Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IEC 62443-4-2 Use Case

Industrial Firewall Profile Proposal for IEC 62443-5

2025

Danksagung

TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung an dieser Publikation:

Projektleitung

Luise Werner, secuvera GmbH

Autoren und mitwirkende Fachleute

Thomas Bleier, B-SEC better secure GmbH & Co KG
Carsten Bokholt, Helmholz GmbH & Co. KG
Sebastian Fritsch, secuvera GmbH
Andreas Fuß, Phoenix Contact GmbH & Co. KG
Marcus Geiger, TÜV SÜD Industrie Service GmbH
Michael Hermes, TÜV SÜD Product Service GmbH
Steffen Heyde, secunet Security Networks AG
Siegfried Müller
Steffen Pfendtner, ads-tec Industrial IT GmbH
Markus Pongratz, Helmholz GmbH & Co. KG

Redaktion

Holger Mühlbauer, Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Impressum

Herausgeber:

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

V 2025-01

Table of Contents

1 Title

Industrial Firewall - Profile proposal for IEC 62443-5

2 Scope

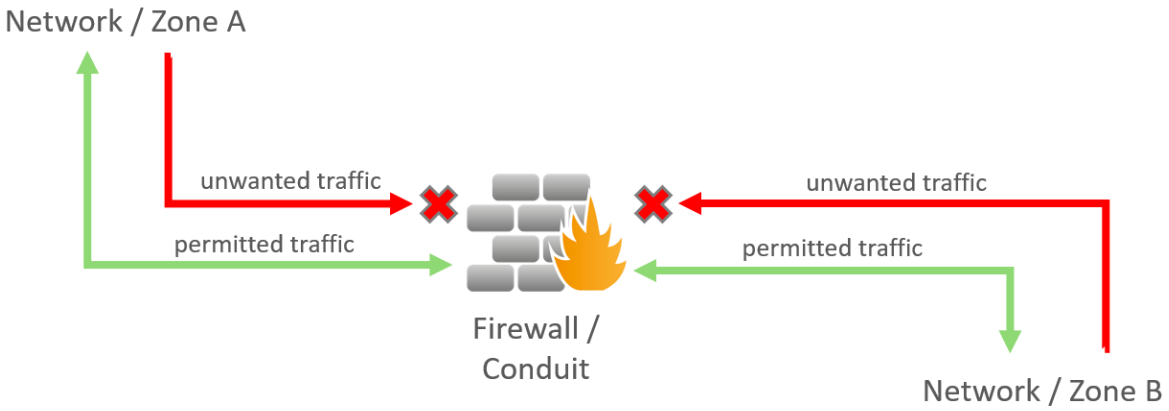
Component Type: The component type according to IEC 62443-4-2 is a "Network Component".

2.1 Specified scope

- The security profile "Industrial Firewall" specifies the widely used automation or IACS component-type Industrial Firewall as part of an OT network.
- The described Industrial Firewall is for usage in a locked cabinet or at least in a restricted factory environment with access by authorized personnel only.
- The Industrial Firewall may only be operated by trained personnel.
- The Industrial Firewall is specified to fulfill the "Zones & Conduits" requirements of IEC 62443-3-3 FR 5 "Restricted data flow".

The core functions of a firewall are to block unwanted data traffic and allow desired traffic to pass. Stateful inspection is the current state of the art in this area.

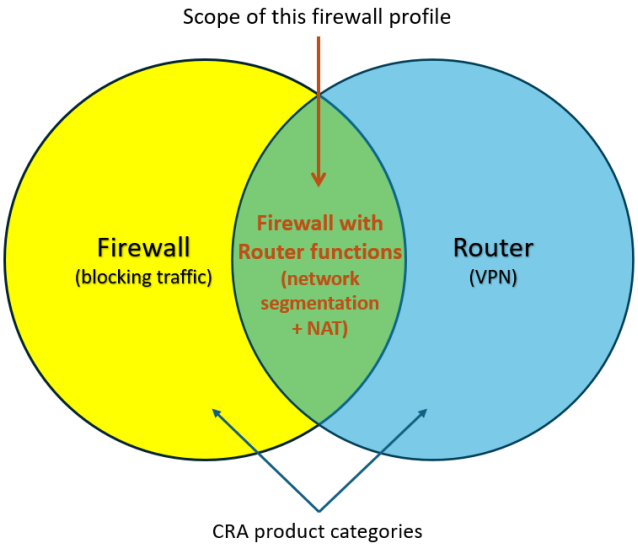
There can be unwanted and desired data traffic on both sides of the network.



