenticator Feedback	x	x	x
CR 1.11 — Unsuccessful Login Attempts	x	x	x
CR 1.12 — System Use Notification	x	x	x
NDR 1.13 — Access via Untrusted Networks	x	x	x
NDR 1.13 (1) — Explicit Access Request Approval		x	x
CR 1.14 — Strength of Symmetric Key-Based Authentication	x	x	x
CR 1.14 (1) — Hardware Security for Symmetric Key-Based Authentication		x	x
FR 2 — Use Control (UC)			
CR 2.1 — Authorization Enforcement	x	x	x
CR 2.1 (1) — Authorization Enforcement for All Users		x	x
CR 2.1 (2) — Permission Mapping to Roles		x	x
CR 2.1 (3) — Supervisor Override		x	x
CR 2.1 (4) — Dual Approval			
CR 2.2 — Wireless Use Control	x	x	x
CR 2.3 — Use Control for Portable and Mobile Devices(a)			
NDR 2.4 — Mobile Code	x	x	x
NDR 2.4 (1) — Mobile Code Authenticity Check		x	x
CR 2.5 — Session Lock	x	x	x
CR 2.6 — Remote Session Termination		x	x
CR 2.7 — Concurrent Session Control		x	x
CR 2.8 — Auditable Events	x	x	x
CR 2.9 — Audit Storage Capacity	x	x	x
CR 2.9 (1) — Warn When Audit Record Storage Capacity Threshold Reached		x	x
CR 2.10 — Response to Audit Processing Failures	x	x	x
CR 2.11 — Timestamps	x	x	x
CR 2.11 (1) —Time Synchronization		x	x
CR 2.11 (2) — Protection of Time Source Integrity		x	x
CR 2.12 — Non-Repudiation	x	x	x

CR 2.12 (1) — Non-Repudiation for All Users			
NDR 2.13 — Use of Physical Diagnostic and Test Interfaces		x	x
NDR 2.13 (1) — Active Monitoring		x	x
FR 3 — System Integrity (SI)			
CR 3.1 — Communication Integrity	x	x	x
CR 3.1 (1) — Communication Authentication		x	x
NDR 3.2 — Protection from Malicious Code	x	x	x
CR 3.3 — Security Functionality Verification	x	x	x
CR 3.3 (1) — Security Functionality Verification During Normal Operation			x
CR 3.4 — Software and Information Integrity	x	x	x
CR 3.4 (1) — Authenticity of Software and Information		x	x
CR 3.4 (2) — Automated Notification of Integrity Violations		x	x
CR 3.5 — Input Validation	x	x	x
CR 3.6 — Deterministic Output	x	x	x
CR 3.7 — Error Handling	x	x	x
CR 3.8 — Session Integrity		x	x
CR 3.9 — Protection of Audit Information		x	x
CR 3.9 (1) — Audit Records on Write-Once Media			
NDR 3.10 — Support for Updates	x	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 Tampering Attempt		x	x
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 Boot Process	x	x	x
NDR 3.14 (1) — Authenticity of Boot Process		x	x
FR 4 — Data Confidentiality (DC)			
CR 4.1 — Information Confidentiality	x	x	x
CR 4.2 — Information Persistence		x	x
CR 4.2 (1) — Erase of Shared Memory Resources		x	x
CR 4.2 (2) — Erase Verification		x	x
CR 4.3 — Use of Cryptography	x	x	x
FR 5 — Restricted Data Flow (RDF)			
CR 5.1 — Network Segmentation	x	x	x
NDR 5.2 — Zone Boundary Protection	x	x	x

NDR 5.2 (1) — Deny All, Permit by Exception		x	x
NDR 5.2 (2) — Island Mode		x	x
NDR 5.2 (3) — Fail Close		x	x
NDR 5.3 — General-Purpose Person-to-Person Communication Restrictions	x	x	x
CR 5.4 — Application Partitioning			
FR 6 — Timely Response to Events (TRE)			
CR 6.1 — Audit Log Accessibility	x	x	x
CR 6.1 (1) — Programmatic Access to Audit Logs		x	x
CR 6.2 — Continuous Monitoring		x	x
FR 7 — Resource Availability (RA)			
CR 7.1 — Denial of Service Protection	x	x	x
CR 7.1 (1) — Manage Communication Load from Component		x	x
CR 7.2 — Resource Management	x	x	x
CR 7.3 — Control System Backup	x	x	x
CR 7.3 (1) — Backup Integrity Verification		x	x
CR 7.4 — Control System Recovery and Reconstitution	x	x	x
CR 7.5 — Emergency Power(b)			
CR 7.6 — Network and Security Configuration Settings	x	x	x
CR 7.6 (1) — Machine-Readable Reporting of Current Security Settings		x	x
CR 7.7 — Least Functionality	x	x	x
CR 7.8 — Control System Component Inventory		x	x

