Cyber Security Standards Compliance Guideline for IRF1000 / IRF3000

IEC62443 - IEC6112-460 - EN18031-1:2024

Firmware Version	2.2.3
Document Version	1.2
Autor	ADS-TEC IIT GmbH
Datum	2025-10-13

Vertaulich
© 2025 ADS-TEC Industrial IT GmbH

Table of Contents

1 Introduction 5
1.1 IEC62443 Standards Family . . . 5
1.1.1 Introduction . . . 5
1.1.2 Overview . . . 5
1.1.3 Structure . . . 5
1.1.4 Key Concepts . . . 6
1.1.4.1 1. Security Levels . . . 6
1.1.4.2 2. Zones and Conduits . . . 6
1.1.4.3 3. Risk Assessment . . . 6
1.1.4.4 4. Lifecycle Security . . . 6
1.1.5 Implementation Benefits . . . 6
1.1.6 Conclusion . . . 7
1.2 DNV Cybersecurity Framework . . . 7
1.2.1 DNV Cybersecurity Requirements . . . 7
1.2.2 Mapping IEC 62443 CRs to DNV Expectations . . . 7
1.3 EN18031-1:2024 (RED) . . . 7
1.3.1 EN 18031-1 for ADS-TEC IIT IRF-Series . . . 7
1.3.2 Alignment with IEC 62443-4-2 . . . 8
1.3.3 Implications for IRF-Series . . . 8
1.3.4 Conclusion . . . 8
1.4 About this document . . . 8
1.4.1 Release Notes . . . 9
1.4.2 Document history . . . 9
1.4.3 Roadmap . . . 9
1.4.4 Latest Firmware Versions (at time of release) . . . 9
1.5 Limitation . . . 9
2 Mapping IEC62443-4-2 9
FR 1 Identification and authentication control . . . 10
CR 1.1 Human user identification and authentication . . . 10
CR 1.2 Software process and device identification and authentication . . . 11
CR 1.3 Account management . . . 12
CR 1.4 Identifier management . . . 12
CR 1.5 Authenticator management . . . 13
CR 1.6 Wireless access management . . . 14
CR 1.7 Strength of password-based authentication . . . 14
CR 1.8 Public key infrastructure certificates . . . 15
CR 1.9 Strength of public key-based authentication . . . 16
CR 1.10 Authenticator feedback . . . 17
CR 1.11 Unsuccessful login attempts . . . 18
CR 1.12 System use notification . . . 18

© 2025 ADS-TEC Industrial IT GmbH

CR 1.13 Access via untrusted networks . . . 19
CR 1.14 Strength of symmetric key-based authentication . . . 20
FR 2 Use control . . . 21
CR 2.1 Authorization enforcement . . . 21
CR 2.2 Wireless use control . . . 22
CR 2.3 Use control for portable and mobile devices . . . 22
CR 2.4 Mobile code . . . 23
CR 2.5 Session lock . . . 24
CR 2.6 Remote session termination . . . 25
CR 2.7 Concurrent session control . . . 26
CR 2.8 Auditable events . . . 27
CR 2.9 Audit storage capacity . . . 28
CR 2.10 Response to audit processing failures . . . 29
CR 2.11 Timestamps . . . 30
CR 2.12 Non-repudiation . . . 30
CR 2.13 Use of physical diagnostic and test interfaces . . . 31
FR 3 System integrity . . . 32
CR 3.1 Communication integrity . . . 32
CR 3.2 Protection from malicious code . . . 33
CR 3.3 Security functionality verification . . . 33
CR 3.4 Software and information integrity . . . 34
CR 3.5 Input validation . . . 35
CR 3.6 Deterministic output . . . 35
CR 3.7 Error handling . . . 36
CR 3.8 Session integrity . . . 37
CR 3.9 Protection of audit information . . . 38
CR 3.10 Support for updates . . . 39
CR 3.11 Physical tamper resistance and detection . . . 40
CR 3.12 Provisioning product supplier roots of trust . . . 40
CR 3.13 Provisioning asset owner roots of trust . . . 41
CR 3.14 Integrity of the boot process . . . 42
FR 4 Data confidentiality . . . 43
CR 4.1 Information confidentiality . . . 43
CR 4.2 Information persistence . . . 44
CR 4.3 Use of cryptography . . . 44
FR 5 Restricted data flow . . . 47
CR 5.1 Network segmentation . . . 47
CR 5.2 Zone boundary protection . . . 48
CR 5.3 General-purpose person-to-person communication restrictions . . . 49
FR 6 Timely response to events . . . 50
CR 6.1 Audit log accessibility . . . 50
CR 6.2 Continuous monitoring . . . 50
FR 7 Resource availability . . . 51

© 2025 ADS-TEC Industrial IT GmbH

CR 7.1 Denial of service protection 51
CR 7.2 Resource management 52
CR 7.3 Control system backup 52
CR 7.4 Control system recovery and reconstitution 53
CR 7.5 Emergency power 54
CR 7.6 Network and security configuration settings 54
CR 7.7 Least functionality 55
CR 7.8 Control system component inventory 56

© 2025 ADS-TEC Industrial IT GmbH

1 Introduction

1.1 IEC62443 Standards Family

1.1.1 Introduction

IEC 62443 is a comprehensive set of standards developed by the International Electrotechnical Commission (IEC) aimed at improving the cybersecurity of Industrial Automation and Control Systems (IACS).

The standards provide a structured approach to address and mitigate security vulnerabilities in industrial environments. Here's a summary of its key components and objectives:

1.1.2 Overview

Purpose: The primary goal of IEC 62443 is to establish a systematic and robust framework to ensure the security and resilience of IACS. It addresses security threats at various levels, from individual components to entire systems, emphasizing both preventive and responsive measures.

Scope: The standards apply to various sectors, including manufacturing, energy, water, transportation, and other critical infrastructure industries. They cater to all stakeholders, including system integrators, asset owners, component suppliers, and service providers.

1.1.3 Structure

IEC 62443 is divided into four main categories:

1. General (Series 1)

- IEC 62443-1-1: Terminology, concepts, and models
- IEC 62443-1-2: Master glossary of terms
- IEC 62443-1-3: System security conformance metrics
- IEC 62443-1-4: IACS security lifecycle and use-case models

2. Policies and Procedures (Series 2)

- IEC 62443-2-1: Establishing an IACS security program
- IEC 62443-2-2: IACS protection profiles
- IEC 62443-2-3: Patch management in the IACS environment
- IEC 62443-2-4: Security program requirements for IACS service providers

3. System (Series 3)

- IEC 62443-3-1: Security technologies for IACS
- IEC 62443-3-2: Security risk assessment and system design
- IEC 62443-3-3: System security requirements and security levels

© 2025 ADS-TEC Industrial IT GmbH

4. Component (Series 4)

- IEC 62443-4-1: Secure product development lifecycle requirements
- IEC 62443-4-2: Technical security requirements for IACS components

6. Component (Series 6)

- IEC 62443-6-1: Security evaluation methodology for IEC 62443-2-4
- IEC 62443-6-2: Security evaluation methodology for IEC 62443-4-2

1.1.4 Key Concepts

1.1.4.1 1. Security Levels

IEC 62443 defines four security levels (SLs) that represent the robustness of security measures:

- **SL 1:** Protection against casual or coincidental violation
- **SL 2:** Protection against intentional violation using simple means with low resources, generic skills, and low motivation
- **SL 3:** Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation
- **SL 4:** Protection against intentional violation using sophisticated means with extensive resources, IACS-specific skills, and high motivation

1.1.4.2 2. Zones and Conduits

The standards introduce the concept of dividing an IACS into security zones and conduits.

- **Zones:** Logical or physical groupings of assets with similar security requirements
- **Conduits:** Communication paths between these zones

1.1.4.3 3. Risk Assessment

A systematic approach to identifying, assessing, and mitigating risks is central to IEC 62443. It emphasizes the need for regular risk assessments to adapt to evolving threats.

1.1.4.4 4. Lifecycle Security

Security considerations must be integrated throughout the entire lifecycle of IACS, from design and development through operation and maintenance to decommissioning.

1.1.5 Implementation Benefits

- **Enhanced Security Posture:** By adhering to IEC 62443, organizations can significantly reduce their vulnerability to cyber threats.
- **Regulatory Compliance:** Helps in meeting industry-specific regulatory requirements and standards.
- **Operational Continuity:** Minimizes the risk of disruptions in industrial operations due to cyber incidents.

© 2025 ADS-TEC Industrial IT GmbH

- **Stakeholder Confidence:** Builds trust among customers, partners, and regulators by demonstrating a commitment to cybersecurity.

1.1.6 Conclusion

IEC 62443 serves as a vital resource for securing industrial automation and control systems against the increasing threats of cyber-attacks.

Its comprehensive approach, covering policies, procedures, systems, and components, provides a robust framework for organizations to protect their critical infrastructure effectively. Implementing these standards not only enhances security but also ensures compliance, operational continuity, and stakeholder confidence.

1.2 DNV Cybersecurity Framework

1.2.1 DNV Cybersecurity Requirements

DNV has introduced a set of rules, class programmes, and guidelines that establish the framework for type approval of cyber-secure components and systems. For ADS-TEC IRF devices, compliance with IEC 62443 and IEC 61162-460 must be mapped against the corresponding DNV requirements to ensure eligibility for type approval and the class notation **Cyber secure**.

The most relevant DNV documents are:

- **DNV-CP-0231** – **Cyber security capabilities of systems and components**: Defines the type approval scheme for cyber security capabilities and references IEC 62443-4-2 as the baseline standard. The achieved security level (SL) must be declared in the type approval certificate.
- **DNV-CG-0325** – **Cyber secure**: Provides detailed guidance aligned with IACS UR E26/E27. It specifies how IEC 62443 requirements shall be applied in the maritime context and identifies which functions must meet which SL.
- **DNV-RU-SHIP Pt.6 Ch.5 Sec.21** – **Cyber secure rules**: Binding class rules that specify the minimum cyber security barriers and documentation requirements for vessels with the **Cyber secure** notation.
- **DNV-CG-0550** – **Maritime services – terms and systematics**: Defines documentation categories (F011, F021, F252, etc.) that are submitted as compliance evidence for cyber security requirements.

