

# **SIEMENS**

## **SIMATIC NET**

**Industrial Ethernet Switches**  
**SCALANCE XB-200, XC-200, XP-200, XF-200BA,**  
**XR-300WG, XC-300, XR-300, XC-400, XR-500**

### **Declaration of Conformity to IEC 62443-4-2**

**Product information**

# Legal Information

## Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 <b>Danger</b>
indicates that death or severe personal injury will result if proper precautions are not taken

 <b>WARNING</b>
indicates that death or severe personal injury may result if proper precautions are not taken

 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.

<b>NOTICE</b>
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

## Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

## Proper use of Siemens products

Note the following:

 <b>WARNING</b>
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

## Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

## Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

---

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>8</b>
1.1	Objective .....	8
1.2	Instructions for use .....	8
1.3	IEC 62443-4-1 and IEC 62443-4-2 certification .....	8
<b>2</b>	<b>Standard IEC 62443 .....</b>	<b>9</b>
2.1	IEC 62443 for product manufacturer .....	9
2.1.1	IEC 62443-4-1 .....	9
2.1.2	IEC 62443-4-2 .....	9
2.1.3	What is a Security Level? .....	10
<b>3</b>	<b>Intent of use and Operational Environment.....</b>	<b>11</b>
3.1	Intended use .....	11
3.2	Target environment.....	11
<b>4</b>	<b>Configuration of SCALANCE products to cover the functional range of IEC 62443-4-2 .....</b>	<b>14</b>
4.1	Security Levels (SL) according to IEC 62443-4-2 that could be achieved - Overview .....	15
4.2	FR 1 – Identification and authentication control (IAC) .....	19
4.2.1	CR 1.1 – Human user identification and Authentication .....	19
4.2.2	CR 1.2 – Software process and devices Identification and authentication .....	19
4.2.3	CR 1.3 – Account Management .....	20
4.2.4	CR 1.4 – Identifier Management.....	20
4.2.5	CR 1.5 – Authenticator Management .....	20
4.2.6	NDR 1.6 – Wireless Access Management .....	21
4.2.7	CR 1.7 – Strength of Password-Based-Authentication.....	21
4.2.8	CR 1.8 – Public Key Infrastructure (PKI) Certificates.....	22
4.2.9	CR 1.9 – Strength of Public Key-Based Authentication.....	22
4.2.10	CR 1.10 – Authenticator Feedback .....	22
4.2.11	CR 1.11 – Unsuccessful Login Attempts.....	22
4.2.12	CR 1.12 – System Use Notification.....	23
4.2.13	NDR 1.13 – Access via Untrusted Networks .....	23
4.2.14	CR 1.14 – Strength of symmetric key-based authentication .....	23
4.3	FR 2 – Use Control .....	24
4.3.1	CR 2.1 – Authorization Enforcement .....	24
4.3.2	CR 2.2 – Wireless use control .....	24
4.3.3	CR 2.3 – Use control for portable and mobile devices.....	25
4.3.4	NDR 2.4 – Mobile code.....	25
4.3.5	CR 2.5 – Session lock .....	25
4.3.6	CR 2.6 – Remote session termination .....	25
4.3.7	CR 2.7 – Concurrent session control .....	26
4.3.8	CR 2.8 – Auditable events .....	26
4.3.9	CR 2.9 – Audit storage capacity .....	26
4.3.10	CR 2.10 - Response to audit processing failures .....	27
4.3.11	CR 2.11 – Timestamp.....	27
4.3.12	CR 2.12 – Non-repudiation.....	28
4.3.13	NDR 2.13 – Use of physical diagnostic and test interfaces .....	28
4.4	FR 3 – System Integrity .....	28
4.4.1	CR 3.1 – Communication Integrity.....	28

---

4.4.2	NDR 3.2 – Protection from malicious code.....	29
4.4.3	CR 3.3 – Security functionality verification.....	29
4.4.4	CR 3.4 – Software and information integrity.....	30
4.4.5	CR 3.5 – Input validation.....	30
4.4.6	CR 3.6 – Deterministic output .....	30
4.4.7	CR 3.7 – Error handling .....	30
4.4.8	CR 3.8 – Session integrity.....	30
4.4.9	CR 3.9 – Protection of audit information.....	31
4.4.10	NDR 3.10 – Support for updates.....	31
4.4.11	NDR 3.11 – Physical tamper resistance and detection .....	31
4.4.12	NDR 3.12 – Provisioning product supplier roots of trust .....	31
4.4.13	NDR 3.13 – Provisioning asset owner roots of trust.....	32
4.4.14	NDR 3.14 – Integrity of the boot process .....	32
4.5	FR 4 – Data Confidentiality.....	32
4.5.1	CR 4.1 – Information Confidentiality .....	32
4.5.2	CR 4.2 – Information Persistence.....	33
4.5.3	CR 4.3 – Use of Cryptography.....	33
4.6	FR 5 – Restricted data flow .....	34
4.6.1	CR 5.1 – Network Segmentation .....	34
4.6.2	NDR 5.2 – Zone Boundary Protection.....	34
4.6.3	NDR 5.3 – General Purpose, Person-To-Person Communication Restrictions .....	34
4.6.4	CR 5.4 – Application partitioning .....	34
4.7	FR 6 – Timely response to events .....	35
4.7.1	CR 6.1 – Audit Log Accessibility.....	35
4.7.2	CR 6.2 – Continuous Monitoring .....	35
4.8	FR 7 – Resource availability .....	35
4.8.1	CR 7.1 – Denial of Service Protection .....	35
4.8.2	CR 7.2 – Resource Management.....	36
4.8.3	CR 7.3 – Control System Backup.....	36
4.8.4	CR 7.4 – Control System Recovery and Reconstitution.....	37
4.8.5	CR 7.5 – Emergency power .....	37
4.8.6	CR 7.6 – Network and Security Configuration Settings .....	37
4.8.7	CR 7.7 – Least Functionality .....	38
4.8.8	CR 7.8 – Control System Component Inventory .....	38

---

## Content of this declaration

This declaration of conformity describes the conformity of the product lines

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XP-200
- SCALANCE XF-200BA
- SCALANCE XR-300WG
- SCALANCE XC-300
- SCALANCE XR-300
- SCALANCE XC-400
- SCALANCE XR-500

with the following standard:

- International standard IEC 62443 "Security for industrial automation and control systems", part 4-2: "Technical security requirements for IACS components" (IEC 62443-4-2 | Version 1.0 | February 2019).

## Scope

This document is valid for the products of the SCALANCE XB-200, XC-200, XP-200, XF-200 and XR300WG product lines from firmware V4.1, as well as the SCALANCE XC-300, XR-300, XC-400 and XR-500 product lines from firmware V1.1. In detail this includes the following products:

<u>SCALANCE XC-200</u>	<u>SCALANCE XP-200</u>	<u>SCALANCE XC-300</u>
SCALANCE XC206-2	SCALANCE XP208	SCALANCE XC316-8
SCALANCE XC206-2SFP	SCALANCE XP208PoE EEC	SCALANCE XC324-4
SCALANCE XC206-2SFP G	SCALANCE XP208G PP	SCALANCE XC332
SCALANCE XC206-2G PoE	SCALANCE XP208G	
SCALANCE XC208	SCALANCE XP208G PoE EEC	<u>SCALANCE XR-300</u>
SCALANCE XC208G	SCALANCE XP216	SCALANCE XR326-8
SCALANCE XC208G PoE	SCALANCE XP216PoE EEC	SCALANCE XR322-12
SCALANCE XC216	SCALANCE XP216G	SCALANCE XR302-32
SCALANCE XC216-3G PoE	SCALANCE XP216G PoE EEC	
SCALANCE XC216-4C		<u>SCALANCE XC-400</u>
SCALANCE XC216-4C G	<u>SCALANCE XF-200BA</u>	SCALANCE XC416-8
SCALANCE XC224	SCALANCE XF204-2BA	SCALANCE XC424-4
SCALANCE XC224-4C G	SCALANCE XF204-2BA DNA	SCALANCE XC432

---

<b><u>SCALANCE XB-200</u></b>	<b><u>SCALANCE XR-300WG</u></b>	<b><u>SCALANCE XR-500</u></b>
SCALANCE XB205-3	SCALANCE XR324WG	SCALANCE XR526-8
SCALANCE XB206-2	SCALANCE XR326-2C PoE WG	SCALANCE XR522-12
SCALANCE XB208	SCALANCE XR328-4C WG	SCALANCE XR502-32
SCALANCE XB213-3		SCALANCE XR524-8WG
SCALANCE XB216		

The document considers product properties and interfaces of the named devices that contribute to comply with the requirements of IEC 62443-4-2. System properties that result from specific networking and individual parameterization of the products to form an overall protection concept, are not in scope. For the declaration of conformity of an entire industrial automation system, in accordance with Part 3-3 "System security requirements and security levels" of the international standard IEC 62443, all system-specific conditions and circumstances must be considered.