4.2.1 Rationale/Adjustment for Non-Selected Component Requirements

The Basic profile is mostly aligned to SL-1 of IEC 62443-4-2 with some additional requirements of SL-2. The Trust and Trust Plus profiles are mostly aligned with SL-3 of IEC 62443-4-2.

Note: In this document two inconsistencies were corrected that appear in the current version of DIN SPEC 27070:2020-03. The corrections include selecting the requirements for NDR 1.13 and moving NDR 1.6 RE (2) to NDR 1.13 RE (1).

4.2.2 Rationale/Adjustment for Modified Component Requirements

Table 3 gives an overview of the modified, i.e. re-mapped, requirements compared to the standard SL from IEC 62443-4-2. The full mapping was already listed in Chapter 4.2. Table 3 contains the requirements (marked with ‘+’) that were specifically selected comparing to SL-1 (Basic) and SL-3 (Trust and Trust Plus).

Table 3 Mapping to IEC 62443-4-2 Component Requirements

Requirement	Basic	Trust	Trust Plus
FR 1 — Identification and Authentication Control (IAC)			
CR 1.2 — Software Process and Device Identification and Authentication	+	x	x
CR 1.2 (1) — Unique Identification and Authentication	+	x	x
CR 1.8 — Public Key Infrastructure Certificates	+	x	x
CR 1.9 — Strength of Public Key-Based Authentication	+	x	x
CR 1.14 — Strength of Symmetric Key-Based Authentication	+	x	x
FR 2 — Use Control (UC)			
CR 2.11 (2) — Protection of Time Source Integrity		+	+
FR 3 — System Integrity (SI)			
CR 3.3 (1) — Security Functionality Verification During Normal Operation			+

The rationales for the modified mappings are given in the following:

a) Authentication in IDS is based on public key infrastructure (PKI), therefore stronger requirements are needed. In the case of Basic profile, which is based on SL-1, the additional component requirements 1.2, 1.2(1), 1.8, 1.9 and 1.14 ensure compatibility and the same level of security for the authentication mechanism between IDS components.

b) The CR 2.11 (2) “Protection of Time Source Integrity” is desired to make any attack on the PKI system detectable and trackable. This requirement increases the level of trust for all certified IDS participants in the PKI system.

c) The CR 3.3 (1) “Security Functionality Verification During Normal Operation” is a stricter requirement that only applies to Trust Plus in order to allow real-time remote attestation checks by other Security Gateways (see COM 04).

4.3 Additional Requirements

In the context of IDS, additional requirements are needed to fulfil the objectives for the Security Gateway shown in Chapter 1.4. The additional requirements are listed in Table 4.

Table 4 Additional Requirements Specific to Secure Gateway

Requirement	Basic	Trust	Trust Plus
Communication Integrity			
COM 01 – Security Gateways communicate with each other only via authenticated, encrypted and integrity protected connections.	x	x	x
COM 02 – Security Gateway certificates facilitate mutual authentication of Security Gateways every time connection is established.	x	x	x
COM 03 – Encryption and integrity protection is facilitated by means of mechanisms considered state of the art by BSI TR 02102-1, NIST SP 800-175b, or an equivalent crypto catalogue.	x	x	x
COM 04 – Security Gateways allow each other to check integrity of each other's software stack via remote attestation.		x	x
COM 05 – Proof of integrity refers to two elements of Security Gateway: — bootloader and — kernel.		x	x
COM 06 – Proof of integrity additionally refers to Security Gateway's — configuration and — apps installed.			x
Data Usage Control			
USC 01 – Security Gateway allows data providers to define usage policies with regard to data offered.	x	x	x
USC 02 – Security Gateway offering data sends usage policy to be applied to Security Gateway requesting data every time connection is established.		x	x
USC 03 – Security Gateway facilitates technical enforcement of data usage policy specified.		x	x
USC 04 – Changes to data usage policy can be made only by administrators of Security Gateway or data provider. In case of changes made to policy, connection between two Security Gateways is reestablished.		x	x
USC 05 – Administrators cannot change rules regarding data flow without data provider taking notice of the change and approving it.			x
Information Model			
INF 01 – Security Gateway provides self-description (i.e. metadata) via a defined interface.	x	x	x
INF 02 – Security Gateway sends metadata to Broker for being registered there.	x	x	x