1.2.2 Mapping IEC 62443 CRs to DNV Expectations

For each IEC 62443-4-2 security requirement (CR), the following aspects will be documented:

1 **IEC 62443 Requirement** – The formal technical requirement from IEC 62443-4-2.

2 **IRF Capability** – The level of security that IRF devices support (for the current generation, up to **SL3**).

3 **DNV Expectation** – The acceptance criteria for type approval, referencing CP-0231, CG-0325, and RU-SHIP rules. This shows whether SL2 is sufficient or if higher levels (SL3–SL4) may be required in specific applications.

4 **Maritime Relevance** – Links to IEC 61162-460 where applicable, ensuring alignment with maritime access control, secure area separation, and interface security requirements.

1.3 EN18031-1:2024 (RED)

1.3.1 EN 18031-1 for ADS-TEC IIT IRF-Series

© 2025 ADS-TEC Industrial IT GmbH

The **IRF-Series firewall and router family** is marketed as **CE-conformant products** within the European Union. As such, they fall under the framework of **EN 18031-1:2024** (**Information technology security evaluation – Security evaluation for industrial automation and control systems – Part 1: General requirements**). EN 18031-1 is a **horizontal standard** for cybersecurity evaluation of industrial products, providing a European framework for security features that must be assessed for **CE-marked devices**. It ensures that cybersecurity requirements are systematically addressed **alongside traditional safety and EMC requirements** in the conformity process.

1.3.2 Alignment with IEC 62443-4-2

To ensure consistency with established industrial automation security frameworks, **Annex B of EN 18031-2:2024** provides a **direct mapping** between the EN 18031 evaluation classes and the **IEC 62443-4-2:2019 component requirements (CRs).**

This mapping enables a traceable link between:

- EN 18031-1 horizontal requirements for CE compliance
- IEC 62443-4-2 component requirements for industrial cybersecurity
- Device-specific implementation on IRF-Series interfaces (**Web-UI, JSON-RPC API, Big-LinX VPN, Firewalling**)

1.3.3 Implications for IRF-Series

For the IRF-Series, this means:

- Each of the **47 IEC 62443-4-2 CRs** is aligned with EN 18031-1 through a mapping of the 47 CRs to each **“EN18031-1 Interface.”**
- Where **Annex B of EN 18031-2** provides mappings (e.g. **Access Control → CR 1.x, Secure Communication → CR 4.x, Logging → CR 6.x**), these are systematically applied in the development process.
- This ensures that **notified bodies** and **class societies** can trace the IRF feature set simultaneously against both IEC 62443 and EN 18031 requirements.

1.3.4 Conclusion

By applying **EN 18031-1** as the horizontal standard, and using **Annex B of EN 18031-2** to link into **IEC 62443-4-2**, the IRF-Series provides:

- **CE conformity evidence** for the European market

1.4 About this document

This document evaluates each of the **47 component requirements (CRs) of IEC 62443-4-2** in four functional areas of the **ADS-TEC Industrial IT IRF1000 and IRF3000** products:

- **Remote access** via Big-LinX VPN (remote maintenance use case)
- **Administration** via Web-UI and JSON-RPC API
- **Firewalling and network policy enforcement**
- **Physical Access Device Protection**

For each CR, the document:

- Describes how the IRF-Series implements the requirements

© 2025 ADS-TEC Industrial IT GmbH

- Identifies the applicable firmware version and models

This structure ensures **traceability** between product configuration, IEC 62443 component requirements, and the **maritime class requirements** applied by DNV.

1.4.1 Release Notes

This document is released together with and updated for each software version of the mentioned products.

- The **first version** containing IEC 62443 features for IRF1000 and IRF3000 was **2.0.0**.
- **All previous versions** cannot be regarded as IEC 62443 compliant due to their **legacy authentication mechanism**.

1.4.2 Document history

The **document history** provides a chronological overview of the document updates.

- 1.0: Initial document on version 2.2.3 was published on **2025-09-16**.
- 1.1: Update with clarifications on **2025-10-09**.
- 1.2: Update with clarifications on **2025-10-13**.

1.4.3 Roadmap

This document also provides the **current feature roadmap**, highlighting:

- Capabilities that are already implemented
- Capabilities that are planned in order to fulfill specific security requirements

1.4.4 Latest Firmware Versions (at time of release)

- **IRF1000:** 2.2.3
- **IRF3000:** 2.2.3

1.5 Limitation

All listed features have been developed over the past **20 years** of ADS-TEC industrial firewall software development, with great caution and security awareness.

However, the **ADS-TEC Industrial IT secure development process** has **not yet been certified** according to **IEC 62443-4-1**. Therefore, all features remain subject to **re-factoring** once the final certification process begins in **2025**.

All listed features have **not yet been certified or validated** according to **IEC 62443-6-2** by any external certification authority.

All planned future software features are **subject to change** due to the above limitations.

2 Mapping IEC62443-4-2

FR 1 Identification and authentication control

Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets.

CR 1.1 Human user identification and authentication

Components shall provide the capability to identify and authenticate all human users according to IEC 62443 3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.

NOTE Applicable security policies are a local matter

CR 1.1 (1) Unique identification and authentication (SL2)

CR 1.1 (2) Multifactor authentication for all interfaces (SL3)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	For every interface designed as a user interface, such as Web-UI or JSON-RPC, the device mandates authentication. The password for each user can be configured at: **Configuration -> Access Control -> User Accounts** There are two other interface APIs which are designed for interaction with other software only. SNMP and the ADS-TEC proprietary ADSDP. ADSDP is mapped to the same user accounts as the JSON/RPC API but is disabled after the device is commissioned (since version 2.2.0) SNMPv3 users are mapped to the same user accounts as the JSON/RPC API but with a separate SNMP service password.(since version 2.2.0)	IRF1 IRF3	2.0.0
SL2	Additionally required to SL1: There should be created one user on the device for every user which has to access the device. The password for each user can be configured at: Configuration -> Access Control -> User Accounts	IRF1 IRF3	2.0.0
SL3	Multi-factor authentication is not yet implemented. A method using HTTPS Client Certificates will be added with the given future version.	IRF1 IRF3	3.1.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	For CR 1.1 (human authentication) → Big-LinX credentials are out of scope, since they represent device identity. -> CR 3.5 (Device authentication) – Big-LinX VPN credentials (card or certificate) are evaluated there as part of system integrity / device identity.	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	The IRF packet filter operates on network addresses and ports. It does not identify or authenticate individual human users, and thus does not contribute to CR 1.1 (human identification and authentication). In some deployments, a Big-LinX VPN tunnel may assign a per-user IP, which allows firewall rules to be applied indirectly per user. However, this is a function of the VPN service, not of the packet filter itself.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	The IRF's physical user interfaces (buttons, USB ports, SD card slots, I/Os, Ethernet connectors) do not provide logical sessions with human identification or authentication. Therefore, CR 1.1 is not applicable to these interfaces. Security context: Access to these interfaces is controlled by physical protection measures (cabinet locks, restricted areas, tamper seals). Cross-reference: Physical protection measures are covered under IEC 62443 FR-7 (Resource availability)	IRF1 IRF3	n/a

CR 1.2 Software process and device identification and authentication

Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to IEC 62443 3-3 SR1.2. If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to IEC 62443 3-3 SR1.1 may be part of the component identification and authentication process towards the other components.

CR 1.2 (1) Unique identification and authentication (SL3)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2, GEC-3

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	Each user logs in with unique username + password. Sessions are tied to the specific account. Passwords stored hashed (Argon2). Enforce unique accounts can be configured for a individual due to multi user authentication system. Session binding ensures all user actions are attributable. Audit logs link session IDs to usernames. Configuration -> Access Control -> User Accounts	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Big-LinX credentials are out of scope, since they represent device identity. Thus CR 1.x is not applicable.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	The IRF packet filter operates on network addresses and ports. It does not identify or authenticate individual human users, and thus CR 1.x is not applicable.	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	The IRF's physical user interfaces (buttons, USB ports, SD card slots, I/Os, Ethernet connectors) do not provide logical sessions with human identification or authentication. Therefore, CR 1.x is not applicable to these interfaces.	IRF1 IRF3	n/a

CR 1.3 Account management

Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to IEC 62443 3-3 SR 1.3.

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	The device itself can natively manage accounts as described in Configuration -> Access Control -> User Accounts. An integration in a high level management system is not implemented yet but might be released in a future firmware version depending on customer requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	CR 1.x is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.x is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.x is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.4 Identifier management

Components shall provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to IEC 62443 3-3 SR 1.4.

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	The device itself can natively manage accounts as described in Configuration -> Access Control -> User Accounts. An integration in a high level management system is not implemented yet but will be released in a future firmware version.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	CR 1.4 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.4 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.4 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.5 Authenticator management

Components shall provide the capability to:

a) support the use of initial authenticator content;

b) support the recognition of changes to default authenticators made at installation time;

c) function properly with periodic authenticator change/refresh operation; and

d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.