## **Terminology**

If information applies to all product lines, the term "SCALANCE products" is used. If information relates to a specific product line or device, the product line or device name is used, respectively.

## **Target Group**

This document is primarily aimed at people in the areas of:

- System- and device purchase
- Project planning / implementation
- System integrators
- Network integrators

---

## Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit [www.siemens.com/cybersecurity-industry](http://www.siemens.com/cybersecurity-industry).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under <https://www.siemens.com/cert>.

# 1 Introduction

## 1.1 Objective

- The document will provide transparency across the product's security capabilities to assist in protecting industrial automation systems against cyberthreats in daily operation in accordance with the requirements of the international standard IEC 62443. This includes an overview of product features and interfaces that help to reduce threats to operations and thus support the productivity and availability even in the event of security incidents.
- Given transparency will provide assistance with the IEC 62443 compliant integration of products into an overall security concept, considering system-specific conditions.
- Given transparency will provide assistance with tenders or system designs regarding conformity with the international standard IEC 62443 Part 4-2.

## 1.2 Instructions for use

Based on a risk-based approach, the international standard IEC 62443, "Security for industrial automation and control systems", describes in several parts both a concept and technical requirements with which industrial automation systems can be protected against security threats. In addition to plant operators, service providers and system integrators, the standard also addresses product suppliers.

In order to empower service providers, operators and integrators to set up a secure automation system that complies with Part 3-3, Part 4-2 addresses the product manufactures and describes the necessary product characteristics of a component for this purpose.

As it is not necessary to fulfill all product security requirement to achieve an IEC 62443-3-3 compliant system, it is of particular importance to consider a product's intended use and its corresponding target environment. These definitions are basis for further interpretation, which requirements must be fulfilled by a product and how the product can be securely integrated into an overall system. It is also crucial that, in addition to the technical product features, the development process defined in accordance with Part 4-1 has been applied. These aspects are generally explained in chapter 3.

The fulfillment of the product requirements from Part 4-2 of the standard is presented in detail in chapter 4. The overview is intended as a guide and supplements the product documentation.

For a simplified usage of this document, the same structure and requirement identifiers as in the IEC 62443 standard will be used.

## 1.3 IEC 62443-4-1 and IEC 62443-4-2 certification

The SCALANCE XB-200, XC-200, XP-200, XF-200BA, XR-300WG, XC-300, XR-300, XC-400 and XR-500 product lines are certified by TÜV Süd. The certification process confirmed a maturity level 3 of the secure product development process. The certificates can be downloaded:

- IEC 62443-4-1 certificate:  
<https://www.siemens.com/global/en/general/system-certificates/di-pa.html>
- IEC 62443-4-2 certificate:  
<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity/certification-standards.html>

## 2 Standard IEC 62443

### 2.1 IEC 62443 for product manufacturer

#### 2.1.1 IEC 62443-4-1

This part of the standard includes security-relevant requirements related to the product development process. Among others, it comprises requirements such as capabilities and expertise, security of third-party components, process and quality assurance, secure architecture and design, and issue handling as well as security updates, patches and change management. Secure implementation of technical product capabilities is only possible if these requirements are fulfilled.

IEC 62443-4-1 describes the requirements for the manufacturer's development process, which are clustered into eight practices:

- Security management
- Specification of security requirements
- Secure by design
- Secure implementation
- Security verification and validation testing
- Management of security-related issues
- Security update management
- Security guidelines

Besides these requirements, the standard also defined four so called 'maturity levels' describing how strong the requirements are considered during the product development:

- Maturity level 1: Initial - Processes are unpredictable, poorly controlled and reactive
- Maturity level 2: Managed - Processes are characterized but reactively used
- Maturity level 3: Defined - Processes are characterized and proactively deployed
- Maturity level 4: Improved - Processes are measured, controlled and continuously improved.

Note: In case of a process certification, higher maturity levels can only be achieved with re-certification after existing processes have initially been verified.

#### 2.1.2 IEC 62443-4-2

IEC 62443-4-2 defines security requirements for components used in industrial automation and control systems (IACS). These requirements are called Component Requirements (CR) which are closely related to the System Requirements (SR) defined in IEC 62443-3-3. Both CR and SR are technical requirements grouped in seven Foundational Requirements (FR). Component Requirements (CR) can be supplemented by one or more Requirement Enhancements (RE) demanding further and more strict capabilities of a specific requirement.

Component Requirements (CR) and their associated Requirement Enhancements (RE) are each assigned to one of the four risk-based Security Levels (SL1 to SL4). With this assignment a component's capability to provide a certain level of protection is classified. However, in order to achieve a certain Security Level for an entire IACS according to IEC 62443-3-3, it is possible to combine different components in such a way that the overall system meets the desired security level, even if a single component does not fulfill all Component Requirement and their Enhancements assigned to the desired security level.

For this purpose, the components intended use and intended operation environment must be reflected to verify if required security functionality can be provided or supplemented by other components.

As described, IEC 62443-4-2 defines the technical components of automation systems based on seven Foundational Requirements (FR):

- Identification and Authentication Control (IAC)
- Use Control (UC)
- system integrity (SI)
- Data Confidentiality (DC)
- Restricted Data Flow (RDF)
- Timely Response to Events (TRE)
- Resource Availability (RA)

### 2.1.3      **What is a Security Level?**

While the IEC 62443 series follows a risk-based approach, the defined security levels are intended to provide an indication of the protection to be achieved. The standard defines four graded security levels that shall provide protection against different skill sets, resources and efforts. The Security Levels are defined in part 4-2 chapter 3.3 of IEC 62443 as follows:

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

A Security Level 0 is implicitly defined if there is no demand for any protection and security requirements.

For the sake of transparency and simplicity, this document will neither differentiate the different types of security levels nor will it summarize the requirement fulfillment to an overall security level. Instead, the document will provide information on the fulfillment of the individual requirement and their proper configuration.

## 3 Intent of use and Operational Environment

### 3.1 Intended use

The typical use of the SCALANCE X Industrial Ethernet Switches and Routers is to provide robust and reliable network connectivity in industrial environments, including discrete manufacturing and process industries. SCALANCE X devices fall into the category of

- network devices,

which means that in addition to the basic component requirements (CR) of IEC 62443-4-2, the specific requirements for network devices (NDR) must also be considered.

The typical intended use as industrial Ethernet switches and routers is largely defined by the following product features:

- **Scalability and flexibility** with modular and powerful configurations for various network structures
- **High network availability** through integrated redundancy mechanisms and system redundancy
- **Support for real-time communication** standards such as PROFINET and EtherNet/IP
- **Integration with automation systems** and other digital signaling devices via integrated signaling contacts

The typical intended use described serves solely as a guide for interpreting conformity with IEC 62443-4-2. The relevant product characteristics are described in detail in chapter 4. Other deployment scenarios of the SCALANCE X product lines not shown are expressly reserved and may require a separate and specific conformity assessment for this purpose.