INF 03 – Self-description contains the following information: — cryptographic hash of Security Gateway certificate, — name of Security Gateway operator, — data endpoints offered by Security Gateway, — log format of data endpoints offered, — security profile of Security Gateway (i.e. security features supported), — Security Gateway ID.	x	x	x
INF 04 – Security Gateway offering data evaluates self description of Security Gateway requesting data.	x	x	x
INF 05 – Attestations regarding dynamic attributes are transmitted every time connection between two Security Gateways is established and can therefore be used for access control decisions.	x	x	x
Identity and Access Management			
IAM 01 – Security Gateway is unambiguously identified by means of a UUID (see also CR 1.2 (1)).	x	x	x
IAM 02 – UUID is contained in an X.509v3 certificate signed by a Certification Authority accepted by data provider and data consumer.	x	x	x
IAM 03 – Security Gateway supports central time service (e.g. to verify certificates).	x	x	x
IAM 04 – Security Gateway supports online status check of certificates issued (e.g. Online Certificate Status Protocol, OCSP).	x	x	x
IAM 05 – Security Gateway supports service for attestation of dynamic attributes, from which it receives certified attribute information (e.g. through JSON Web Tokens).	x	x	x
Broker Service Connection			
BRK 01 – Security Gateway supports broker service inquiries by means of browsing self-descriptions of Security Gateways registered there.	x	x	x
BRK 02 – Security Gateway supports registration with a broker by transmitting self-description.	x	x	x
BRK 03 – Security Gateway supports updates of self-description stored at broker (e.g. when new service is offered).	x	x	x
Software Platform Requirements			
OS 01 – Security Gateway supports installation and execution of containers.	x	x	x
OS 02 – Security Gateway enforces strict separation of data processing apps. Communication between apps takes place via approved channels only (i.e. whitelisting of data exchange channels).		x	x
OS 03 – Security Gateway verifies authenticity and integrity of data services prior to installation and execution.		x	x
OS 04 – Security Gateway verifies authenticity and integrity of all system components prior to execution.		x	x

OS 05 – All data services installed are strictly isolated from each other by default. Communication channels must be explicitly activated (i.e. whitelisting of channels).		x	x
OS 06 – Containers are strictly separated from each other and from underlying operating system layers.		x	x
OS 07 – System data backups as well as backups of data transferred between Security Gateways are always encrypted before being stored outside system.		x	x
Apps and App Store Connection			
APS 01 – Security Gateway supports only apps possessing a valid signature. This signature is the signed check sum of the software artifact, which was created by means of a private key of the app publisher.		x	x
APS 02 – Security Gateway verifies signature after app was downloaded and before it is installed, and before every execution of app. Public key of app publisher is contained in an X.509v3 certificate signed by a Certification Authority accepted by data provider and data consumer.	x	x	x
APS 03 – Security Gateway supports apps carrying usage policies, allowing restriction of use and encapsulation of licensing information.		x	x
APS 04 – Security Gateway checks minimum requirements of apps regarding runtime environment (e.g. with regard to memory capacity or number of CPU cores) and ensures these requirements are fulfilled as long as app is active.		x	x
APS 05 – Security Gateway supports apps delivered and installed as independent software containers (i.e. apps bring along possible dependencies of e.g. software modules themselves and can be used irrespective of Security Gateway's configuration).	x	x	x
APS 06 – Security Gateway receives apps from a central app store. Among other things, this requirement is important to ensure that the use of an app does not impair the functionality of other apps (or of the Security Gateway itself).	x	x	x
Data Usage Transparency			
AUD 01 – Security Gateway logs each access control decision in the form of an integrity protected log entry.	x	x	x
AUD 02 - Security Gateway logs every access to data in the form of an integrity protected entry.	x	x	x
AUD 03 – Security Gateway logs any changes made to its configuration in the form of integrity protected entries.	x	x	x
AUD 04 – Security Gateway logs every case in which a service receives fewer resources than requested (e.g. fewer RAM capacity).		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 (see Table 2), no special test environment is required. The tested Security Gateway (DUT) will be inspected with the help of a testing workstation.

For testing the additional requirements specific to the Security Gateway, the required components and the high-level architecture are presented in figure 3.