CR 1.5 (1) Hardware security for authenticators (SL3)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2, AUM-3, AUM-4

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Requirements are fulfilled by the device itself: a) Password for initial setup for user 'admin' is set by default. b) After login, the Config Wizard forces the user to change the password in the WebUI. If the password is not changed, the initial setup wizard cannot be finished. c) Passwords can be changed anytime via WebUI. d) Passwords are stored in hashed form with the Argon2 algorithm and all password fields are masked with bullets. Access via WebUI is only possible with HTTPS. We recommend that all passwords should be rotated regularly.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL2	For Big-LinX VPN, there is no factory default authenticator. Instead, the initial authenticator (software certificate, pre-shared key, or optional hardware token) must always be provisioned by the administrator before VPN use. This ensures that no default values exist at delivery. Authentication credentials for Big-LinX VPN (certificates or optional hardware tokens) can be updated or rotated by the administrator. All credentials are stored securely (in smartcards or protected device configuration) and transmitted only via encrypted channels.	IRF1 IRF3	2.0.0
SL3	Big-LinX VPN optionally supports hardware token–based authenticators (smartcards with PIV applet) that securely store X.509 certificates for VPN authentication. This meets the SL3 requirement for hardware-backed protection where tokens are deployed, while ensuring administrative control of all authenticators.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
SL3	Big-LinX VPN already supports hardware token–based authentication (smartcards with PIV applet). With the future version this will be extended to store the software certificates which are provisioned to the device in a OpTee based certificate store which provides hardware based security as well.	IRF14x2 IRF1 IRF3	3.1.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.5 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.5 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.6 Wireless access management

CR 1.6 / NDR 1.6 – Wireless access management

The wireless access management requirements are network-component-specific and can be located as requirements for network-components in Clause 15.

NDR 1.6 – Wireless access management (SL1)

NDR 1.6. (1) Unique identification and authentication (SL2)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	CR 1.6 is only partially applicable, as the IRF does not act as a wireless access point. For WWAN/WLAN client modes, authentication is managed externally by the mobile provider or access point infrastructure. The IRF enforces identical authentication for all management interfaces regardless of transport medium. Administrators can also disable management access over wireless interfaces. This implementation satisfies the intent of CR 1.6 where applicable and covers the requirements of SL1–SL3.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	CR 1.6 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.6 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.6 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.7 Strength of password-based authentication

For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to

© 2025 ADS-TEC Industrial IT GmbH

internationally recognized and proven password guidelines

CR 1.7 (1) Password generation and lifetime restrictions for human users (SL3)

CR 1.7 (2) Password lifetime restrictions for all users (human, software process, or device) (SL4)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2, AUM-5, AUM-6

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL2	The password policy can be enabled globaly. If it is enabled the password entropy must be high according to the zxcvbn algorithmn. This algorithm checks the strength of passwords for more than just length and complexity and is an internationally recognized standard for password strength. The devices do not support external authentication. The reuse of old passwords can be disabled by configurable policy.	IRF1 IRF3	2.0.0
SL3	The lifetime of passwords can be configured. To enhance security, you can configure the system to store a specified number of password hashes. This prevents the reuse of passwords. Additionally, you can set the lifetime of passwords to further enforce regular updates.	IRF1 IRF3	2.1.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	not applicable as Big-LinX VPN uses only certificate based authentication	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.7 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.7 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.8 Public key infrastructure certificates

When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with IEC 62443-3- 3 SR1.8.

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	The device supports X.509 certificates with full PKI/CA integration. Certificates can be uploaded and managed via Configuration → General Settings → Certificates and assigned for HTTPS Web-UI access. Details on supported cryptographic algorithms are documented in CR 4.3 – Use of cryptography (Web-UI). For using your own certificate for the Web interface HTTPS access: 1. Upload the certificate into the Certificate Store: Configuration -> General Settings -> Certificates 2. Configure the web server to use this certificate: Configuration -> Services -> Web Server	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL3	All Big-LinX VPN authentication certificates are issued by a managed PKI infrastructure at ADS-TEC Industrial IT and its associated partner companies. Details on negotiated TLS and VPN cryptographic algorithms are documented in CR 4.3 – Use of cryptography (Big-LiNX VPN).	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.8 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.8 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.9 Strength of public key-based authentication

For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to:

a) validate certificates by checking the validity of the signature of a given certificate;

b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;

c) validate certificates by checking a given certificate's revocation status;

d) establish user (human, software process or device) control of the corresponding private key;

e) map the authenticated identity to a user (human, software process or device); and

f) ensure that the algorithms and keys used for the public key authentication conform to 8.5. (CR4.3)

CR 1.9 (1) Hardware security for public key-based authentication (SL3)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2, CCK-1

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL2	The Web-UI / JSON-RPC API HTTPS-Server supports X.509 certificates with public key infrastructure (PKI) and certification authority (CA). Certificates can be uploaded and managed at: Configuration → General Settings → Certificates. The device validates certificate signatures, certificate chains, and revocation status via CRLs. Self-signed certificates can also be deployed if explicitly distributed to all peers. The authenticated identity is mapped via the certificate subject (CN or DN).	IRF1 IRF3	2.0.0
SL3	The Private Key of the HTTPS Web Server will be stored in a hardware security based certificate engine. This engine uses a NXP SoC based Op-Tee secure application.	IRF1 IRF3	3.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL2	Big-LiNX VPN supports authentication with X.509 certificates issued by the ADS-TEC managed PKI infrastructure. Certificates are validated against the CA chain, including signature and revocation status checks. The authenticated identity is mapped using the certificate subject (CN or DN).	IRF1 IRF3	2.0.0
SL3	For SL3, Big-LiNX VPN supports the use of smartcards with PIV applets as hardware tokens. These smartcards securely store private keys and perform cryptographic operations outside of the device, ensuring hardware-based protection of authenticators as required by IEC 62443 SL3.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.9 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.9 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.10 Authenticator feedback

When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authenticator information during the authentication process.

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2, AUM-3

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device itself provides the capability to obscure feedback of authenticator information during authentication. This includes masking password input fields with bullets/asterisks.	IRF1 IRF3	2.0.0
SL2	no additional requirements	IRF1 IRF3	2.0.0
SL3	no additional requirements	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	CR 1.10 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.10 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.10 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.11 Unsuccessful login attempts

When a component provides an authentication capability, the component shall provide the capability to:

a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and

b) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached. An administrator may unlock an account prior to the expiration of the timeout period.

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2, AUM-6

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	The device can enforce limits on unsuccessful login attempts by any user (human, software process, or device). It provides the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts during a configurable time period. b) deny access for a specified period of time or until unlocked by an administrator once the limit has been reached. Configuration path: WebUI -> Configuration -> Access control -> User accounts -> Security	IRF1 IRF3	2.1.3

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	CR 1.11 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.11 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.11 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.12 System use notification

When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

© 2025 ADS-TEC Industrial IT GmbH

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	The device shall provide the capability to display a configurable system use notification message before authentication when local human user access/HMI is provided. The notification message can be customized by authorized personnel. It should typically state: - The system is the property of the asset owner. - System usage may be monitored, recorded, and audited. - Unauthorized use is prohibited and may result in penalties. - By using the system, the user consents to monitoring. Implementation on IRF1000/IRF3000: This capability is provided via configurable login banners. Configuration path: WebUI -> Configuration -> Access control -> User accounts -> Security / Banner	IRF1 IRF3	2.1.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	CR 1.12 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.12 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.12 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.13 Access via untrusted networks

CR 1.13 / NDR 1.13 – Access via untrusted networks

The access via untrusted networks requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

NDR 1.13 – Access via untrusted networks (SL1)

NDR 1.13. (1) Explicit access request approval (SL3)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device provides access control for its WebUI/API. Access can be restricted to specific trusted interfaces. Configuration path: WebUI → Configuration → Access Control → Web Access.	IRF1 IRF3	2.0.0
SL2	Same as SL1. No additional requirements.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	To facilitate this feature, users must use one of the devices VPN features to first establish a secure interface and then disable all other untrusted networks in general but the access over the VPN interfaces. The VPN interface itself must then be controlled by a physical key switch which will allow explicit access request approval.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL3	Big-LinX VPN can be controlled by a physical key switch or a similar API call on the Web UI JSON/RPC interface to provide explicit access request approval	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	The device contains extensive packet filter functions to provide access protection from untrusted to trusted networks and vice versa	IRF1 IRF3	2.0.0
SL3	The packet filter rules can be configured with relation to physical input switch which allows explicit access request approval.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.13 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

CR 1.14 Strength of symmetric key-based authentication

For components that utilize symmetric keys, the component shall provide the capability to:

a) establish the mutual trust using the symmetric key;

b) store securely the shared secret (the authentication is valid as long as the shared secret remains secret);

c) restrict access to the shared secret; and

d) ensure that the algorithms and keys used for the symmetric key authentication conform to 8.5.

CR 1.14 (1) Hardware security for symmetric key-based authentication (SL3)

EN 18031-1 mapping: ACM-1, ACM-2, AUM-1, AUM-2, CCK-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
n/a	n/a, the Web UI does not use symmetric key-based authentication.	IRF1 IRF3	n/a

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a, symmetric key-based authentication is not used for Big-LinX VPN	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 1.14 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 1.14 is not applicable, for justification please refer to CR 1.1	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

FR 2 Use control

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

CR 2.1 Authorization enforcement

Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.

CR 2.1 (1) Authorization enforcement for all users (humans, software processes and devices) (SL2)

CR 2.1 (2) Permission mapping to roles (SL2)

CR 2.1 (3) Supervisor override (SL3)

CR 2.1 (4) Dual approval (SL4)

EN 18031-1 mapping: ACM-1, ACM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The implemented user identities of the devices and the related user rights and permissions can be assigned to the user.	IRF1 IRF3	2.0.0
SL2	Role based concepts are not implemented yet. In the implemented concept identities/users are (single) roles. At this point you have to configure every identity with the permissions you want to give those identities. Role based concept will be implemented in a future firmware version. The main improvement comparing to the current implementation will be that the "admin" users username will no longer be hard coded.	IRF1 IRF3	3.0.0
SL3	There is no use case for a global supervisor override of all functions on the Web-UIs authorization enforcement. The device supports supervisor override regarding the VPN and packet filter functions. Therefore this component requirement is not applicable regarding the Web-UI interface.	IRF1 IRF3	n/a

SL	Functional Area: Big-LinX VPN	Products	Version
SL3	It is possible to use the Digital Inputs of the devices (IRF1000: 1x Digital Inputs, IRF34X1: 2 x Digital Inputs, IRF38x1: 5 Digital Inputs) to active/deactivate the VPN channel. Use the "VPN Key Switch Big-LinX" feature in the Web UI to enable this functionality: Configuration -> VPN -> Big-LinX	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL3	It is possible to use the Digital Inputs of the devices (IRF1000: 1x Digital Inputs, IRF34X1: 2 x Digital Inputs, IRF38x1: 5 Digital Inputs) to active/deactivate packet filter rules. Use the Paket Filter Wizard to configure rules which depend on a state of the Digital Inputs. By using this feature it is possible to implement a supervisor override for specific data streams.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	The security context of the product relies on physical protection of the device. Therefore authorization enforcement is not applicable for all physical interfaces of the device.	IRF1 IRF3	n/a

CR 2.2 Wireless use control

If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.