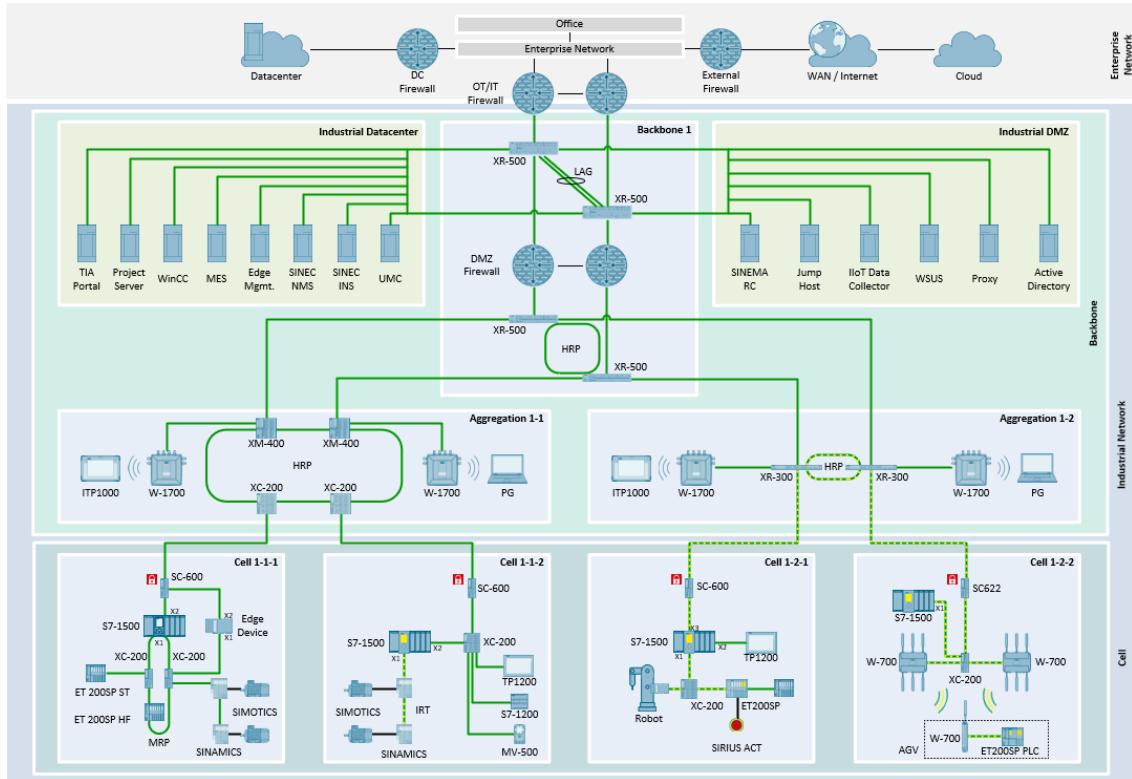
Note:

Further detailed information on product properties and possible applications of the SCALANCE X product lines can be found on the Internet: [www.siemens.com/scalance-x](http://www.siemens.com/scalance-x)

### 3.2 Target environment

The target environment, also called intended operational environment, in which the SCALANCE X product lines are used has a significant influence on the technical product features required by Part 4-2 and is decisive for the assessment of conformity.

In general, SCALANCE X product lines are to be operated as part of an industrial infrastructure and as shown in the following diagram, are primarily designed for the Industrial Backbone, Aggregation and Cell layers.



The following environmental conditions were assumed for the conformity assessment presented in chapter 4:

#### Physical protection of the component in the target environment

- Operation of the component in a controlled, monitored environment or in a closed area, such as a control cabinet.

#### Network zones and interfaces

- Insecure protocols are deactivated in the device configuration. Device access via secure protocol variants, such as HTTPS.

#### Network infrastructure

- A RADIUS server with user management is used for central user authentication. User authentication via RADIUS is configured on the device.
- Password management and the application of password policies are carried out via a central user database.
- Configurable protection against "brute force" attacks is provided.
- The secure syslog client is configured in the device and recorded audit and security events are sent to a syslog server in the network for further processing.
- The time protocols (Simple Network Time Protocol client, NTP client / secure NTP client, SIMATIC time client, NTP Server) are configured to use synchronized time in the network and necessary on devices such as servers, PLCs, or for the analysis of log-messages.

### **Remote access**

- Remote access from insecure network areas is terminated either before or directly on the device.

The target environment described is intended solely as a guide for interpreting conformity with IEC 62443-4-2 and expressly describes only one of many possibilities. Other network architectures not shown, including their specific environmental conditions, may require a separate conformity assessment.

Note:

Further detailed information on the Siemens security concept can be found on the Internet:

[www.siemens.com/industrialsecurity](http://www.siemens.com/industrialsecurity)

<https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf>

## 4 Configuration of SCALANCE products to cover the functional range of IEC 62443-4-2

References to the related sections in the *SCALANCE XB-200, XC-200, XP-200, XF-200 and XR300WG* configuration manuals (WBM / CLI) have been added (CM CLI / CM WBM: <Section>) and are based on the latest available firmware version at the time of publishing (FW V4.5). The scope of this report applies to all firmware versions starting from V4.1 and onwards.

References to the *SCALANCE XC-300, XR-300, XC-400 and XR-500* Configuration Manuals (WBM / CLI) have also been added (CM CLI / CM WBM: <Section>) and are based on the latest available firmware version at the time of publishing (FW V1.2). The scope of this report applies to all firmware versions starting from V1.1 and onwards.

The documents can be downloaded from the Siemens Industry Online Support:

- Configuration Manual for Web-based Management (CM WBM) V4.5:  
<https://support.industry.siemens.com/cs/ww/en/view/109825995>
- Configuration Manual for Command Line Interface (CM CLI) V4.5:  
<https://support.industry.siemens.com/cs/ww/en/view/109825994>
- Configuration Manual for Web-based Management (CM WBM) V1.2:  
<https://support.industry.siemens.com/cs/ww/en/view/109826940>
- Configuration Manual for Command Line Interface (CM CLI) V1.2:  
<https://support.industry.siemens.com/cs/ww/en/view/109826950>

### Operating Instructions

- SCALANCE XB-200: <https://support.industry.siemens.com/cs/ww/en/view/109823193>
- SCALANCE XC-200: <https://support.industry.siemens.com/cs/ww/en/view/109743149>
- SCALANCE XP-200: <https://support.industry.siemens.com/cs/ww/en/view/109741534>
- SCALANCE XF-200BA: <https://support.industry.siemens.com/cs/ww/en/view/109750282>
- SCALANCE XR-300WG: <https://support.industry.siemens.com/cs/ww/en/view/109748979>
- SCALANCE XC-300: <https://support.industry.siemens.com/cs/ww/en/view/109817774>
- SCALANCE XR-300: <https://support.industry.siemens.com/cs/ww/en/view/109972620>
- SCALANCE XC-400: <https://support.industry.siemens.com/cs/ww/en/view/109964151>
- SCALANCE XR-500: <https://support.industry.siemens.com/cs/ww/en/view/109972621>

### Color Coding Legend for Security Levels (SL):

	Requirement is fulfilled
	Requirement is not fulfilled
	Not applicable
	No requirement defined in 62443-4-2

## 4.1 Security Levels (SL) according to IEC 62443-4-2 that could be achieved - Overview

FR = Foundational Requirements, CR = Component Requirements, NDR = Network device

The “Integration” column shows:

C: The requirement is fulfilled by the component itself.

S: The requirement can be fulfilled by integration into a system. For this the component might provide a technical feature or interface. The integration is described in the component’s security guideline.