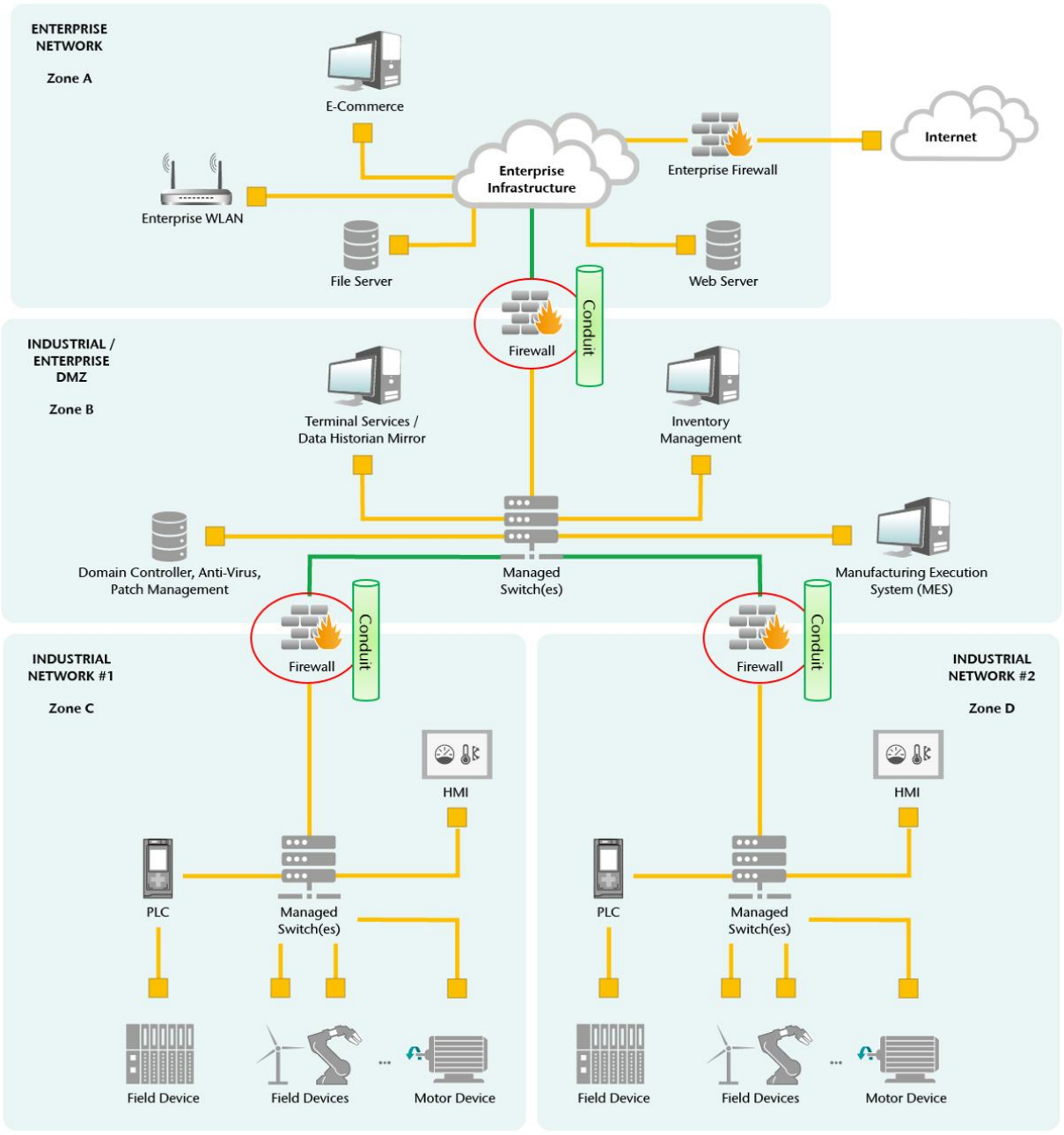
While "firewalls" or "routers" are often discussed, the scope of this profile is intended to describe the real-world combination of a firewall with router functions.