EN 18031-1 mapping: ACM-1, ACM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device can restrict management access via wireless connections. Critical actions can be denied to wireless devices by deactivating Web Access for wireless interfaces. Configuration → Access Control → Web Access.	IRF1 IRF3	2.0.0
SL2	Same as SL1. No additional requirements.	IRF1 IRF3	2.0.0
SL3	Same as SL1. No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	The BLX VPN can be used as an extended mechanism to secure wireless-originated access to the WebUI/API. Access from untrusted wireless networks is denied unless a secure VPN tunnel is established. This ensures that wireless usage is restricted and monitored, and that management access is only possible through explicitly authorized VPN connections.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	The device's integrated packet filter can restrict management access based on interface type (wired vs. wireless). This ensures that critical actions cannot be performed via wireless networks unless explicitly allowed.	IRF1 IRF3	2.0.0
SL2	Same as SL1.	IRF1 IRF3	2.0.0
SL3	Same as SL1.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 2.2 is not applicable, for justification please refer to CR 2.1	IRF1 IRF3	n/a

CR 2.3 Use control for portable and mobile devices

There is no component level requirement associated with IEC 62443 3-3 SR 2.3.

© 2025 ADS-TEC Industrial IT GmbH

EN 18031-1 mapping: ACM-1, ACM-2

CR 2.4 Mobile code

CR 2.4 / NDR 2.4 – Mobile code

The use control requirements for mobile code are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

NDR 2.4 – Mobile code (SL1)

NDR 2.4. (1) Mobile code authenticity check (SL2)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Mobile code execution is implemented by a Docker Engine. If the Docker Engine is disabled, no mobile code can be run. In any case the mobile code run by the integrated docker engine can not influence the Web-UI and is not related in any way but the Web UI is the main interface to enabled the code authenticity check.	IRF1 IRF3	2.0.0
SL2	It is recommended to allow only carefully checked custom docker images if the Docker Engine is enabled. To use code authenticity check private Docker Registries must be used: • Docker containers can only be pulled using a Docker Registry secured with TLS (X.509). • A private Docker Registry must be used containing only authorized and security-checked containers. • Public Docker Registries like hub.docker.com must be disabled.	IRF1 IRF3	2.0.0
SL3	Same as SL2. No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Mobile code execution is implemented by a Docker Engine. If the Docker Engine is disabled, no mobile code can be run. The mobile code can interact with the Big-LinX VPN as the Docker Engine is integrated with a separate virtual network interface, and its traffic is routed and filtered like any other physical IP network interface.	IRF1 IRF3	2.0.0
SL2	It is recommended to allow only carefully checked custom docker images if the Docker Engine is enabled: • Docker containers can only be pulled using a Docker Registry secured with TLS (X.509). • A private Docker Registry must be used containing only authorized and security-checked containers. • Public Docker Registries like hub.docker.com must be disabled.	IRF1 IRF3	2.0.0
SL3	Same as SL2. No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	Mobile code execution is implemented by a Docker Engine. If the Docker Engine is disabled, no mobile code can be run. The mobile code network interface is filtered like any other physical interface by the integrated packet filter.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL2	It is recommended to allow only carefully checked custom docker images if the Docker Engine is enabled: • Docker containers can only be pulled using a Docker Registry secured with TLS (X.509). • A private Docker Registry must be used containing only authorized and security-checked containers. • Public Docker Registries like hub.docker.com must be disabled.	IRF1 IRF3	2.0.0
SL3	Same as SL2. No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Mobile code execution is implemented by a Docker Engine. If the Docker Engine is disabled, no mobile code can be run. There is no interface to upload mobile code (Docker images) without network connectivity to a Docker Registry.	IRF1 IRF3	n/a

CR 2.5 Session lock

If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability

a) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and

b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device provides automated logout after inactivity as well as a manual logout button which terminates the session. Every user login results in a new session. The session timeout value can be configured.	IRF1 IRF3	2.1.0
SL2	Same as SL1. No additional requirements.	IRF1 IRF3	2.1.0
SL3	Same as SL1. No additional requirements.	IRF1 IRF3	2.1.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Under a broad interpretation of CR 2.5, the Big-LiNX VPN connection can be regarded as a “session.” The device supports a configurable inactivity timeout for the VPN tunnel, after which the channel is automatically terminated. A VPN session can also be terminated manually by the user or administrator. If the configured conditions (e.g., VPN Digital Input switch) still permit access, the channel can be re-enabled by the WWH control channel. This interpretation is beyond the literal wording of CR 2.5, which only applies to human user interfaces, but is provided here to meet auditor expectations.	IRF1 IRF3	2.1.0
SL2	Same as SL1. No additional requirements.	IRF1 IRF3	2.1.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
SL3	Same as SL1. No additional requirements.	IRF1 IRF3	2.1.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	n/a – The packet filter operates at the network layer and does not provide a user session. Session lock is not applicable.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	n/a – The device does not provide a local HMI session. All management is remote via WebUI/API, where session lock is implemented.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

CR 2.6 Remote session termination

If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device provides the capability to terminate remote sessions automatically after a configurable timeout of inactivity or by manual termination through the WebUI. This ensures that abandoned remote sessions do not remain active indefinitely.	IRF1 IRF3	2.0.0
SL2	Same as SL1. No additional requirements.	IRF1 IRF3	2.0.0
SL3	Same as SL1. No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Under a broad interpretation of CR 2.6, a VPN tunnel is regarded as a “session.” The Big-LinX VPN can be terminated automatically via inactivity timeout or manually by the user/administrator. Additionally, the VPN channel can be switched off locally using a digital input. This ensures that VPN channels do not remain active indefinitely without authorization.	IRF1 IRF3	2.0.0
SL2	Same as SL1. No additional requirements.	IRF1 IRF3	2.0.0
SL3	Same as SL1. No additional requirements.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	n/a – The packet filter operates at the network layer and does not establish or maintain user sessions. Session termination is not applicable.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	n/a – The device does not provide a local HMI session. All management is remote via WebUI/API or VPN, where session termination is implemented.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

CR 2.7 Concurrent session control

Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	no requirements	IRF1 IRF3	2.0.0
SL3	The number of concurrent sessions for the web-UI is limited to 20 session for each user account.	IRF1 IRF3	2.2.4

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	n/a – CR 2.7 requires limiting concurrent sessions per user. Big-LinX VPN supports only a single VPN tunnel per device, so concurrent session control is not applicable.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	n/a – The packet filter operates at the network layer and does not provide user sessions. Session control is not applicable.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	n/a – The device does not provide a local HMI session. All management is remote via WebUI/API or VPN, where session handling is implemented.	IRF1 IRF3	n/a
SL2	Same as SL1.	IRF1 IRF3	n/a
SL3	Same as SL1.	IRF1 IRF3	n/a

CR 2.8 Auditable events

Components shall provide the capability to generate audit records relevant to security for the following categories:

a) access control;

b) request errors;

c) control system events;

d) backup and restore event;

e) configuration changes; and

f) audit log events.

Individual audit records shall include:

a) timestamp;

b) source (originating device, software process or human user account);

c) category;

d) type;

e) event ID; and

f) event result.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device implements a Eventlog as internal Syslog Server. A Remote Syslog Server can be configured to store all events.	IRF1 IRF3	2.0.0
SL1	Extended function with 2.2.0: The device itsself has a special audit logging system for all kind of events. Events are stored in the audit log file in the local flash memory of the device. Logging of all system relevant events is activated by default and cannot be deactivated. Events include system start, stop, configuration changes, login/logout attempts, errors, and warnings. The audit log file can be exported via WebUI in its raw format for external analysis.	IRF1 IRF3	2.2.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL2	no additional requirements	IRF1 IRF3	2.0.0
SL2	no additional requirements	IRF1 IRF3	2.2.0
SL3	no additional requirements	IRF1 IRF3	2.0.0
SL3	no additional requirements	IRF1 IRF3	2.2.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	The Eventlog records all Big-LinX events. A Remote Syslog server can be configured to store them.	IRF1 IRF3	2.0.0
SL1	Extended functionality: The Audit Log will be extended to report application specific Events for Big-LinX VPN connections. They will be stored persistently on the device itself.	IRF1 IRF3	2.2.4
SL2	no additional requirements	IRF1 IRF3	2.0.0
SL3	no additional requirements	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	The packet filter firewall can be configured with rules that generate Audit Log Events if the rule matches. The number of these Events is limited to prevent a flooding of the Audit Log.	IRF1 IRF3	2.2.0
SL2	no additional requirements	IRF1 IRF3	2.2.0
SL3	no additional requirements	IRF1 IRF3	2.2.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The Eventlog of the device will report system startup events. This is the primary indicator of physical tampering of the power supply if the device. A Remote Syslog Server can be configured to store these events.	IRF1 IRF3	2.0.0
SL1	The Audit Log will be extended to report application specific Events for Device Events like USB device insertion or I/O Events, or Ethernet Link Events	IRF1 IRF3	2.2.4
SL2	no additional requirements	IRF1 IRF3	2.0.0
SL3	no additional requirements	IRF1 IRF3	2.0.0

CR 2.9 Audit storage capacity

Components shall

a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and

© 2025 ADS-TEC Industrial IT GmbH

b) provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.