Number	Description	Integration	Security Level			
			1	2	3	4
<b>Identification and authentication control (IAC)</b>						
CR 1.1	Human user identification and authentication	C	✓	✓	✓	✓
CR 1.1 RE1	Unique Identification and Authentication	S		✓	✓	✓
CR 1.1 RE2	Multifactor Authentication for All Interfaces				-	-
CR 1.2	Software Process and Device Identification and Authentication	C		✓	✓	✓
CR 1.2 RE1	Unique Identification and Authentication	C			✓	✓
CR 1.3	Account Management	S	✓	✓	✓	✓
CR 1.4	Identifier Management	C	✓	✓	✓	✓
CR 1.5	Authenticator Management	C	✓	✓	✓	✓
CR 1.5 RE1	Hardware Security for Authenticators				-	-
NDR 1.6	Wireless Access Management					
NDR 1.6 RE1	Unique Identification and Authentication					
CR 1.7	Strength of Password-Based Authentication	C	✓	✓	✓	✓
CR 1.7 RE1	Password Generation and Lifetime Restrictions for Human Users				-	-
CR 1.7 RE2	Password Lifetime Restrictions for All Users (Human, Software Process or Device)					-
CR 1.8	Public Key Infrastructure (PKI) Certificates	C		✓	✓	✓
CR 1.9	Strength of Public Key-Based Authentication			-	-	-
CR 1.9 RE1	Hardware Security for Public Key-Based Authentication				-	-
CR 1.10	Authenticator Feedback	C	✓	✓	✓	✓
CR 1.11	Unsuccessful Login Attempts	C	✓	✓	✓	✓
CR 1.12	System Use Notification	C	✓	✓	✓	✓
NDR 1.13	Access via Untrusted Networks					
NDR 1.13 RE1	Explicit Access Request Approval					
CR 1.14	Strength of Symmetric Key-Based Authentication	C		✓	✓	✓
CR 1.14 RE1	Hardware Security for Symmetric Key-Based Authentication				-	-

Number	Description	Integration	Security Level			
			1	2	3	4
<b>Use Control (UC)</b>						
CR 2.1	Authorization Enforcement	C	✓	✓	✓	✓
CR 2.1 RE1	Authorization Enforcement for All Users (Humans, Software Processes and Devices)	C		✓	✓	✓
CR 2.1RE2	Permission Mapping to Roles	C		✓	✓	✓
CR 2.1 RE3	Supervisor Override					
CR 2.1 RE4	Dual Approval					
CR 2.2	Wireless Use Control					
CR 2.3	Use control for portable and mobile devices					
NDR 2.4	Mobile Code					
NDR 2.4 RE1	Mobile Code Authenticity Check					
CR 2.5	Session Lock	C	✓	✓	✓	✓
CR 2.6	Remote Session Termination	C		✓	✓	✓
CR 2.7	Concurrent Session Control	C			✓	✓
CR 2.8	Auditable Events	C	✓	✓	✓	✓
CR 2.9	Audit Storage Capacity	C	✓	✓	✓	✓
CR 2.9 RE1	Warn when Audit Record Storage Capacity Threshold Reached	C			✓	✓
CR 2.10	Response to Audit Processing Failures	S	✓	✓	✓	✓
CR 2.11	Timestamps	C	✓	✓	✓	✓
CR 2.11 RE1	Time Synchronization	C		✓	✓	✓
CR 2.11 RE2	Protection of Time Source Integrity	C				✓
CR 2.12	Non-Repudiation	C	✓	✓	✓	✓
CR 2.12 RE1	Non-Repudiation for All Users					-
NDR 2.13	Use of Physical Diagnostic and Test Interfaces	C		✓	✓	✓
NDR 2.13 RE1	Active Monitoring				-	-
<b>System Integrity (SI)</b>						
CR 3.1	Communication Integrity	C	✓	✓	✓	✓
CR 3.1 RE1	Communication Authentication	C		✓	✓	✓
NDR 3.2	Protection from Malicious Code	C	✓	✓	✓	✓
CR 3.3	Security Functionality Verification	C	✓	✓	✓	✓

Number	Description	Integration	Security Level			
			1	2	3	4
CR 3.3 RE1	Security Functionality Verification During Normal Operation	C	-	-	-	✓
CR 3.4	Software and Information Integrity	-	-	-	-	-
CR 3.4 RE1	Authenticity of Software and Information	-	-	-	-	-
CR 3.4 RE2	Automated Notification of Integrity Violations	-	-	-	-	-
CR 3.5	Input Validation	C	✓	✓	✓	✓
CR 3.6	Deterministic Output	-	-	-	-	-
CR 3.7	Error Handling	C	✓	✓	✓	✓
CR 3.8	Session Integrity	C	-	✓	✓	✓
CR 3.9	Protection of Audit Information	C	-	✓	✓	✓
CR 3.9 RE1	Audit Records on Write-Once Media	-	-	-	-	-
NDR 3.10	Support for Updates	C	✓	✓	✓	✓
NDR 3.10 RE1	Update Authenticity and Integrity	C	-	✓	✓	✓
NDR 3.11	Physical Temper Resistance and Detection	-	-	-	-	-
NDR 3.11 RE1	Notification of a Tampering Attempt	-	-	-	-	-
NDR 3.12	Provisioning Product Supplier Roots of Trust	C	-	✓	✓	✓
NDR 3.13	Provisioning Asset Owner Roots of Trust	C	-	✓	✓	✓
NDR 3.14	Integrity of the Boot Process	-	-	-	-	-
NDR 3.14 RE1	Authenticity of the Boot Process	-	-	-	-	-
<b>Data Confidentiality (DC)</b>						
CR 4.1	Information Confidentiality	C	✓	✓	✓	✓
CR 4.2	Information Persistence	C	-	✓	✓	✓
CR 4.2 RE1	Erase of Shared Memory Resources	-	-	-	-	-
CR 4.2 RE2	Erase Verification	-	-	-	-	-
CR 4.3	Use of Cryptography	C	✓	✓	✓	✓
<b>Restricted Data Flow (RDF)</b>						
CR 5.1	Network Segmentation	C	✓	✓	✓	✓
NDR 5.2	Zone Boundary Protection	-	-	-	-	-
NDR 5.2 RE1	Deny All, Permit by Exception	-	-	-	-	-
NDR 5.2 RE2	Island mode	-	-	-	-	-
NDR 5.2 RE3	Fail Close	-	-	-	-	-
NDR 5.3	General Purpose Person-To-Person Communication Restrictions	-	-	-	-	-

Number	Description	Integration	Security Level			
			1	2	3	4
CR 5.4	Application partitioning					
<b>Timely Response to Events (TRF)</b>						
CR 6.1	Audit Log Accessibility	C	✓	✓	✓	✓
CR 6.1 RE1	Programmatic Access to Audit Logs	C			✓	✓
CR 6.2	Continuous Monitoring	S		✓	✓	✓
<b>Resource Availability (RA)</b>						
CR 7.1	Denial of Service Protection	C	✓	✓	✓	✓
CR 7.1 RE1	Manage Communication Load from Component	C		✓	✓	✓
CR 7.2	Resource Management	C	✓	✓	✓	✓
CR 7.3	Control System Backup	C	✓	✓	✓	✓
CR 7.3 RE1	Backup Integrity Verification			-	-	-
CR 7.4	Control System Recovery and Reconstitution	C	✓	✓	✓	✓
CR 7.5	Emergency power					
CR 7.6	Network and Security Configuration Settings	C	✓	✓	✓	✓
CR 7.6 RE1	Machine-Readable Reporting of Current Security Settings	C			✓	✓
CR 7.7	Least Functionality	C	✓	✓	✓	✓
CR 7.8	Control System Component Inventory	C		✓	✓	✓

- ✓ Requirement is fulfilled.
- Requirement is not fulfilled.

## 4.2 FR 1 – Identification and authentication control (IAC)

### 4.2.1 CR 1.1 – Human user identification and Authentication

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 1.1	<p>By default, the product requires authentication via password for every human user interface (SSH, HTTPS or console port) each time a user logs on.</p> <p>All other interfaces are deactivated by default.</p> <p>The password for the user can be configured at:</p> <p><b>Security &gt;&gt; Users &gt;&gt; Passwords</b> (CM WBM: 6.7.3 / CM CLI: 12.1.2)  <b>Security &gt;&gt; Users &gt;&gt; Passwords</b> (CM WBM: 6.7.3 / CM CLI: 12.1.2)</p>
Reaching SL 2 – 4	CR 1.1 RE1	<p>Additionally required:</p> <p>To reach SL 2, the SCALANCE X device must additionally use an external RADIUS server for unique identification and authentication.</p> <p>The integration of an external RADIUS server can be configured at:</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)  <b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.12)  <b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 6.7.4.1 / CM CLI: 12.2.2.1)  <b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 6.7.4.2 / CM CLI: 12.2)  <b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)  <b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.10)  <b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 6.7.4.1 / CM CLI: 12.2.2.1)  <b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 6.7.4.2 / CM CLI: 12.2)</p> <p>Hint: It must be a unique shared secret defined for each RADIUS client</p>
Reaching SL 3 – 4	CR 1.1 RE2	There are no functions implemented in the product that help to achieve the designated security level.