Router functions, in the firewall context, refers to network segmentation and NAT.

VPN connections as used typically for remote maintenance or M2M are not referred to in this profile.



2.2 Application example / Use case



2.3 Out-of-scope

- Firewall Systems that are used outside of an industrial automation system or OT network.
- Fieldbuses, like EtherNet/IP or PROFINET will only process as Layer 2 or Layer 3 messages, not as Fieldbus data.
- VPN, remote access and M2M might be additional features of a firewall device; however, these features are out of scope here.
- 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.
- Deep packet inspection is an option for industrial firewall but out of scope regarding the security considerations of this profile.
- Intrusion Detection Systems and Intrusion Prevention Systems are not covered by this document.
- Virtual Firewall appliances are out of scope.

2.4 Core functions

The core function of an industrial firewall is to block all unwanted traffic. In degraded mode an industrial firewall shall never letting pass unwanted traffic! In an extreme degraded mode, nothing will pass the firewall ("fail close").

The industrial firewall is NOT a safety device. Fail close, block all traffic, is the safe and secure status.

2.5 Assets that shall be protected

The firewall configuration and audit logs are assets that shall be protected. The firewall configuration also includes login data, keys and certificates.

The firmware is an asset but the protection goal is only integrity and authenticity. The protection goal confidentiality is not considered.

Data that passes the firewall or is blocked are no assets that need to be protected by the firewall.
If deep packet inspection is implemented, additional security risks shall be evaluated.

Depending on the risk-analysis of the asset owner, further protection goals might be required.

3 Motivation

Preliminary work for the creation of a harmonized standard for industrial firewalls (62443-5-x) considering the CRA specifications.

Specify the security requirements for an industrial firewall to fulfill the "Zones & Conduits" requirements of IEC 62443-3-3 FR 5 "Restricted data flow"

- Based on TeleTrusT Use Case Industrial Firewall
- SL-2 and SL-3 for 62443-5
- SL-2 for CRA
- SL-1 and SL-4 not addressed here
- CRA-relevant: "Firewall" class (not "Router" class)

4 Supporting organization or association [optional]

TeleTrusT Working Group "Smart Grids/Industrial Security"

5 Terms, definitions, abbreviated terms, acronyms, and conventions

6 Selected IEC 62443 standard(s)

IEC 62443-4-2

7 List of selected IEC 62443 requirements and mapping

The following table contains a mapping of the Component Requirements from IEC 62443-4-2 to the defined security profile and Security-Level capability.

When a manufacturer wants to claim SL-C 2 for an industrial firewall all requirements marked with an ‘X’ in column ‘SL-2’ shall be implemented.

When a manufacturer wants to claim SL-C 3 for an industrial firewall all requirements marked with an ‘X’ in column ‘SL-3’ shall be implemented.

Requirements not marked are optional.

Requirements marked with 'N/A' are technically not applicable for the firewall definition (see chap. 2).