CR 2.9 (1) Warn when audit record storage capacity threshold reached (SL3)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The internal Audit Log file is stored in a preallocated storage area. The system uses a ring buffer.	IRF1 IRF3	2.2.0
SL2	No additional requirements	IRF1 IRF3	2.2.0
SL3	Not yet implemented. Planned for a future firmware release (beyond IRF1000/IRF3000 v2.3.0 rev-a). Planned implementation: - Configurable minimum log retention period (days) - Syslog warning when retention cannot be guaranteed - Status LED indication of audit log overflow	IRF1 IRF3	2.3.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

CR 2.10 Response to audit processing failures

Components shall

a) provide the capability to protect against the loss of essential services and functions in the

event of an audit processing failure; and

b) provide the capability to support appropriate actions in response to an audit processing

failure according to commonly accepted industry practices and recommendations.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device continues to provide essential services even in the case of an audit processing failure (e.g., audit log overflow). Audit logs are stored in a ring buffer to ensure that failures in audit processing do not affect the availability of essential functions. Warnings in case of audit processing failures are provided via Syslog and Status LED (see CR 2.9).	IRF1 IRF3	2.2.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

CR 2.11 Timestamps

Components shall provide the capability to create timestamps (including date and time) for use in audit records.

CR 2.11 (1) Time synchronization (SL2)

CR 2.11 (2) Protection of time source integrity (SL4)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device generates timestamps (date and time) for audit records using the system clock (Linux time). Format follows ISO/IEC 8601:2004.	IRF1 IRF3	2.2.0
SL2	In addition, the device supports time synchronization with an external NTP server to ensure system-wide consistent timestamps.	IRF1 IRF3	2.2.0
SL3	Same as SL2. No additional requirements.	IRF1 IRF3	2.2.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	n/a – see Functional Area Web-UI / JSON-RPC API	IRF1 IRF3	n/a

CR 2.12 Non-repudiation

If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.

CR 2.12 (1) Non-repudiation for all users (SL4)

EN 18031-1 mapping: none

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device provides non-repudiation for human users via the audit log. All actions performed via WebUI/API are logged together with the authenticated username. Audit logs cannot be silently modified, as they are stored in a ring buffer and supplemented with internal protection mechanisms according to the threat model.	IRF1 IRF3	2.2.0
SL2	Same as SL1. No additional requirements.	IRF1 IRF3	2.2.0
SL3	Same as SL1. No additional requirements.	IRF1 IRF3	2.2.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a – The VPN provides only encrypted tunnel access and does not log individual user actions inside the tunnel. Non-repudiation is therefore not applicable. The Big-LinX cloud system will record the specific users and their actions.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	n/a – The packet filter enforces static network rules at the IP/port level. It does not provide user authentication or log individual user actions. Non-repudiation is therefore not applicable. However, if the Audit Log is used as option of a packet filter rule, then of course the Audit Log Event record is changeable by any user.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	n/a – The device does not provide a local HMI or console with authenticated user actions. All management requiring non-repudiation occurs via the WebUI/API. Non-repudiation is therefore not applicable at the physical access level.	IRF1 IRF3	n/a

CR 2.13 Use of physical diagnostic and test interfaces

CR 2.13 / NDR 2.13 Use of physical diagnostic and test interfaces

The requirements for the use of physical diagnostic and test interfaces are component-specific

and can be specified as requirements for each specific component type in sections 12 to 15.

are specified.

NDR 2.13 – Use of physical diagnostic and test interfaces (SL2)

NDR 2.13. (1) Active monitoring (SL3)

EN 18031-1 mapping: none

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL2	The Web-UI / JSON-RPC API does not provide any direct development or diagnostic interfaces in the production software version. Indirectly the Web UI or JSON/RPC API can be used to enable a debug SSH server (with valid permissions and after authorization) which can be regarded as test interface. The debug SSH server is only accessible by ADS-TEC IIT software developers and authorization in only possible by RSA keys which are stored and managed at ADS-TEC according to the IEC62443 4-1 process and private key protection. By default this SSH interface is disabled and it can only be enabled by the device owner after authorization with the current username and password, which are not known to ADS-TEC IIT.	IRF1 IRF3	2.2.0
SL3	The enabling of the SSH debug server is logged in the Audit Log in the same way as any other change of the device configuration.	IRF1 IRF3	2.2.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a – The VPN does not provide any diagnostic or test interfaces. Non-applicable for CR 2.13.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	n/a – The packet filter operates at the network layer and does not provide any diagnostic or test interfaces. Non-applicable for CR 2.13.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL2	Internal UARTs are without function in the production software version since the product does exist. The device will fulfill the CR2.13 requirement by preventing unauthorized use of factory diagnostic/test interfaces with version 3.0.0. Before version 3.0.0 the device relies on a physical protection by the devive housing and tamper seal only as all physical test and debug interfaces are not reachable on external interfaces.	IRF1 IRF3	3.0.0
SL3	All diagnostic/test interfaces will be disabled in production devices. Therefore, active monitoring and logging of interface access attempts will not be applicable.	IRF1 IRF3	3.0.0

FR 3 System integrity

Ensure the integrity of the component to protect against unauthorized manipulation or modification.

CR 3.1 Communication integrity

Components shall provide the capability to protect integrity of transmitted information.

CR 3.1 (1) Communication authentication

EN 18031-1 mapping: SCM-1, SCM-2, SCM-4, SSM-1, SSM-2

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The Web-UI and JSON-RPC API enforce HTTPS using TLS 1.2/1.3 to protect data integrity during transmission.	IRF1 IRF3	2.0.0
SL2	TLS server certificate can be used to validate and ensure authenticity of the communication endpoint. Weak or unauthenticated connections are not permitted.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL3	No additional requirements beyond SL2.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	VPN integrity is ensured by OpenVPN (TLS 1.2) and HTTPS-based WWH control channel with mutual X.509 certificate authentication.	IRF1 IRF3	2.0.0
SL2	Big-LiNX validates servers and enrolled clients via precommissioned CA certificates, ensuring authenticity of communication.	IRF1 IRF3	2.0.0
SL3	No additional requirements beyond SL2.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable: The packet filter itself does not provide cryptographic protection for communication integrity. Integrity and authenticity are ensured by higher-level mechanisms such as TLS (Web-UI/JSON-RPC) or VPN tunnels (OpenVPN/IPsec).	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Not applicable: Physical access protection of the device does not implement communication integrity. Integrity and authenticity of transmitted data are provided by cryptographic mechanisms such as TLS and VPN.	IRF1 IRF3	n/a

CR 3.2 Protection from malicious code

CR 3.2 / NDR 3.2 – Protection from malicious code

The protection from malicious code requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

NDR 3.2 – Protection from malicious code

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
n/a	CR 3.2 is not applicable, for justification please refer to CR 3.1	IRF1 IRF3	n/a

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	CR 3.2 is not applicable, for justification please refer to CR 3.1	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	CR 3.2 is not applicable, for justification please refer to CR 3.1	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	CR 3.2 is not applicable, for justification please refer to CR 3.1	IRF1 IRF3	n/a

CR 3.3 Security functionality verification

© 2025 ADS-TEC Industrial IT GmbH

Components shall provide the capability to support verification of the intended operation of security functions according to IEC 62443-3-3 SR3.3.

CR 3.3 (1) Security functionality verification during normal operation

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	no requirement	IRF1 IRF3	2.0.0
SL1	The Security functionality can be verified according to the user manual and the Eventlog / Syslog messages of The Device.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	VPN functionality can be verified by checking standard system logs and VPN connection status in the Web-UI. Failed or blocked VPN sessions are logged, and active sessions can be confirmed.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	During normal operation, VPN operation can be continuously verified through monitoring of logs and VPN status in the management interface.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	The packet filter ruleset can be verified by reviewing the active configuration in the Web-UI and testing connections. Blocked packets generate log entries, which allows the user to confirm that firewall rules are enforced.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	During normal operation, packet filter activity can be verified continuously by monitoring the audit log (dropped/allowed packets) and checking the firewall status in the management interface.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The Security functionality can be verified according to the user manual and the Eventlog / Syslog messages of The Device.	IRF1 IRF3	2.0.0

CR 3.4 Software and information integrity

Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.

CR 3.4 (1) Authenticity of software and information (SL2)

CR 3.4 (2) Automated notification of integrity violations (SL3)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
n/a	Not applicable: Integrity and authenticity verification of software and configuration is handled under Physical Device Protection.	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable: Big-LiNX VPN does not perform integrity or authenticity checks on software or configuration.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable: The packet filter does not perform integrity or authenticity checks on software or configuration.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The device software image is protected with cryptographic checksums and asymmetric keys. This is validated before a new software is flashed. The configuration files contain additional cryptographic integrity protection as well. The main operating system is running as single image read-only partition. There is no other way to modify the configuration or software of the device in accordance with the security context and secure guidelines of the product.	IRF1 IRF3	2.0.0
SL2	There is no protection against modification of data at rest, this will be added with version 3.0.0. It will only be available for new shipments.	IRF1 IRF3	3.0.0
SL3	Starting with version 3.0.0 the system will do cryptographic integrity checks on the device firmware and will signal any failures with a red Status LED.	IRF1 IRF3	3.0.0

CR 3.5 Input validation

Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.

EN 18031-1 mapping: GEC-6

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	All input is validated before usage by the Web-UI and JSON-RPC API interfaces.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	All input is validated before usage by the Big-LiNX VPN interface.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	All input is validated before usage by the packet filter / firewall interface.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	All input is validated before usage by the physical device interfaces.	IRF1 IRF3	2.0.0

CR 3.6 Deterministic output

Components that physically or logically connect to an automation process shall provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.