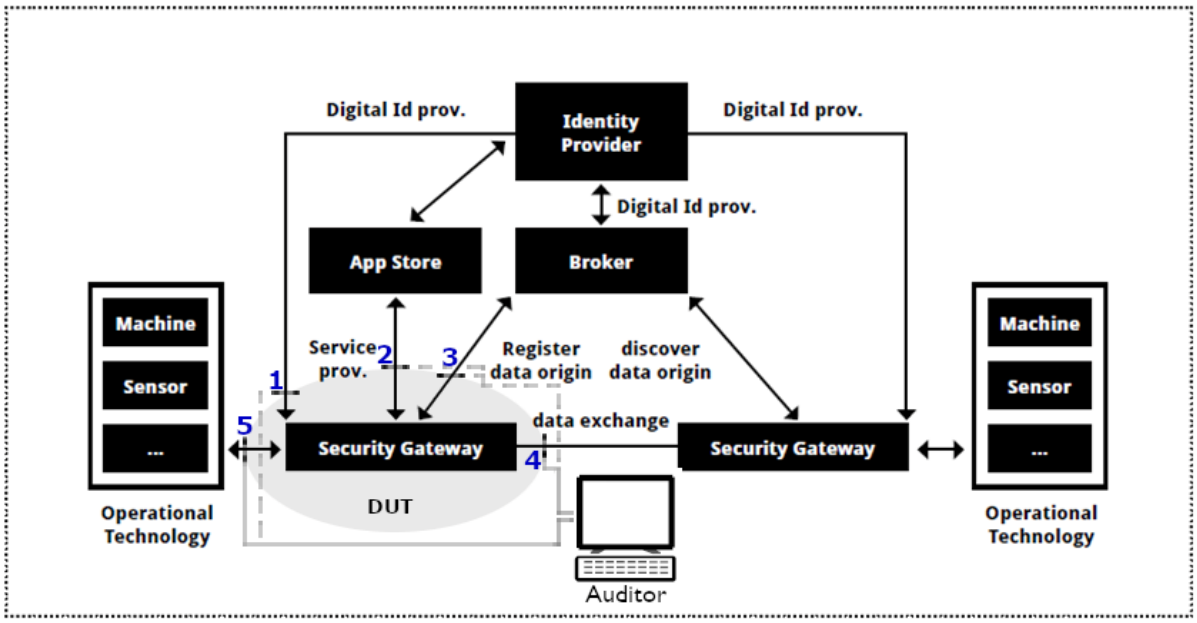

Figure 3 — Test Setup with Required Test Environment

Following are the additional test components shown in figure 3:

a) Broker
   - Acts as a register of metadata communicated by the IDS components. With its help will be checked if information communicated is sound and, additionally, there are no information leakages in the self-descriptions sent by the Security Gateway.

b) Identity Provider (incl. PKI Provider)
   - Provides reliable identification of Security Gateways and other participants. Its services are necessary as basis for verifying the access control decision.

c) App Store

[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 IECEE or IEC in the future.

- Makes available apps to Security Gateways. Test activities in this area include interoperability and security checks, like correct verification of app's signature and enforcement of usage policies.

d) (Second) Security Gateway
   - For establishing the connection compatibility, authentication and message exchange characteristics (encryption and integrity checks) between two Security Gateways. Each gateway must assure each other of the integrity of operating systems and other components installed on them.

e) OT equipment
   - This includes PLCs, sensors and actuators, acting either as provider or/and as consumers of information that is passed through the gateway.

5.2 Required Test Interfaces

With reference to Figure 3, the connections marked with 1, 2, 3, 4 and 5 are considered to be outside of the untrusted network. Chapter 2.2 provides more details about the role of the Connector and the communication partner.
The connection marked with 5 can originate from a trusted network (OT equipment) and can bundle interfaces to OT protocols like ProfiNET or EtherCAT as well as OPC-UA or MQTT. This interface can be monitored in order to observe if any traffic manages to bypass the Connector.