### 4.2.2 CR 1.2 – Software process and devices Identification and authentication

How to configure SCALANCE products devices to cover the functional range of IEC 62443-4-2		
Reaching SL 1	CR 1.2	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 1.2	<p>SCALANCE products must use a customer X.509 certificate for unique identification and authentication.</p> <p>The integration of a customer X.509 certificate be configured at:</p> <p><b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)  <b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)</p>
Reaching SL 3 – 4	CR 1.2 RE1	See CR 1.2

#### 4.2.3 CR 1.3 – Account Management

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 1.3	<p>The SCALANCE product must use an external RADIUS server for unique identification and authentication of the accounts.</p> <p>It is possible to configure up to 4 external RADIUS servers as Backups.</p> <p>The integration of an external RADIUS server can be configured at:</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.12)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 6.7.4.1 / CM CLI: 12.2.2.1)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 6.7.4.2 / CM CLI: 12.2)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.10)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 6.7.4.1 / CM CLI: 12.2.2.1)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 6.7.4.2 / CM CLI: 12.2)</p> <p>Hint: There must be a unique shared secret defined for each RADIUS client</p>

#### 4.2.4 CR 1.4 – Identifier Management

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 1.4	<p>Local identifier management is supported by the SCALANCE product itself. The username is the local identifier and must be unique on the SCALANCE product.</p> <p>The local user can be configured at</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p> <p>It is also possible to delegate the identifier management to an external RADIUS server.</p> <p>The SCALANCE product supports the identification and authentication via X.509 certificates.</p> <p>The integration of a customer X.509 certificate be configured at</p> <p><b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)</p> <p><b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)</p>

#### 4.2.5 CR 1.5 – Authenticator Management

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 1.5	<p>Automatically fulfilled by SCALANCE products:</p> <p>a) default passwords for the default authenticators, unique default self-signed certificates</p>

		<p>b) The default authenticators must be changed at first login.</p> <p>c) Passwords and other authentication methods can be changed at any time.</p> <p>d) Passwords are stored encrypted</p> <p>Alternative: in addition, RADIUS offers the possibility of password aging.</p> <p>The integration of an external RADIUS server can be configured at:</p> <p><b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 6.7.4.1 / CM CLI: 12.2.2.1)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 6.7.4.2 / CM CLI: 12.2)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 6.7.4.1 / CM CLI: 12.2.2.1)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 6.7.4.2 / CM CLI: 12.2)</p>
Reaching SL 3 – 4	CR 1.5 RE1	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.

#### 4.2.6 NDR 1.6 – Wireless Access Management

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 1.6	Not applicable. The SCALANCE products within the scope of this report have no wireless interfaces/functionality.
Reaching SL 2 – 4	NDR 1.6 RE1	See NDR 1.6

#### 4.2.7 CR 1.7 – Strength of Password-Based-Authentication

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 1.7	<p>The SCALANCE products provide the capability to use predefined password policies, which can be configured in the device. It is also possible to create User-defined password policies.</p> <p>The password policy can be configured at:</p> <p><b>Security &gt;&gt; Passwords &gt;&gt; Options</b> (CM WBM: 6.7.3.2 / CM CLI: 12.1.4.1)</p> <p><b>Security &gt;&gt; Passwords &gt;&gt; Options</b> (CM WBM: 6.7.3.2 / CM CLI: 12.1.4.1)</p> <p>It is also possible to realize functionality with an external RADIUS server that possesses the capability to enforce configurable password strength</p> <p>The integration of an external RADIUS server can be configured at:</p> <p><b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 5.7.4.1 / CM CLI: 12.2.2.1)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 5.7.4.2 / CM CLI: 12.2)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; General</b> (CM WBM: 6.7.4.1 / CM CLI: 12.2.2.1)</p> <p><b>Security &gt;&gt; AAA &gt;&gt; RADIUS Client</b> (CM WBM: 6.7.4.2 / CM CLI: 12.2)</p>

Reaching SL 3 – 4	CR 1.7 RE1	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.
Reaching SL 4	CR 1.7 RE2	See CR 1.7 RE1

#### 4.2.8 CR 1.8 – Public Key Infrastructure (PKI) Certificates

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1	CR 1.8	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 1.8	<p>The SCALANCE product supports the identification and authentication via X.509 certificates.</p> <p>The integration of a customer X.509 certificate be configured at:</p> <p><b>System &gt;&gt; Load &amp; Save (CM WBM: 6.4.6 / CM CLI: 4.2.1)</b></p> <p><b>System &gt;&gt; Load &amp; Save (CM WBM: 6.4.6 / CM CLI: 4.2.1)</b></p>

#### 4.2.9 CR 1.9 – Strength of Public Key-Based Authentication

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1	CR 1.9	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 1.9	<p>There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement. For security recommendations, refer to:</p> <p><b>Security Recommendations (CM WBM 3)</b></p> <p><b>Security Recommendations (CM WBM 3)</b></p>
Reaching SL 3 – 4	CR 1.9 RE1	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.

#### 4.2.10 CR 1.10 – Authenticator Feedback

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1 – 4	CR 1.10	The SCALANCE product obscures feedback of authenticator information during the authentication process via WBM, SSH or Telnet.

#### 4.2.11 CR 1.11 – Unsuccessful Login Attempts

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
--	--	--

Reaching SL 1 – 4	CR 1.11	SCALANCE products provide the capability to manage the Brute Force Prevention. Brute Force Prevention (BFP) refers to the protection of the device from unauthorized access by trying a sufficiently large number of passwords. The number of incorrect logins attempts within a specific time period is limited for this purpose.  Brute Force Prevention can be configured and managed by: <b>Security &gt;&gt; Brute Force Prevention</b> (CM WBM: 6.7.6 / CM CLI: 12.6) <b>Security &gt;&gt; Brute Force Prevention</b> (CM WBM: 6.7.8 / CM CLI: 12.8)
-------------------	---------	--

#### 4.2.12 CR 1.12 – System Use Notification

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 1.12	SCALANCE products show a configurable system use notification before authentication via SSH/WBM.  The system use notification can be customized at: <b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1) <b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)

#### 4.2.13 NDR 1.13 – Access via Untrusted Networks

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 1.13	Not applicable. SCALANCE products do not provide the functionality to be used as a firewall product.
Reaching SL 3 – 4	NDR 1.13 RE1	See NDR 1.13

#### 4.2.14 CR 1.14 – Strength of symmetric key-based authentication

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	CR 1.14	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 1.14	Automatically fulfilled by SCALANCE products:  a) Symmetric key authentication is used by e.g. RADIUS, NTP → pre-shared key must be provided by authorized user  b) The key is securely stored encrypted into the configuration data in the filesystem.  c) The users have only access to specific files and file types and therefore the access is restricted.  d) The cryptographic means are compliant with CR 4.3 – Use of cryptography
Reaching SL 3 – 4	CR 1.14 RE1	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.

## 4.3 FR 2 – Use Control

### 4.3.1 CR 2.1 – Authorization Enforcement

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 2.1	<p>The product implemented predefined roles and therefore related user rights and permissions, which can be assigned to users.</p> <p>Users, roles and groups settings can be configured at:</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.12)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.10)</p>
Reaching SL 2 – 4	CR 2.1 RE1	<p>Automatically fulfilled by SCALANCE products:</p> <p>All users must be associated to a role (Predefined roles or other created roles).</p> <p>Users, roles and groups settings can be configured at:</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.12)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Groups</b> (CM WBM: 6.7.2.3 / CM CLI: 12.1.4.10)</p>
Reaching SL 2 – 4	CR 2.1 RE2	<p>Automatically fulfilled by SCALANCE products:</p> <p>Only the role “admin” is authorized to map user to roles.</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Local Users</b> (CM WBM: 6.7.2.1 / CM CLI: 12.1.4.6)</p>
Reaching SL 3 – 4	CR 2.1 RE3	Not applicable. The SCALANCE product doesn't support any functionality which may require supervisor override.
Reaching SL 4	CR 2.1 RE4	See CR2.1 RE3

### 4.3.2 CR 2.2 – Wireless use control

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 2.2	Not applicable. The SCALANCE product has no wireless interfaces/functionality.