© 2025 ADS-TEC Industrial IT GmbH

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Not applicable: The device does not directly control automation processes and therefore deterministic output is not relevant for Web-UI or JSON-RPC interfaces.	IRF1 IRF3	n/a
SL1	Not applicable: The device does not directly control automation processes and therefore deterministic output is not relevant for Web-UI or JSON-RPC interfaces.	IRF1 IRF3	n/a

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable: The device does not directly control automation processes and therefore deterministic output is not relevant for Big-LiNX VPN.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable: The device does not directly control automation processes and therefore deterministic output is not relevant for the packet filter / firewall.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Not applicable: The device does not directly control automation processes and therefore deterministic output is not relevant for physical device protection.	IRF1 IRF3	n/a

CR 3.7 Error handling

Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Compliant. Error messages in the Web-UI and JSON-RPC API do not disclose sensitive internal details. For example, on login failure the system only returns a generic error without revealing whether the username or password is valid.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Not applicable. The IRF device only operates as a TCP client for the Big-LinX VPN service. It does not authenticate incoming peers and does not expose error messages to external entities. The only validation performed is certificate chain validation of the Big-LinX server certificate (CA check).	IRF1 IRF3	n/a
SL2	No additional requirements.	IRF1 IRF3	n/a
SL3	No additional requirements.	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	Compliant. By default, the packet filter does not send ICMP reject messages when dropping packets, so no error details are leaked. Administrators may explicitly enable ICMP reject messages if required for debugging, but this is a configurable choice. In the default configuration, no exploitable information is exposed.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	Not applicable. The device does not provide user-facing error messages in the area of physical device protection, therefore CR 3.7 is not relevant here.	IRF1 IRF3	n/a
SL2	No additional requirements.	IRF1 IRF3	n/a
SL3	No additional requirements.	IRF1 IRF3	n/a

CR 3.8 Session integrity

Components shall provide mechanisms to protect the integrity of communications sessions including:

a) the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions);

b) the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and

c) the capability to generate unique session identifiers with commonly accepted sources of randomness.

EN 18031-1 mapping: SCM-1, SCM-2, SCM-4

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	No requirement.	IRF1 IRF3	2.0.0
SL2	Compliant. The Web-UI and JSON-RPC API implement session handling with: logout button and automatic session timeout (configurable from firmware ≥ 2.1.0), unique system-generated random session IDs, and invalidation on logout and reboot.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	No requirement.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
SL2	Compliant. Big-LinX VPN sessions rely on TLS and OpenVPN mechanisms which protect session integrity through multiple means: • Each VPN connection spawns a fresh OpenVPN process with a new TLS session; session IDs are unique and system-random. • OpenVPN's session_id for the control channel is randomly generated and not reused. • Data channel keys are rotated regularly using OpenVPN's built-in renegotiation settings (reneg-bytes, reneg-sec, reneg-pkts), ensuring that symmetric keys are not used beyond acceptable thresholds. • The Big-LinX OpenVPN server enforces session rekeying and expiration policies, ensuring session tokens and keys are refreshed or invalidated after the configured thresholds. • Overall, there is no reuse of keys or sessions across disconnected sessions; every new connection starts fresh.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	No requirement.	IRF1 IRF3	n/a
SL2	Not applicable. The packet filter/firewall does not manage user sessions or session IDs. It operates on packet flows and does not fall under session integrity requirements.	IRF1 IRF3	n/a
SL3	No additional requirements.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	No requirement.	IRF1 IRF3	n/a
SL2	Not applicable. The physical device interfaces do not manage sessions, therefore session integrity is not relevant in this functional area.	IRF1 IRF3	n/a
SL3	No additional requirements.	IRF1 IRF3	n/a

CR 3.9 Protection of audit information

Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.

CR3.9 (1) Audit records on write-once media (SL4)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Audit Log and Eventlog are protected against unauthorized access, modification, and deletion. Logs cannot be modified or deleted apart from being flushed with a factory default reset.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a, for all log access see Web-UI interface.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable, Firewall logs are treated as audit information but access to hose is only possible by Web-UI or JSON/RPC API.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	Pressing the factory defaults button clears all audit logs. To prevent unauthorized deletion, physical access to the reset button must be restricted (e.g., locked enclosure).	IRF1 IRF3	2.0.0

CR 3.10 Support for updates

CR 3.10 / NDR 3.10 – Support for updates

The support for updates requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

NDR 3.10 – Support for updates (SL1)

NDR 3.10 (1) Update authenticity and integrity (SL2)

EN 18031-1 mapping: SUM-1, SUM-2, SUM-3

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Firmware updates can be uploaded and triggered via Web-UI or JSON-RPC API (System → Software Update).	IRF1 IRF3	2.0.0
SL2	Update packages are signed and verified (signature + checksum) before installation, ensuring authenticity and integrity.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Big-LinX VPN provides centralized update management. Devices can receive and install updates remotely.	IRF1 IRF3	2.0.0
SL2	Updates delivered via Big-LinX are digitally signed and verified in the same way as Web-UI uploads (signature + checksum check).	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable. The firewall subsystem is not independently updateable; updates are managed through the device's general update mechanism.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	Updates can be loaded via USB sticks if physical access is available.	IRF1 IRF3	2.0.0

Vertaulich
© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Physical Access Device Protection	Products	Version
SL2	Update packages are signed and verified (signature + checksum). Administrators can disable USB update functionality to prevent unauthorized use.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

CR 3.11 Physical tamper resistance and detection

CR 3.11 / NDR 3.11 – Physical tamper resistance and detection

The physical tamper resistance and detection requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

NDR 3.11 – Physical tamper resistance and detection (SL2)

NDR 3.11.(1) – Notification of a tampering attempt (SL3)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
n/a	Not applicable. Physical tamper resistance and detection are not relevant for Web-UI or JSON-RPC API.	IRF1 IRF3	n/a

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable. Physical tamper resistance and detection are not relevant for Big-LinX VPN.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable. Physical tamper resistance and detection are not relevant for the packet filter or firewall subsystem.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	No requirement.	IRF1 IRF3	2.2.0
SL2	A tamper seal is present on the device housing to detect unauthorized opening. This provides basic tamper evidence at the device level. The seal has been added for all shipments starting from 08/2025.	IRF1 IRF3	2.2.0
SL3	Planned for firmware version 3.1.0: one of the digital inputs can be configured as a tamper detection signal. This allows external housings with tamper switches to trigger an event, so unauthorized cabinet door opening can be detected and logged in the audit log.	IRF1 IRF3	3.1.0

CR 3.12 Provisioning product supplier roots of trust

CR 3.12 / NDR 3.12 – Provisioning product supplier roots of trust

The provisioning product supplier roots of trust requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

NDR 3.12 – Provisioning product supplier roots of trust (SL2)

EN 18031-1 mapping: none

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL2	The device contains RSA keys for verification of vendor software updates. The keys are provisioned during device manufacturing. This key cannot be overwritten or extracted by the user.	IRF1 IRF3	2.0.0
SL2	Improvement: At manufacturing, each device receives a CA certificate bound to its serial number, provisioned into the hardware-based secure element. This certificate is used to generate the device's default HTTPS certificate, providing a trusted mechanism to verify the device's origin even with an untrusted network connection	IRF1 IRF3	3.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	no requirement	IRF1 IRF3	2.0.0
SL2	The devices include the CA certificate chain to validate Big-LinX server certificates. As Big-LinX is an ADS-TEC service, this chain represents a special product supplier root of trust. The Big-LinX Root-CA is hard-coded in the read-only part of the software and cannot be overwritten by users. Updates of the Root-CA are only possible via signed software updates, ensuring authenticity and integrity.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable. Provisioning of product supplier roots of trust is performed at manufacturing and not related to the firewall subsystem.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	no requirements	IRF1 IRF3	2.0.0
SL2	The device contains RSA keys for verification of vendor software updates. The keys are provisioned during device manufacturing. They are stored in a read-only filesystem.	IRF1 IRF3	2.0.0
SL2	Extended function: A new supplier root of trust is provisioned at production into hardware protected key storage. This feature is only available for new shipments and not retrofittable on existing devices.	IRF1 IRF3	3.0.0

CR 3.13 Provisioning asset owner roots of trust

CR 3.13 / NDR 3.13 – Provisioning asset owner roots of trust

The provisioning asset owner roots of trust requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

NDR 3.13 – Provisioning asset owner roots of trust (SL2)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	No requirement.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL2	The asset owner can provision and replace the device's HTTPS server certificate, which acts as the root of trust for the Web-UI. This enables the owner to enforce their own PKI trust anchors, ensuring that the device's web services are authenticated against asset owner–controlled roots of trust. The asset owner can provision the docker registries public CA certificate as well to restrict the usage of mobile code.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable. Provisioning of asset owner roots of trust is only relevant for Docker container execution via Web-UI/API, not for the firewall subsystem.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Not applicable. Provisioning of asset owner roots of trust is only relevant for Docker container execution via Web-UI/API, not for physical device protection.	IRF1 IRF3	n/a

CR 3.14 Integrity of the boot process

CR 3.14 / NDR 3.14 – Integrity of the boot process

The integrity of the boot process requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

Network devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

The requirements for the four SL levels that relate to NDR 3.14 are:

- SL-C(SI, component) 1: NDR 3.14
- SL-C(SI, component) 2: NDR 3.14 (1)
- SL-C(SI, component) 3: NDR 3.14 (1)
- SL-C(SI, component) 4: NDR 3.14 (1)

(1) Authenticity of the boot process Network devices shall use the component's product supplier roots of trust to verity the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
n/a	Not applicable. Integrity of the boot process is verified internally by the device, not via Web-UI or JSON-RPC API.	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable. Integrity of the boot process is verified internally by the device, not related to Big-LinX VPN.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable. Integrity of the boot process is verified internally by the device, not related to the firewall subsystem.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The device is verifying the integrity of the monolithic firmware image and its configuration data at boot time prior usage.	IRF1 IRF3	2.0.0
SL2	Authentication verification of boot process relevant firmware and configuration data prior to the use, and use of product suppliers roots of trust for verification. Will be added to new shipments from firmware ≥ 3.0.0.	IRF1 IRF3	3.0.0

FR 4 Data confidentiality

Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure.