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 3), 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	
COM 01 – Security Gateways communicate with each other only via authenticated, encrypted and integrity protected connections.	Accept: • The Security Gateway accepts a secure connection for another Security Gateway. Not accept: • The connection does not guarantee authentication, encryption, or integrity.
COM 02 – Security Gateway certificates facilitate mutual authentication of Security Gateways every time connection is established.	Accept: • The Security Gateway accepts a connection for another Security Gateway with a valid certificate originating from an accepted Identity Provider. Not accept: The Security Gateway proceeds with the authentication when: • the second Security Gateway tries to authenticate without a certificate, or • the partner gateway certificate is not valid.
COM 03 – Encryption and integrity protection is facilitated by means of mechanisms considered state of the art by BSI TR 02102-1, NIST SP 800-175b, or an equivalent crypto catalog.	Accept: • State-of-the-art encryption and integrity protection mechanisms are used. Not accept:

	• The implemented crypto has weaker security properties as the security primitives described in the referred standards.
COM 04 – Security Gateways allow each other to check integrity of each other's software stack via remote attestation.	Accept: • Remote attestation functionality is implemented. Not accept: • The implementation of the remote attestation check affects the confidentiality, integrity, or availability.
COM 05 – Proof of integrity refers to two elements of Security Gateway: — bootloader and — kernel.	Accept: • The Security Gateway enforces the proof of integrity for both the bootloader as well as the kernel.
COM 06 – Proof of integrity additionally refers to Security Gateway's — configuration and — apps installed.	Accept: • The Security Gateway enforces the proof of integrity for both the configuration, as well as installed apps.
Data Usage Control	
USC 01 – Security Gateway allows data providers to define usage policies with regard to data offered.	Accept: • Data usage policies can be defined by data providers.
USC 02 – Security Gateway offering data sends usage policy to be applied to Security Gateway requesting data every time connection is established.	Accept: • The data-providing Security Gateway sends the usage policy to the requesting Security Gateway with every new connection.
USC 03 – Security Gateway facilitates technical enforcement of data usage policy specified.	Accept: • The Security Gateway enforces the usage policy.
USC 04 – Changes to data usage policy can be made only by administrators of Security Gateway or data provider. In case of changes made to policy, connection between two Security Gateways is reestablished.	Accept: • Changes to the data usage policy can be made by administrators or data provider. • After a change to the usage policy, the connection is reestablished.
USC 05 – Administrators cannot change rules regarding data flow without data provider taking notice of the change and approving it.	Accept: • Data providers are notified about changes to the data flow by administrators. • Changes take effect only after the data provider approved the changes.
Information Model	
INF 01 – Security Gateway provides self-description (i.e. metadata) via a defined interface.	Accept: • The gateway provides a self-description that can be understood by other gateways.

INF 02 – Security Gateway sends metadata to Broker for being registered there.	Accept: • The gateway sends a self-description to the broker that can be understood there.
INF 03 – Self-description contains the following information: — cryptographic hash of Security Gateway certificate, — name of Security Gateway operator, — data endpoints offered by Security Gateway, — log format of data endpoints offered, — security profile of Security Gateway (i.e. security features supported), — Security Gateway ID.	Accept: • The self-description contains the required information.
INF 04 – Security Gateway offering data evaluates self-description of Security Gateway requesting data.	Accept: • The Security Gateway evaluates the self-description of the requesting Security Gateway.
INF 05 – Attestations regarding dynamic attributes are transmitted every time connection between two Security Gateways is established and can therefore be used for access control decisions.	Accept: • Dynamic attributes are sent with each connection. • The dynamic attributes are used for access control decisions.
Identity and Access Management	
IAM 01 – Security Gateway is unambiguously identified by means of a UUID (see also CR 1.2 (1)).	Accept: • The Security Gateway poses a unique UUID. Not accept: • The UUID has not the required format.
IAM 02 – UUID is contained in an X.509v3 certificate signed by a Certification Authority accepted by data provider and data consumer.	Accept: • The Security Gateway certificate contains the UUID and is signed by a certified identity provider.
IAM 03 – Security Gateway supports central time service (e.g. to verify certificates).	Accept: • At least one time-synchronisation service can be configured.
IAM 04 – Security Gateway supports online status check of certificates issued (e.g. Online Certificate Status Protocol, OCSP).	Accept: • The Security Gateway supports at least one online status check service for certificates.
IAM 05 – Security Gateway supports service for attestation of dynamic attributes, from which it receives certified attribute information (e.g. through JSON Web Tokens).	Accept: • The Security Gateway is able to register to the service for attestation of dynamic attributes. • The Security Gateway is able to consume certified attribute information.
Broker Service Connection	