### 4.3.3 CR 2.3 – Use control for portable and mobile devices

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 2.3	There is no requirement defined in 62443-4-2 to reach this security level.

### 4.3.4 NDR 2.4 – Mobile code

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 2.4	Not applicable. The SCALANCE product doesn't support mobile code execution.
Reaching SL 2 – 4	NDR 2.4 RE1	See NDR 2.4

### 4.3.5 CR 2.5 – Session lock

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 2.5	<p>The SCALANCE products automatically logout (session termination) after a defined time of inactivity that requires re-authentication afterward.</p> <p>The default session timeouts for SCALANCE products are set to</p> <ul style="list-style-type: none"> <li>○ WBM: 900s</li> <li>○ CLI via SSH: 300s</li> </ul> <p>Individual time intervals can be configured at:</p> <p><a href="#">System &gt;&gt; Auto Logout (CM WBM: 6.4.12 / CM CLI: 4.1.9.3 &amp; 5.2.2.1)</a></p> <p><a href="#">System &gt;&gt; Auto Logout (CM WBM: 6.4.12 / CM CLI: 4.1.9.3 &amp; 5.2.2.1)</a></p>

### 4.3.6 CR 2.6 – Remote session termination

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	CR 2.6	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 2.6	<p>The SCALANCE products automatically logout (session termination) after a defined time of inactivity that requires re-authentication afterward.</p> <p>The default session timeouts for SCALANCE products are set to</p> <ul style="list-style-type: none"> <li>○ WBM: 900s</li> <li>○ CLI via SSH: 300s</li> </ul> <p>Individual time intervals can be configured at:</p> <p><a href="#">System &gt;&gt; Auto Logout (CM WBM: 6.4.12 / CM CLI: 4.1.9.3 &amp; 5.2.2.1)</a></p> <p><a href="#">System &gt;&gt; Auto Logout (CM WBM: 6.4.12 / CM CLI: 4.1.9.3 &amp; 5.2.2.1)</a></p>

### 4.3.7 CR 2.7 – Concurrent session control

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 2	CR 2.7	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 3 – 4	CR 2.7	<p>The number of concurrent sessions on SCALANCE products is limited. The default number of max. concurrent sessions for SCALANCE products is set to:</p> <ul style="list-style-type: none"> <li>○ WBM: 10</li> <li>○ CLI: 8</li> </ul>

### 4.3.8 CR 2.8 – Auditable events

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 2.8	<p>The SCALANCE products automatically generate logs. The entries in the table are limited to 1200 entries and can contain 400 entries for each severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table.</p> <p>Event Log: shows overall system events.</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.6 / CM CLI: 13.1.3.7)</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.5 / CM CLI: 13.1.3.7)</p> <p>Event Log can be configured at:</p> <p><b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)</p> <p><b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)</p> <p>All logs are readable by authenticated users.</p> <p>IEC62443-4-2 Requirement 2.8 a – f: The Event Logs, generated by the SCALANCE product are syslog conform. Syslog format is described in the manual:</p> <p><b>Appendix A</b> (CM WBM: Appendix A "Syslog messages")</p> <p><b>Appendix A</b> (CM WBM: Appendix A "Syslog messages")</p> <p>Remote logging via syslog can be configured at:</p> <p><b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.1.8.15)</p> <p><b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.3.2.1)</p>

### 4.3.9 CR 2.9 – Audit storage capacity

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 2.9	The locally stored log ring-buffer has a capacity of 400 entries per log-severity. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table.

		<b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.6 / CM CLI: 13.1.3.7)  <a href="#"><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.5 / CM CLI: 13.1.3.7)</a>
Reaching SL 3 – 4	CR 2.9 RE1	The SCALANCE products can be configured to output an alarm message when the number of entries in the table reach a user-specified threshold.  <b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)  <a href="#"><b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)</a>

#### 4.3.10 CR 2.10 - Response to audit processing failures

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1 – 4	CR 2.10	<p>Automatically fulfilled by SCALANCE products.</p> <p>The audit and logging event of SCALANCE products are not able to influence the main function of the processes.</p> <ul style="list-style-type: none"> <li>a) The logging and essential function of "switching" are functionally separated.</li> <li>b) SNMP and syslog interface can be used to get information about failures.</li> </ul>

#### 4.3.11 CR 2.11 – Timestamp

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1 – 4	CR 2.11	<p>Automatically fulfilled by SCALANCE products.</p> <p>The SCALANCE product automatically creates time stamps for every log event in the related log tables.</p>
Reaching SL 2 – 4	CR 2.11 RE1	<p>Additionally required:</p> <p>The created time stamps in SCALANCE products are synchronized with the system wide time source that might be synchronized as</p> <ul style="list-style-type: none"> <li>o Simple Network Time Protocol Client</li> <li>o NTP Client / Secure NTP Client</li> <li>o SIMATIC Time Client</li> <li>o NTP Server</li> <li>o PTP (only possible for devices that support PTP)</li> </ul> <p>The Time synchronization can be configured at:</p> <p><b>System &gt;&gt; System Time</b> (CM WBM: 6.4.11 / CM CLI: 6)  <a href="#"><b>System &gt;&gt; System Time</b> (CM WBM: 6.4.11 / CM CLI: 6)</a></p>
Reaching SL 4	CR 2.11 RE2	<p>Additionally required:</p> <p>The SCALANCE product supports secure NTP Client. Therefore, no unauthorized time-synchronization is possible. Additional information about last-sync and last-used sync mechanism are shown in the manual:</p>

		<b>System &gt;&gt; System Time &gt;&gt; NTP Client</b> (CM WBM: 6.4.11.5 / CM CLI: 6.2)  <b>System &gt;&gt; System Time &gt;&gt; NTP Client</b> (CM WBM: 6.4.11.5 / CM CLI: 6.2)
--	--	--

#### 4.3.12 CR 2.12 – Non-repudiation

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1 – 4	CR 2.12	<p>Any configuration changes are logged in the event logs. For security-relevant log messages, the events can be associated to a user.</p> <p>Event Log: Shows overall system events.</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.6 / CM CLI: 13.1.3.7)</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.5 / CM CLI: 13.1.3.7)</p> <p>Event Log can be configured at:</p> <p><b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)</p> <p><b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)</p>
Reaching SL 4	CR 2.12 RE1	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.

#### 4.3.13 NDR 2.13 – Use of physical diagnostic and test interfaces

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1	NDR 2.13	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	NDR 2.13	The device protects against unauthorized use of the physical factory diagnostic and test interface(s). The C-Plug interface is only accessible during boot-up via C-Plug, and only signed firmware can be uploaded, with no read or control access possible.
Reaching SL 3 – 4	NDR 2.13 RE1	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.

### 4.4 FR 3 – System Integrity

#### 4.4.1 CR 3.1 – Communication Integrity

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>
--

Reaching SL 1 – 4	CR 3.1	SCALANCE products allow remote access to its configuration interfaces via encrypted SSH V2.0 (command line interface) or HTTPS (web-based management) via SSL/TLS V1.3. Such protocols include mechanisms to assure integrity and authenticity of transmitted data.  SSL/TLS and SSH can be configured at:  <b>System &gt;&gt; Configuration</b> (CM WBM: 6.4.1 / CM CLI: 8.9.2.5)  <b>System &gt;&gt; Configuration</b> (CM WBM: 6.4.1 / CM CLI: 8.10.2.6)
Reaching SL 2 – 4	CR 3.1 RE1	See CR 1.2

#### 4.4.2 NDR 3.2 – Protection from malicious code

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 3.2	Automatically fulfilled by SCALANCE products. Firmware files are integrity protected by a cryptographic signature and the signature is checked during firmware upload. Other uploaded files have a checksum, and a format check.  Firmware File or other files can be loaded at:  <b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)  <b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)

#### 4.4.3 CR 3.3 – Security functionality verification

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 3.3	On the SCALANCE products it is possible to verify the intended operation of security functions at any time by analyzing the log files for configuration changes, usage of VPN connections.  Event Log: Shows overall system events.  <b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.6 / CM CLI: 13.1.3.7)  <b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.5 / CM CLI: 13.1.3.7)  Event Log can be configured at:  <b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)  <b>System &gt;&gt; Events &gt;&gt; Configuration</b> (CM WBM: 6.4.7.1 / CM CLI: 13.1.8.4)  Remote logging via syslog can be configured at:  <b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.1.8.15)  <b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.3.2.1)
Reaching SL 4	CR 3.3 RE1	The diagnostic information which includes the verification of security functions is accessible through the normal interfaces (WBM, CLI or SNMP). Normal operation is provided independently.