Table1 Mapping to IEC 62443-4-2 Component Requirements

Requirement	SL-2	SL-3	Contextual mapping
FR 1 - Identification and Authentication Control (IAC)			
CR 1.1 Human user identification and authentication	X	X	Applicable for all interfaces that allow access to sensitive assets and have "human users". *Rational and supplemental guidance:* Anonymous users and users who are not yet logged in only have access rights to information that does not require protection.
CR 1.1 RE(1) Unique identification and authentication	X	X	You can also create personalized admin users. The counterexample would be that there is only one admin user with an associated authentication information that is shared by several human users.
CR 1.1 RE(2) Multifactor authentication for all interfaces		X	The multi-factor-authentication should be implemented for SL-3 but might be implemented by a central user authentication system.
CR 1.2 Software process and device identification and authentication	X	X	Applicable for all interfaces that allow access to assets requiring protection (e.g. configuration, audit logs) and have "device users". *Rational and supplemental guidance:* Anonymous users and users who are not yet logged in only have access rights to information that does not require protection.
CR 1.2 RE(1) Unique identification and authentication		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	N/A	N/A	Wireless interfaces are out of scope in this security profile!
CR 1.7 Strength of password-based authentication	X	X	
CR 1.7 RE(1) Password generation and lifetime restrictions for human users		X	
CR 1.7 RE(2) Password lifetime restrictions for all users (human, software process, or device)			
CR 1.8 Public key infrastructure certificates		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		X	
CR 1.14 Strength of symmetric key-based authentication	N/A	N/A	No interfaces with symmetric key-based authentication are used in this security profile.
CR 1.14 RE(1) Hardware security for symmetric key-based authentication	N/A	N/A	*See above*

Requirement	SL-2	SL-3	Contextual mapping
FR 2 - Use Control (UC)			
CR 2.1 Authorization enforcement	X	X	Whenever a human user has access to an interface with access to assets requiring protection, the interface shall enforce authorization. *Rational and supplemental guidance:* Anonymous users and users who are not yet logged in only have access rights to information that does not require protection!
CR 2.1 RE(1) Authorization enforcement for all users (humans, software processes and devices)	X	X	Whenever a user (human, device, service, ...) has access to an interface with assets requiring protection, the interface shall enforce authorization. It shall be possible to see who has accessed it (→ audit log). *Rational and supplemental guidance:* Excluding "public" information (not requiring protecting).
CR 2.1 RE(2) Permission mapping to roles	X	X	Supplementary to CR 2.1: Access to information requiring protection shall be regulated individually for each role.
CR 2.1 RE(3) Supervisor override	N/A	N/A	Requirement not relevant for industrial firewall profile because an industrial firewall does not control anything.
CR 2.1 RE(4) Dual approval	N/A	N/A	Requirement not relevant for Industrial Firewall profile because an Industrial Firewall does not control anything.
CR 2.2 Wireless use control	N/A	N/A	No Industrial Wireless firewall is defined in this profile. Wireless is outside the scope.
~~CR 2.3 Use control for portable and mobile devices~~	N/A	N/A	*(is no longer in the standard)* Portable and mobile devices are out of scope in this security profile.
CR 2.4 Mobile code	N/A	N/A	No industrial firewall with external/reloadable code is defined in this profile.
CR 2.5 Session lock	X	X	User shall be able to log out or is automatically logged out after inactivity (timeout).
CR 2.6 Remote session termination	X	X	One of the three options of the standard is already sufficient.
CR 2.7 Concurrent session control		X	The number of concurrent sessions on interfaces can, but does not have to be configurable. It can also be fixed.
CR 2.8 Auditable events	X	X	Control system events are firewall events.
CR 2.9 Audit storage capacity	X	X	No specific storage size is specified in the profile. Each manufacturer shall define a suitable size themselves. It should be possible to justify the appropriate size. CR 2.9 b) Important: logging shall not affect the core functions of the industrial firewall!
CR 2.9 RE(1) Warn when audit record storage capacity threshold reached		X	See above.
CR 2.10 Response to audit processing failures	a) N/A	a) N/A	CR 2.10 a) N/A. Related to the core functions.