BRK 01 - Security Gateway supports broker service inquiries by means of browsing self-descriptions of Security Gateways registered there.	Accept: • The Security Gateway answers with a self-description if contacted by a broker.
BRK 02 – Security Gateway supports registration with a broker by transmitting self-description.	Accept: • The Security Gateway registers itself by sending a self-description to a broker.
BRK 03 – Security Gateway supports updates of self-description stored at broker (e.g. when new service is offered).	Accept: • The Security Gateway sends updates of the self-description to the associated broker.
Software Platform Requirements	
OS 01 – Security Gateway supports installation and execution of containers.	Accept: • The Security Gateway allows for the installation and execution of containers.
OS 02 – Security Gateway enforces strict separation of data processing apps. Communication between apps takes place via approved channels only (i.e. whitelisting of data exchange channels).	Accept: • Data processing and communication between apps is orchestrated and supervised.
OS 03 – Security Gateway verifies authenticity and integrity of data services prior to installation and execution.	Accept: • The authenticity and integrity of all data services is verified prior to installation and execution.
OS 04 – Security Gateway verifies authenticity and integrity of all system components prior to execution.	Accept: • The authenticity and integrity of all system components is verified prior to execution.
OS 05 – All data services installed are strictly isolated from each other by default. Communication channels must be explicitly activated (i.e. whitelisting of channels).	Accept: • The data services are strictly isolated from each other. • The communication channels are whitelisted by the administrator.
OS 06 – Containers are strictly separated from each other and from underlying operating system layers.	Accept: • The containers are strictly separated between each other and from the underlying operating system.
OS 07 – System data backups as well as backups of data transferred between Security Gateways are always encrypted before being stored outside system.	Accept: • All backup outside the gateway is encrypted.
Apps and App Store Connection	
APS 01 – Security Gateway supports only apps possessing a valid signature. This signature is the signed check sum of the software artifact, which was created by	Accept: • The Security Gateway allows the installation of signed apps. Not Accept:

means of a private key of the app publisher.	• The certificate used to sign the app is not valid.
APS 02 – Security Gateway verifies signature after app was downloaded and before it is installed, and before every execution of app. Public key of app publisher is contained in an X.509v3 certificate signed by a Certification Authority accepted by data provider and data consumer.	Accept: • The app signature is verified after download. • The app signature is verified before installation. • The app signature is verified before each execution.
APS 03 – Security Gateway supports apps carrying usage policies, allowing restriction of use and encapsulation of licensing information.	Accept: • The Security Gateway allows for the apps to specify usage and license policies.
APS 04 – Security Gateway checks minimum requirements of apps regarding runtime environment (e.g. with regard to memory capacity or number of CPU cores) and ensures these requirements are fulfilled as long as app is active.	Accept: • The Security Gateway performs checks of the minimum required runtime environment for the app. • The Security Gateway ensures the fulfilment of the requirements when the app is active.
APS 05 – Security Gateway supports apps delivered and installed as independent software containers (i.e. apps bring along possible dependencies of e.g. software modules themselves and can be used irrespective of Security Gateway's configuration).	Accept: • An app as an independent artefact (container) can be loaded manually.
APS 06 – Security Gateway receives apps from a central app store. Among other things, this requirement is important to ensure that the use of an app does not impair the functionality of other apps (or of the Security Gateway itself).	Accept: • The Security Gateway is able to download and install apps from a central app store. Not accept: • Apps are not checked if they conflict with other apps.
Data Usage Transparency	
AUD 01 – Security Gateway logs each access control decision in the form of an integrity protected log entry.	Accept: • The Security Gateway is able to detect and log each access control decision. • The logs are integrity-protected.
AUD 02 – Security Gateway logs every access to data in the form of an integrity protected entry.	Accept: • The Security Gateway is able to detect and log each access event.
AUD 03 – Security Gateway logs any changes made to its configuration in the form of integrity protected entries.	Accept: • The Security Gateway is able to detect and log changes made to its configuration. • The logs are integrity-protected.

AUD 04 – Security Gateway logs every case in which a service receives fewer resources than requested (e.g. fewer RAM capacity).	Accept: • The Security Gateway is able to detect and log low resource events for an app.

Note: The acceptance criteria listed before are the first set and will be enhanced in the future by the corresponding IDSA working group.

6 List of Abbreviations

Table 6 Abbreviations

Abbreviation	Meaning
IDS	International Data Spaces
DUT	Device Under Test
OT	Operational Technology
PLC	Programmable Logic Controller
PKI	Public Key Infrastructure

7 Definitions

Table 7 Definitions

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

See also the chapter “3 BASIC TERMINOLOGY” from [DIN-SPEC-27070].

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

[DIN-SPEC-27070] DIN SPEC 27070:2020-03, Requirements and reference architecture of a security gateway for the exchange of industry data and services

[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.