#### 4.4.4 CR 3.4 – Software and information integrity

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 3.4	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.
Reaching SL 2 – 4	CR 3.4 RE1	See CR 3.4
Reaching SL 3 – 4	CR 3.4 RE2	See CR 3.4

#### 4.4.5 CR 3.5 – Input validation

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 3.5	<p>Automatically fulfilled by SCALANCE products.</p> <p>All input values have specified lengths and types for CLI and WBM, with implemented checks. An invalid syntax will not be accepted as input.</p>

#### 4.4.6 CR 3.6 – Deterministic output

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 3.6	Not applicable. The SCALANCE product doesn't have outputs which are used for process operation.

#### 4.4.7 CR 3.7 – Error handling

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 3.7	<p>The SCALANCE products describe the log messages, that do not expose any sensitive information (e.g. at login). The messages presented to the user in the CLI- or web-interface do also not include sensitive information.</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.6 / CM CLI: 13.1.3.7)</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.5 / CM CLI: 13.1.3.7)</p> <p><b>Appendix A</b> (CM WBM: Appendix A "Syslog messages")</p> <p><b>Appendix A</b> (CM WBM: Appendix A "Syslog messages")</p>

#### 4.4.8 CR 3.8 – Session integrity

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	CR 3.8	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 3.8	Session integrity is ensured by session invalidation upon user-logout.

#### 4.4.9 CR 3.9 – Protection of audit information

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	CR 3.9	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 3.9	The audit information stored on the device are automatically protected against unauthorized access, modification and deletion.  No access to logging data is possible for users.
Reaching SL 4	CR 3.9 RE1	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

#### 4.4.10 NDR 3.10 – Support for updates

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 3.10	Firmware updates are a supported function. The functionality of the device is interrupted in this case.
Reaching SL 2 – 4	NDR 3.10 RE1	The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the SCALANCE products. If a new firmware file was downloaded and the device has not yet restarted, the firmware version of the downloaded firmware file is displayed. After the next device restart, the loaded firmware will be activated and used.

#### 4.4.11 NDR 3.11 – Physical tamper resistance and detection

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	NDR 3.11	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	NDR 3.11	The SCALANCE product itself does not offer physical tamper resistance and detection to provide a suitable level of protection. The device shall be operated in a physically protected environment, as described in the intended operational environment.  Security recommendation: Before installing the device, check the condition for any visible damages on the housing. Limit physical access to the device exclusively to trusted personnel.
Reaching SL 3 – 4	NDR 3.11 RE1	See NDR 3.11

#### 4.4.12 NDR 3.12 – Provisioning product supplier roots of trust

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	NDR 3.12	There is no requirement defined in 62443-4-2 to reach this security level.

Reaching SL 2 – 4	NDR 3.12	<p>Automatically fulfilled by SCALANCE products.</p> <p>The root of trust is a unique self-signed default TLS Certificate per device, and this is obfuscated and stored outside of loadable firmware in the HWInfo of the SCALANCE products.</p>
-------------------	----------	--

#### 4.4.13 NDR 3.13 – Provisioning asset owner roots of trust

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	NDR 3.13	<p>There is no requirement defined in 62443-4-2 to reach this security level.</p>
Reaching SL 2 – 4	NDR 3.13	<p>The SCALANCE products provide the capability to install user-certificates. The certificate can be uploaded to the device without any tools. The user-certificates are stored in flash memory inside the component.</p> <p><b>System &gt;&gt; Load &amp; Save (CM WBM: 6.4.6 / CM CLI: 4.2.1)</b></p> <p><b>System &gt;&gt; Load &amp; Save (CM WBM: 6.4.6 / CM CLI: 4.2.1)</b></p>

#### 4.4.14 NDR 3.14 – Integrity of the boot process

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 3.14	<p>There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.</p> <p>Security recommendations:</p> <ul style="list-style-type: none"> <li>- Limit physical access to the device exclusively to trusted personnel.</li> <li>- If possible, operate the devices only within a protected network area</li> </ul>
Reaching SL 2 – 4	NDR 3.14 RE1	See NDR 3.14

### 4.5 FR 4 – Data Confidentiality

#### 4.5.1 CR 4.1 – Information Confidentiality

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 4.1	<p>The SCALANCE products send confidential data encrypted by default when unsecure protocols have not been activated. Passwords for local users are stored encrypted on the device.</p> <p>See operating instructions for the respective SCALANCE device:</p> <p><b>Security recommendations (OI XB-200: 3)</b></p> <p><b>Security recommendations (OI XC-200: 3)</b></p> <p><b>Security recommendations (OI XP-200: 3)</b></p>

		<b>Security recommendations</b> (OI XF-200BA: 3) <b>Security recommendations</b> (OI XR-300WG: 3) <b>Security recommendations</b> (OI XC-300: 3) <b>Security recommendations</b> (OI XR-300: 3) <b>Security recommendations</b> (OI XC-400: 3) <b>Security recommendations</b> (OI XR-500: 3)
--	--	--

#### 4.5.2 CR 4.2 – Information Persistence

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1	CR 4.2	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 4.2	<p>The functionality of the SCALANCE products' reset button resets all confidential data, including the passwords and certificates stored on the device permanently.</p> <p>The reset button can be configured at:</p> <p style="color: blue;"><b>System &gt;&gt; Button</b> (CM WBM: 6.4.13 / CM CLI: 5.3)</p> <p style="color: blue;"><b>System &gt;&gt; Button</b> (CM WBM: 6.4.13 / CM CLI: 5.3)</p>
Reaching SL 3 – 4	CR 4.2 RE1	<p>Not applicable, as the component doesn't expose shared memory resources to unauthorized components.</p> <p>As the operating system is one process, no inter-process communication and shared resources are necessary.</p>
Reaching SL 3 – 4	CR 4.2 RE2	There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.

#### 4.5.3 CR 4.3 – Use of Cryptography

<b>How to configure SCALANCE products to cover the functional range of IEC 62443-4-2</b>		
Reaching SL 1 – 4	CR 4.3	<p>The product uses encryption methods (ciphers) for different network protocols e.g. HTTPS via SSL, SSH, VPN, Syslog, etc. The encryption methods are described at:</p> <p style="color: blue;"><b>Appendix B</b> (CM WBM: Appendix B "Ciphers used")</p> <p style="color: blue;"><b>Appendix B</b> (CM WBM: Appendix B "Ciphers used ")</p>

## 4.6 FR 5 – Restricted data flow

### 4.6.1 CR 5.1 – Network Segmentation

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 5.1	<p>SCALANCE products support Network segmentation by VLAN and Private VLAN. See manual for SCALANCE products:</p> <p><a href="#">Technical basics &gt;&gt; VLAN (CM WBM: 5.4)</a></p> <p><a href="#">Technical basics &gt;&gt; VLAN (CM WBM: 5.4)</a></p> <p>VLAN can be configured at:</p> <p><a href="#">Layer 2 &gt;&gt; VLAN (CM WBM: 6.5.4 / CM CLI: 7.1)</a></p> <p><a href="#">Layer 2 &gt;&gt; VLAN (CM WBM: 6.5.4 / CM CLI: 7.1)</a></p>

### 4.6.2 NDR 5.2 – Zone Boundary Protection

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 5.2	Not applicable. The SCALANCE products within the scope of this report do not provide the functionality to be used as a firewall product.
Reaching SL 2 – 4	NDR 5.2 RE1	See NDR 5.2
Reaching SL 3 – 4	NDR 5.2 RE2	See NDR 5.2
Reaching SL 3 – 4	NDR 5.2 RE3	See NDR 5.2

### 4.6.3 NDR 5.3 – General Purpose, Person-To-Person Communication Restrictions

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	NDR 5.3	Not applicable. SCALANCE products do not provide the functionality to be used as a firewall product.