	b) X	b) X	CR 2.10 b) X *To be discussed by standardization committee:* In IEC 62443-4-2 the requirement consists of part a) and b). Since CR 2.10 a) is "N/A" and CR 2.10 b) is linked to "AND", CR 2.10 b) would actually also be "N/A". We recommend to separate a) and b).
CR 2.11 Timestamps	X	X	There shall be a time source and a time stamp.
CR 2.11 RE(1) Time synchronization	X	X	It shall be possible to synchronize the time in the system. Objective→ All logs in IACS should be comparable. Technical examples: SNTP, NTP
CR 2.11 RE(2) Protection of time source integrity			Multiple time sources can only be used from SL-4 onwards→ for robustness.
CR 2.12 Non-repudiation	X	X	Refers to configuration and not to the data passed through! → Audit logging
CR 2.12 RE(1) Non-repudiation for all users	X	X	Included for SL-2 and SL-3! It is not clear why something should *not* be logged for any reason. Difference to CR 2.12: in CR 2.12 human user logging. Examples where logging is also required: • Configuration change via API • Inputs that change the function of the firewall, e.g. releases, using key switches to open the diagnostic port *To be discussed by standardization committee:* activated by default, secure-by-default as difference between CR 2.12 and RE(1)?
NDR 2.13 Use of physical diagnostic and test interfaces	X	X	Examples of test interfaces: JTAG or other interfaces that are available/open in production, e.g. to perform initial configuration (1) Firewall only has internal test and diagnostic interfaces: Then physical access limited by a control cabinet is sufficient to fulfill the requirement. Transport is not considered here, as it is considered in CR 3.11. (2) Firewall has externally accessible test or diagnostic interfaces: Externally accessible interfaces with additional function shall be considered separately. The requirements of the standard shall then also be considered for the interface. Attack scenario: An attacker can influence the firewall to reboot, for example. In the first few seconds, the interface has a diagnostic or update function and the attacker exploits this.

			If a device has diagnostic functions open by default when booting, this shall be protected. Example protection mechanisms: Hardware jumper on the circuit board. *Rational and supplemental guidance:* Device is in locked cabinet or locked factory.
NDR 2.13 RE(1) Active monitoring		X	Objective of this requirement: Do not route the functional JTAG port to the outside! If it is, then only with authorization and possibly also monitoring. *Current state of the art:* If externally accessible JTAG interface, then automatically only SL-1 (due to NDR 2.13) or currently still unknown protection mechanisms are used. (1) see NDR 2.13 Firewall only has test and diagnostic interfaces to the inside. In this case, physical access ("scope") limited by a control cabinet is sufficient to meet the requirement. Transport is not considered here, as it is considered in CR 3.11. *To be discussed by standardization committee:* Interpretation for embedded not clear: What does authorized reading mean? Memory dump, executed sequence What does diagnosis mean? Fusing away JTAG is the current state of the art. Active monitoring can only be carried out if own firmware is running, and this does not run when influenced. Differences: NDR 2.13 is "I protect it", RE is "even if someone accesses it, it is written to log files, but no alarm is required". *Practical case:* Debug function switched on and switching on should be logged. Passive reading is already prevented by NDR 2.13. However, if authorized reading takes place, then logging is required. If authorization was implemented by the control cabinet, then the control cabinet shall be logged.