CR 4.1 Information confidentiality

Components shall

a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and

b) support the protection of the confidentiality of information in transit as defined in

IEC 62443 3-3 SR 4.1.

EN 18031-1 mapping: SCM-3, SSM-3

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	All user interactions with the Web-UI require authentication. Web access is only permitted via HTTPS, ensuring confidentiality of information in transit. Passwords are stored as Argon2 hashes, ensuring confidentiality of password information.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Big-LinX VPN data is encrypted by OpenVPN, the Big-LinX WWH control channel is encrypted by TLS 1.2.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	not applicable	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The device has only internal storage chips which cannot be plugged. All user supplied data is stored there, access to this will need a physical opening of the housing which will break the tampering seal.	IRF1 IRF3	2.0.0
SL3	Starting with version 3.0.0 all data will be encrypted using a hardware based cryptographic mechanism.	IRF1 IRF3	3.0.0

CR 4.2 Information persistence

Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.

CR 4.2 (1) Erase of shared memory resources (SL3)

CR 4.2 (2) Erase verification (SL3)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Factory Reset erases all user-supplied data (configurations, Docker containers, customer-settings, VPN certificates/keys).	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Big-LinX VPN configuration and key material are erased with Factory Reset. If Big-LinX smartcards are used, they must be physically removed at decommissioning.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	Firewall/packet filter configuration is erased together with all other configurations during Factory Reset.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The device can as well be fully wiped by pressing the Factory Default button at power-up. The button is located at the back of the device so it can be mechanically secured during mounting. It cannot be disabled or protected by authentication. This guarantees data wipe even if the administrator password is lost.	IRF1 IRF3	2.0.0
SL2	no additional requirement	IRF1 IRF3	2.0.0
SL3	After a Factory Reset, the Status LED blinks to indicate that the device is in commissioning mode. This provides verification that the reset occurred.	IRF1 IRF3	2.2.0

CR 4.3 Use of cryptography

© 2025 ADS-TEC Industrial IT GmbH

If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

EN 18031-1 mapping: CCK-1, CCK-2, CCK-3, CRY-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL2	The integrated web server supports the following cryptographic algorithms: **TLS 1.2 (20 cipher suites accepted):** - RSA, DHE-RSA, ECDHE-RSA key exchanges with AES-128/256 in GCM, CCM, CBC modes - Example: TLS*ECDHE*RSA*WITH*AES*256*GCM*SHA384 (ECDH secp256r1, 256 bits)* *- DH key exchange: 2048 bits* *- Forward secrecy supported* *- Legacy/weak ciphers (RC4) not supported* **TLS 1.3 (3 cipher suites accepted):** - *TLS*CHACHA20*POLY1305*SHA256 (ECDH X25519) - TLS*AES*256*GCM*SHA384 (ECDH X25519) - TLS*AES*128*GCM*SHA256 (ECDH X25519) This configuration ensures interoperability with legacy systems while maintaining compliance with modern cryptographic standards. Cross-reference: CR 1.8 – Public key infrastructure certificates (Web).	IRF14x2 IRF1 IRF3	2.2.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
SL2	The system is using an integrated SSL library which supports the following algorithms in general. Please note that insecure and deprecated cryptographic algorithms are included with full intent as customers must be able to attach old legacy systems in many cases. In case of insecure algorithms, they must be explicitly enabled for such cases depending on the specific interface (e.g., OpenVPN, IPsec). **Symmetric Ciphers:** aes-128-cbc, aes-128-cfb, aes-128-cfb1, aes-128-cfb8, aes-128-ctr, aes-128-ecb, aes-128-ofb, aes-192-cbc, aes-192-cfb, aes-192-cfb1, aes-192-cfb8, aes-192-ctr, aes-192-ecb, aes-192-ofb, aes-256-cbc, aes-256-cfb, aes-256-cfb1, aes-256-cfb8, aes-256-ctr, aes-256-ecb, aes-256-ofb, aes128, aes128-wrap, aes192, aes192-wrap, aes256, aes256-wrap, bf, bf-cbc, bf-cfb, bf-ecb, bf-ofb, blowfish, cast, cast-cbc, cast5-cbc, cast5-cfb, cast5-ecb, cast5-ofb, chacha20, des, des-cbc, des-cfb, des-cfb1, des-cfb8, des-ecb, des-ede, des-ede-cbc, des-ede-cfb, des-ede-ecb, des-ede-ofb, des-ede3, des-ede3-cbc, des-ede3-cfb, des-ede3-cfb1, des-ede3-cfb8, des-ede3-ecb, des-ede3-ofb, des-ofb, des3, des3-wrap, desx, desx-cbc, id-aes128-wrap, id-aes128-wrap-pad, id-aes192-wrap, id-aes192-wrap-pad, id-aes256-wrap, id-aes256-wrap-pad, id-smime-alg-CMS3DESwrap, rc2, rc2-128, rc2-40, rc2-40-cbc, rc2-64, rc2-64-cbc, rc2-cbc, rc2-cfb, rc2-ecb, rc2-ofb, rc4, rc4-40 **Digest (Hash) Algorithms:** md4, md5, rmd160, sha1, sha224, sha256, sha3-224, sha3-256, sha3-384, sha3-512, sha384, sha512, sha512-224, sha512-256, shake128, shake256 **Elliptic Curve Parameters:** secp112r1, secp112r2, secp128r1, secp128r2, secp160k1, secp160r1, secp160r2, secp192k1,	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
SL2	secp224k1, secp224r1, secp256k1, secp384r1, secp521r1, prime192v1, prime192v2, prime192v3, prime239v1, prime239v2, prime239v3, prime256v1, wap-wsg-idm-ecid-wtls6, wap-wsg-idm-ecid-wtls7, wap-wsg-idm-ecid-wtls8, wap-wsg-idm-ecid-wtls9, wap-wsg-idm-ecid-wtls12, brainpoolP160r1, brainpoolP160t1, brainpoolP192r1, brainpoolP192t1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1 Cross-reference: CR 4.3 – Use of cryptography (Big-LinX VPN).		2.0.0
SL2	Big-LinX VPN uses OpenVPN (compiled with OpenSSL) and supports LZO/LZ4 compression and PKCS#11 smartcard integration. - Control channel uses TLS 1.2 with cipher suite `DHE-RSA-AES256-GCM-SHA384` (RSA 2048-bit, ephemeral DH, provides PFS). - Data channel uses AES-256-CBC with HMAC-SHA1 (160-bit). - Session keys: 256-bit AES, negotiated per session. - Certificates validated against ADS-TEC CA chain, including EKU check for TLS Web Server Authentication. - Server identity verified (`verify-x509-name server`). - Authentication caching disabled (`auth-nocache`). Cross-reference: CR 1.8 – Public key infrastructure certificates (Big-LinX VPN).	IRF1 IRF3	2.0.0
SL3	All Big-LinX VPN authentication certificates are issued by a managed PKI infrastructure at ADS-TEC Industrial IT and its associated partner companies. - PKCS#11 smartcards (Java Card) may be used for hardware-backed key storage. - Smartcards securely store the client certificate/private key and perform cryptographic operations outside the device. - This provides hardware protection for authenticators in compliance with IEC 62443 SL3.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL2	Version 3.0.0 will add a hardware based cryptographic protected secure boot mechanism	IRF1 IRF3	3.0.0

FR 5 Restricted data flow

Segment the control system via zones and conduits to limit the unnecessary flow of data.

CR 5.1 Network segmentation

Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Network segmentation is not directly applicable to the Web-UI. Segmentation features are implemented at the networking and firewall level, not via the management interface. But of course these features can and must be configured by using the Web-UI.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	The Big-LinX VPN is implemented as IP-routed virtual subnet. All data can be filtered by the packet filter of the device.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	The main purpose of the device packet filter is to provide network segmentation. This can achieved via routing and firewall configuration by the user.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The ETH1 to ETH4/ETH8 ports are a physically distinct hardware interfaces, separated from the each other and not implemented with VLANs. This design enforces zone separation at the hardware level, serving as a boundary between external and internal network zones.	IRF3	2.0.0
SL1	The LAN1, LAN2 and LAN3 ports are a physically distinct hardware interfaces, separate from the WAN port and not implemented with VLANs. This design enforces zone separation at the hardware level, serving as a boundary between external (WAN) and internal (LAN) network zones.	IRF1	2.0.0
SL1	The WAN port is a physically distinct hardware interface, separate from LAN ports and not implemented with VLANs. This design enforces zone separation at the hardware level, serving as a boundary between external (WAN) and internal (LAN) network zones.	IRF1	2.0.0

CR 5.2 Zone boundary protection

CR 5.2 / NDR 5.2 – Zone boundary protection

The zone boundary protection requirements are network-component-specific and can be located as requirements for network devices in Clause 15.

NDR 5.2. (1) Deny all, permit by exception (SL2)

NDR 5.2. (2) Island mode (SL3)

NDR 5.2. (3) Fail close (SL3)

EN 18031-1 mapping: GEC-2, NMM-1, TCM-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The firewall subsystem ca be configured by the Web-UI to implement zone boundary protection	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	The packet filter provides monitoring and control of communication at zone boundaries, enforcing compartmentalization. This is the main purpose of the firewall subsystem.	IRF1 IRF3	2.0.0
SL2	Yes, the packet filter is deny-all by default. Admin users must reconfigure this during commissioning if they want different behavior.	IRF1 IRF3	2.0.0
SL3	Island mode is provided by digital input switches which can change the behavior of the configured packet filter rules. For example, if the switch is enabled, all traffic is dropped. Fail-close is the standard behavior: if the device's connection tracking table is overflowed, no new connection can be established.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The LAN1, LAN2 and LAN3 ports are assigned to a distinct security zone. Its hardware separation supports enforcement of zone boundaries by the system’s packet filter. The firewall software applies rules at this boundary, but the interface's role as a physical ingress point is inherent in the design.	IRF1	2.0.0
SL1	The ETH1 to ETH4/ETH8 ports are assigned to distinct security zones. The hardware separation supports enforcement of zone boundaries by the system’s packet filter. The firewall software applies rules at this boundary, but the interfaces' role as a physical ingress point is inherent in the design.	IRF3	2.0.0
SL1	The WAN port is assigned to a distinct security zone. Its hardware separation supports enforcement of zone boundaries by the system’s packet filter. The firewall software applies rules at this boundary, but the interface's role as a physical ingress point is inherent in the design.	IRF1	2.0.0

CR 5.3 General-purpose person-to-person communication restrictions

CR 5.3 / NDR 5.3 – General-purpose person-to-person communication restrictions

The general-purpose person-to-person communication restriction requirements are network component-specific and can be located as requirements for network devices in Clause 15.