Requirement	SL-2	SL-3	Contextual mapping
FR 3 - System Integrity (SI)			
CR 3.1 Communication integrity	X	X	Standard for Integrity is CRC; Authenticity is added. SL-1: CRC possibly permissible SL-2: According to "good practice", firewall needs better protection than CRC!
CR 3.1 RE (1) Communication authentication	X	X	At this point, a distinction between (1) routed data and (2) data from/to the firewall is relevant. (1) Authentication does not have to be ensured for transmitted data. (2) Authentication shall be ensured for configuration data and other data from/to the firewall.
NDR 3.2 Protection from malicious code	X	X	(1) With a monolithic firmware image, nothing else needs to be implemented to fulfill this requirement. (2) If there is a possibility to add binaries or executable scripts at operating system level, this requirement shall be considered.
CR 3.3 Security functionality verification	X	X	CR 3.3 is a requirement for the user documentation and not a technical requirement for the firewall, because usually no test tools are supplied, but reference is made to publicly available tools. *To be discussed by standardization committee:* *(because it is more of a certification assessment):* Theoretically, everything in the 62443-4-2 should be documented in the manual as to how the operator can test whether the requirements have been implemented. This would mean that the manufacturer's requirement tests would have to be passed on to the operator. The question is what percentage shall be fulfilled: e.g. do not check every event in the audit logging.
CR 3.3 RE(1) Security functionality verification during normal operation			Only required from SL-4 onwards.
CR 3.4 Software and information integrity	X	X	(1) With a monolithic firmware image, nothing else needs to be implemented to fulfill this requirement. (2) If there is a possibility to change config. data at operating system level, this requirement shall be considered.
CR 3.4 RE(1) Authenticity of software and information	X	X	
CR 3.4 RE(2) Automated notification of integrity violations		N/A	(1) On failed boot: N/A, we cannot do automated notification. The device shall be in "Fail Close" on failed boot. (2) In case of an invalid Config→ The device can no longer be trusted. Operating errors cannot be detected, but a

			corrupted configuration can. A corrupted Config is a hard fail, i.e. the device locks everything ("Fail Close").
CR 3.5 Input validation	X	X	
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 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			Only as of SL-4.
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	Physical tamper detection is relevant during transportation; example: device seal. If necessary, device seal on packaging to detect unauthorized pre-configuration. After installation in the locked cabinet, tamper detection is no longer so critical.
NDR 3.11 (1) Notification of a tampering attempt		N/A	The component shall be protected by a tamper seal (upon transport before cabinet installation). Physical access to the component is restricted in this security profile→ locked cabinet. Modifications of the components could be seen by a broken tamper seal. The seal supports the secure delivery process. Integrators can verify the seal status after unboxing and before commissioning. *Probably only relevant from SL-4 onwards, but if the firmware has been modified, which part of the firmware should notify in case of corruption?*
NDR 3.12 Provisioning product supplier roots of trust	X	X	Typical implementation/example: Manufacturer-specific or device-specific key/certificate is uploaded during production. Device-specific trust anchors during production shall be implemented in such a way that the operator can check whether the device/software is "valid", e.g. hash value, public certificate. From production to "trust on first use" (1) NDR 3.12 Supplier root of trust, product supplier = manufacturer (2) NDR 3.13 Asset owner root of trust, asset owner = end user *Further application example:* Configuration is also encrypted and checked during transmission/use. The integrator is not explicitly mentioned here. But could be relevant.

NDR 3.13 Provisioning asset owner roots of trust	X	X	Option for the asset owner to securely store their own device certificates/keys. These shall then be securely stored, backed up and used. Examples: Web interface/TLS certificate
NDR 3.14 Integrity of the boot process	X	X	Example: Hash, certificate Integrity and Authenticity of configuration: see above
NDR 3.14 (1) Authenticity of the boot process	X	X	Example: Secure Boot

Requirement	SL-2	SL-3	Contextual mapping
FR 4 - Data confidentiality (DC)			
CR 4.1 Information confidentiality	X	X	*Rational and supplemental guidance:* Only applicable for assets that require protection. (see chap. 2.4)
CR 4.2 Information persistence	X	X	Example mechanism: Factory default button
CR 4.2 RE(1) Erase shared memory resources	X	X	State of the art: Use established encryption libraries and vulnerability update on libraries. Implement correct memory protection in case of own realization. Consideration of decommissioning (disposal, reuse, resale) Not considered: "take apart" and "desolder". *Reference:* CWE-226: "Sensitive Information in Resource Not Removed Before Reuse" (https://cwe.mitre.org/data/definitions/226.html)
CR 4.2 RE(2) Erase verification		X	*Example:* Note on the website, IP addresses are back to default, LEDs are lit. This means that assets requiring protection shall be deleted in a non-recoverable manner. Related to CR 4.2 and not to CR 4.2 RE(1). Differentiation: Is it a secure deletion or just a deletion? RE(1) For a factory reset, the device shall have the ability to erase assets requiring protecting. RE(2) Confirmation of successful erasure to user, e.g. via LED.
CR 4.3 Use of cryptography	X	X	Examples can be: HTTPS, secure boot, securing the configuration, firmware update signature