NDR 5.3 – General purpose, person-to-person communication restrictions

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The Web-UI can be used to implement general purpose comm restrictions based on IP protocol, ports and destination addresses.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Big-LinX VPN traffic can be filtered using the packet filter. See functional area 'Packet Filter' for details.	IRF1 IRF3	n/a

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	The packet filter can block general-purpose communication traffic (e.g., email protocols, social media, messaging systems) by filtering ports, addresses, and protocols. This prevents malware introduction and data leakage.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Not applicable.	IRF1 IRF3	n/a

FR 6 Timely response to events

Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

CR 6.1 Audit log accessibility

Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

CR 6.1 (1) Programmatic access to audit logs (SL3)

EN 18031-1 mapping: NMM-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Audit logs can be viewed read-only via the Web-UI.	IRF1 IRF3	2.2.0
SL3	Programmatic access to audit.log is possible via JSON-RPC API download. This enables integration with external SIEM systems.	IRF1 IRF3	2.2.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Audit log accessibility is not applicable to the Big-LinX VPN related interfaces. Please see the Web-UI interface.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Audit log accessibility is not applicable to the Packet Filter interface. Packet Filter Logs are accessible with the Web-UI interface. Please see the Web-UI interface.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Audit log accessibility is not applicable to the physical device interfaces. Please see the Web-UI interface.	IRF1 IRF3	n/a

CR 6.2 Continuous monitoring

Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

EN 18031-1 mapping: NMM-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	The device can continuously be monitored using The Eventlog and a remote Syslog Server.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Enhancement: The new Audit logs (starting with 2.2.0) can be accessed read-only via Web-UI and polled via JSON-RPC API. Continuous monitoring is supported through external polling. No syslog forwarding is available.	IRF1 IRF3	2.2.0
SL2	The Audit.log will be extended to stream its logs to the devices Eventlog and thus to remote Syslog Server.	IRF1 IRF3	3.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable, see Functional Area Web-UI / JSON RPC	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable, see Functional Area Web-UI / JSON RPC	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Not applicable, see Functional Area Web-UI / JSON RPC	IRF1 IRF3	n/a

FR 7 Resource availability

Ensure the availability of components against the degradation or denial of essential services.

CR 7.1 Denial of service protection

Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event

CR 7.1 (1) Manage communication load from component (SL2)

EN 18031-1 mapping: RLM-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Essential function: Unauthorized users cannot log in even under DoS conditions. Device automatically recovers when overload ends.	IRF1 IRF3	2.2.0
SL2	Packet filter and Web-UI rate rules mitigate DoS attempts (e.g., large unauthenticated HTTP POST floods). Deny-all by default and authentication remain enforced.	IRF1 IRF3	2.2.0
SL3	Same as SL2. Fail-close principle applies; no insecure bypass of authentication.	IRF1 IRF3	2.2.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	not applicable, the Big-LinX VPN and WWH are TCP Clients, the DoS protection is handled on the server side, not by the device	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	Essential function: Firewall rules are always enforced under DoS; no unfiltered traffic is passed. Device recovers automatically after DoS ends.	IRF1 IRF3	2.0.0
SL2	Packet filter enforces deny-all by default. Rate limiting and connection tracking mitigate floods.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL3	Same as SL2. Fail-close principle applies; if conntrack table is full, no new connections are allowed.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	The device cannot protect itself from DoS attacks based on physical access. This is in accordance with the Security Context of thus class of products.	IRF1 IRF3	n/a

CR 7.2 Resource management

Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.

EN 18031-1 mapping: RLM-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Resource availability is ensured by OS design. Authentication remains fully operational even under resource exhaustion. Security enforcement never fails and recovery is automatic.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Resource availability is ensured by OS design. VPN authentication remains fully operational even under resource exhaustion. Unauthorized access is never possible and recovery is automatic.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	Resource availability is ensured by OS design. Firewall rules remain fully operational under resource exhaustion. Unauthorized traffic is never passed and recovery is automatic.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Not applicable.	IRF1 IRF3	n/a

CR 7.3 Control system backup

Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.

© 2025 ADS-TEC Industrial IT GmbH

CR 7.3 (1) Verification of data backup integrity (SL2)

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Configuration backup is possible via Web-UI/JSON-RPC without interrupting operation. Backup can be stored on Smartcard or downloaded. Only externally unmodified backups can be restored. Sensitive data (passwords) are protected by Argon2 hashing is technically possible. Device keys are not included but if customers uploaded keys for VPN or Web Servers, these will be included. Integrity verification ensures backup validity before restore. The file is encrypted with a vendor specific shared key, but the files can be loaded by any similar valid ADS-TEC IIT device.	IRF1 IRF3	2.0.0
SL2	Backup integrity verification is supported. Only unmodified backups can be restored.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Big-LinX VPN configuration is included in the system backup. The Big-LinX client certificate (and its RSA private key) is never included in the backup and is regarded as a device key. See Web-UI	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Firewall configuration is included in the standard system backup, see Web-UI.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The physical device provides the Big-LinX Smartcard slot as backup medium and upload by using a USB stick on system startup. The backup to the Big-LinX Smartcard can be done during standard operation of the device. Backup to USB stick is not currently not supported.	IRF1 IRF3	2.0.0
SL2	Backup integrity verification is enforced when the backup files are loaded from USB Stick or Big-LinX Smartcard. Only unmodified backups can be restored.	IRF1 IRF3	2.0.0

CR 7.4 Control system recovery and reconstitution

Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.

EN 18031-1 mapping: GEC-4, RLM-1

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	After a failure, the device reloads the last saved startup configuration, ensuring recovery to a secure state. If config is missing, factory defaults are applied, which are designed to be secure.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	VPN configurations are restored as part of system recovery. After failure, last saved startup config is loaded. If missing, factory defaults are applied, ensuring secure recovery.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	Firewall rules are restored as part of system recovery. After failure, last saved startup config is loaded. If missing, factory defaults are applied, ensuring secure recovery.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	Physical device ensures secure recovery. Last saved startup configuration is reloaded after failure. If missing, factory defaults are applied, ensuring recovery to a secure baseline.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

CR 7.5 Emergency power

There is no component level requirement associated with IEC 62443 3-3 SR 7.5.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
n/a	Not applicable.	IRF1 IRF3	n/a

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	Not applicable.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	Not applicable.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	Not applicable.	IRF1 IRF3	n/a

CR 7.6 Network and security configuration settings

© 2025 ADS-TEC Industrial IT GmbH

Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings

CR 7.6 (1) Machine-readable reporting of current security settings (SL3)

EN 18031-1 mapping: GEC-2, GEC-3, GEC-4

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Secure configuration is supported. Current network and security settings can be viewed in Web-UI/API.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	Configuration can be exported in JSON (machine-readable) via API.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	See Web-UI. Big-LinX VPN configuration is included in system configuration and can be exported as part of system config.	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	See Web-UI. Firewall configuration is included in system configuration and can be exported as part of system config.	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
n/a	See Web-UI, Not applicable directly to the physcal access interfaces	IRF1 IRF3	n/a

CR 7.7 Least functionality

Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.

EN 18031-1 mapping: GEC-2, GEC-5

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	By default, only HTTPS is enabled. No unnecessary services are active. Administrators must explicitly enable other services.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
SL1	Big-LinX VPN is disabled by default. Administrators must configure VPN tunnels explicitly or insert a Big-LinX Smartcard to enable it.	IRF1 IRF3	2.0.0

SL	Functional Area: Packet Filter / Firewall	Products	Version
SL1	Firewall/packet filter is enabled by default with deny-all baseline. Administrators must explicitly configure the default policy on first use.	IRF1 IRF3	2.2.0

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	The device relies on physical protection by default. USB is enabled by default to allow provisioning with Configuration files or Firmwareupdates. The Factory Default Button is always enabled. Ethernet ports can be disabled but access relies on physical protection if the port is in use.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH

CR 7.8 Control system component inventory

Components shall provide the capability to support a control system component inventory according to IEC 62443-3-3 SR 7.8.

EN 18031-1 mapping: none

SL	Functional Area: Web-UI / JSON-RPC API	Products	Version
SL1	Product serial number, type, and firmware version can be viewed in Web-UI under Information → Product. Web-UI also provides SBOM. API access supports machine-readable retrieval.	IRF1 IRF3	2.0.0
SL2	No additional requirements.	IRF1 IRF3	2.0.0
SL3	No additional requirements.	IRF1 IRF3	2.0.0

SL	Functional Area: Big-LinX VPN	Products	Version
n/a	n/a	IRF1 IRF3	n/a

SL	Functional Area: Packet Filter / Firewall	Products	Version
n/a	n/a	IRF1 IRF3	n/a

SL	Functional Area: Physical Access Device Protection	Products	Version
SL1	Physical device provides unique hardware serial number for inventory purposes. This includes Ethernet MAC address and WWAN IMEI if a mobile network modem is integrated in the product.	IRF1 IRF3	2.0.0

© 2025 ADS-TEC Industrial IT GmbH