Requirement	SL-2	SL-3	Contextual mapping
FR 5 - Restricted Data Flow (RDF)			
CR 5.1 Network segmentation	X	X	Ensure that no data that is not explicitly permitted is transferred from one side to the other in all operating states→ core functions
NDR 5.2 Zone boundary protection	X	X	This is the core function of the Industrial Firewall!
NDR 5.2 (1) Deny all, permit by exception	X	X	"Deny all" means from an insecure to a secure zone (e.g. outside to inside, WAN to LAN). *Rational and supplemental guidance:* Default setting “allow-all” from LAN to WAN in most industrial firewalls introduces additional risk, see chap. 0.
NDR 5.2 (2) Island mode			See safety discussion in the "Scope" chapter
NDR 5.2 (3) Fail close	X	X	See "Scope" in particular system start-up and HW errors→ essential function
NDR 5.3 General-purpose person-to-person communication restrictions	X	X	Possible through firewall rules. It shall be possible to prevent Internet access. "Person-to-person DPI" is not required!

Requirement	SL-2	SL-3	Contextual mapping
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	X	e.g. syslog, state of the art!
CR 6.2 Continuous monitoring	X	X	e.g. Syslog

Requirement	SL-2	SL-3	Contextual mapping
FR 7 - Resource Availability (RA)			
CR 7.1 Denial of service protection	X	X	See "fail close" → Nothing unauthorized may be transmitted.
CR 7.1 RE(1) Manage communication load from component	X	X	Robustness is required. System should return to normal operating state after DoS event.
CR 7.2 Resource management	X	X	Robustness is required.
CR 7.3 Control system backup	X	X	Backup of the configuration shall be possible
CR 7.3 RE(1) Backup integrity verification	X	X	Examples: Input validation, checksum
CR 7.4 Control system recovery and reconstitution	X	X	e.g. Factory Reset, Restore Configuration
CR 7.6 Network and security configuration settings	X	X	Manual shall describe the security configuration.
CR 7.6 RE(1) Machine-readable reporting of current security settings		X	Configuration file or report file shall be machine-readable.
CR 7.7 Least functionality	X	X	Functions that are not required are deactivated by default; deactivation of other functions is explained in the manual.
CR 7.8 Control system component inventory	X	X	Device shall be able to identify itself. (device type, FW version, customer-specific device name if applicable, etc...) → Asset management

8 Security risk evaluation of the security profile

In this profile it is assumed, that the risk is already reduced by the following:

- Physical access is limited (locked control cabinet, cell, factory).

Additional risks may be introduced by the following and shall be considered additionally:

- Default setting “allow-all” from LAN to WAN in most industrial firewalls, see NDR 5.2 (1).
- If safety functions are tunneled via the firewall, the "fail-close" case of the firewall shall be considered for the safety assessment. Island operation might be necessary.

This profile can only represent a general risk assessment for industrial firewalls. However, each application scenario shall be assessed by the operator/integrator himself. Each operator may have a different "risk requirement".

8.1 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 core functions of the Industrial Firewall cannot be guaranteed.

The functionality of the Industrial Firewall is limited to ISO/OSI layer 4, but the IP stack shall 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 data assets (defined in chap. 2.5) 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.

9 Annex

9.1 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

[IEC62443-6-2] IEC TS 62443-6-2:2025, Security for industrial automation and control systems - Part 6-2: Security evaluation methodology for IEC 62443-4-2

[IEC62443-1-5] IEC TS 62443-1-5:2023, Security for industrial automation and control systems - Part 1-5: Scheme for IEC 62443 security profiles

[Use Case Industrial Firewall] TeleTrusT (2021): IEC 62443-4-2 Use Case Industrial Firewall

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 Fachleute, 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 Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

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

TeleTrusT
Pioneers in IT security.