### 4.6.4 CR 5.4 – Application partitioning

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 5.4	There is no requirement defined in 62443-4-2 to reach this security level.

## 4.7 FR 6 – Timely response to events

### 4.7.1 CR 6.1 – Audit Log Accessibility

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 6.1	<p>The SCALANCE product supports read access to the audit logs "read-only" for the user roles with function rights "1" or "15".</p> <p>User roles can be configured at:</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p><b>Security &gt;&gt; Users &gt;&gt; Roles</b> (CM WBM: 6.7.2.2 / CM CLI: 12.1.4.4)</p> <p>Log files can be analyzed at:</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.6 / CM CLI: 13.1.3.7)</p> <p><b>Information &gt;&gt; Log Table</b> (CM WBM: 6.3.5 / CM CLI: 13.1.3.7)</p>
Reaching SL 3 – 4	CR 6.1 RE1	<p>The device can send the audit records via Syslog to a centralized system.</p> <p>Remote logging via Syslog can be configured at:</p> <p><b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.1.8.15)</p> <p><b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.3.2.1)</p>

### 4.7.2 CR 6.2 – Continuous Monitoring

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	CR 6.2	<p>There is no requirement defined in 62443-4-2 to reach this security level.</p>
Reaching SL 2 – 4	CR 6.2	<p>The SCALANCE product can be continuously monitored e.g. via the defined events that can be exported to an external Syslog-Server.</p> <p>Remote logging via Syslog can be configured at:</p> <p><b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.1.8.15)</p> <p><b>System &gt;&gt; Syslog Client</b> (CM WBM: 6.4.14 / CM CLI: 13.3.2.1)</p> <p>Definition of events are reported can be configured at:</p> <p><b>System &gt;&gt; Events</b> (CM WBM: 6.4.7 / CM CLI: 13.1)</p> <p><b>System &gt;&gt; Events</b> (CM WBM: 6.4.7 / CM CLI: 13.1)</p>

## 4.8 FR 7 – Resource availability

### 4.8.1 CR 7.1 – Denial of Service Protection

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 7.1	Automatically fulfilled by SCALANCE products.

		<p>The essential function is the switching functionality. The robustness is tested during the PROFINET netload test, as well as robustness and vulnerability tests.</p> <p>VLAN can be configured at:</p> <p><b>Layer 2 &gt;&gt; VLAN</b> (CM WBM: 6.5.4 / CM CLI: 7.1)</p> <p><b>Layer 2 &gt;&gt; VLAN</b> (CM WBM: 6.5.4 / CM CLI: 7.1)</p>
Reaching SL 2 – 4	CR 7.1 RE1	<p>The SCALANCE products provide the capability to set network bandwidth limits per port.</p>

#### 4.8.2 CR 7.2 – Resource Management

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 7.2	<p>Automatically fulfilled by SCALANCE products.</p> <p>The SCALANCE products limit the use of resources by security functions to protect against resource exhaustion.</p> <p>The default number of max. concurrent sessions for SCALANCE products is set to:</p> <ul style="list-style-type: none"> <li>○ WBM: 10</li> <li>○ CLI: 8</li> </ul> <p>The configuration limits are described at:</p> <p><b>Description &gt;&gt; Configuration limits</b> (CM WBM: 2.3 / CM CLI: 2.2)</p> <p><b>Description &gt;&gt; Configuration limits</b> (CM WBM: 2.3 / CM CLI: 2.2)</p>

#### 4.8.3 CR 7.3 – Control System Backup

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 7.3	<p>The Configuration (Configuration data, users, certificates) of the device can be done with configPack. This function is independent of other system functionality and does not affect the normal operations.</p> <p>ConfigPack can be downloaded and loaded at:</p> <p><b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)</p> <p><b>System &gt;&gt; Load &amp; Save</b> (CM WBM: 6.4.6 / CM CLI: 4.2.1)</p>
Reaching SL 2 – 4	CR 7.3 RE1	<p>There are no functions implemented for SCALANCE products within this report's scope that help to reach the designated security level for this specific requirement.</p>

#### 4.8.4 CR 7.4 – Control System Recovery and Reconstitution

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 7.4	The SCALANCE products provide the capability to recover to a known secure state after an operational disruption.

#### 4.8.5 CR 7.5 – Emergency power

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 7.5	There is no requirement defined in 62443-4-2 to reach this security level.

#### 4.8.6 CR 7.6 – Network and Security Configuration Settings

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 7.6	<p>Only essential services are enabled on SCALANCE products per default. The manuals include the security documentation and recommendations. The web-based management or CLI provides an overview over the security settings.</p> <p>Security documentation and recommendations can be found at:</p> <p><b>Security Recommendation (CM WBM: 3)</b></p> <p><b>Security Recommendation (CM WBM: 3)</b></p> <p>Security settings can be found at:</p> <p><b>Information &gt;&gt; Security (CM WBM 6.3.19)</b></p> <p><b>Information &gt;&gt; Security (CM WBM 6.3.17)</b></p>
Reaching SL 3 – 4	CR 7.6 RE1	<p>SCALANCE products support SNMPv3 and Syslog. The SNMPv3 values are described in "Scalance_m_msps.mib", which includes all configurable values including security settings. Syslog messages are described in the manual.</p> <p>Scalance_m_msps.mib can be downloaded at:</p> <p><b>System &gt;&gt; Load &amp; Save (CM WBM: 6.4.6 / CM CLI: 4.2.1)</b></p> <p><b>System &gt;&gt; Load &amp; Save (CM WBM: 6.4.6 / CM CLI: 4.2.1)</b></p> <p>SNMP can be configured at:</p> <p><b>System &gt;&gt; SNMP (CM WBM: 6.4.10 / CM CLI: 8.6)</b></p> <p><b>System &gt;&gt; SNMP (CM WBM: 6.4.10 / CM CLI: 8.7)</b></p> <p>Syslog messages are described at:</p> <p><b>Appendix A (CM WBM: Appendix A "Syslog messages")</b></p> <p><b>Appendix A (CM WBM: Appendix A "Syslog messages")</b></p> <p>Remote logging via Syslog can be configured at:</p> <p><b>System &gt;&gt; Syslog Client (CM WBM: 6.4.14 / CM CLI: 13.1.8.15)</b></p> <p><b>System &gt;&gt; Syslog Client (CM WBM: 6.4.14 / CM CLI: 13.3.2.1)</b></p>

#### 4.8.7 CR 7.7 – Least Functionality

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1 – 4	CR 7.7	<p>The SCALANCE products provide the capability to deactivate unnecessary functions, ports and services.</p> <p>Functions, ports and services can be configured at:</p> <ul style="list-style-type: none"> <li>○ <a href="#">System (CM WBM 6.4)</a></li> <li>○ <a href="#">Layer 2 (CM WBM: 6.5)</a></li> <li>○ <a href="#">Layer 3 (CM WBM: 6.6)</a></li> <li>○ <a href="#">Security (CM WBM: 6.7)</a></li> <li>○ <a href="#">System (CM WBM 6.4)</a></li> <li>○ <a href="#">Layer 2 (CM WBM: 6.5)</a></li> <li>○ <a href="#">Layer 3 (CM WBM: 6.6)</a></li> <li>○ <a href="#">Security (CM WBM: 6.7)</a></li> </ul>

#### 4.8.8 CR 7.8 – Control System Component Inventory

How to configure SCALANCE products to cover the functional range of IEC 62443-4-2		
Reaching SL 1	CR 7.8	There is no requirement defined in 62443-4-2 to reach this security level.
Reaching SL 2 – 4	CR 7.8	<p>The inventory functions are provided through web-based configuration or CLI interface. Inventory information is available:</p> <p><a href="#">Information &gt;&gt; Start Page (CM WBM: 6.3.1)</a></p> <p><a href="#">Information &gt;&gt; Versions (CM WBM: 6.3.3 / CM CLI: 4.1.1.30)</a></p> <p><a href="#">Information &gt;&gt; I&amp;M (CM WBM: 6.3.4 / CM CLI 4.1.1.10)</a></p> <p><a href="#">Information &gt;&gt; Start Page (CM WBM: 6.3.1)</a></p> <p><a href="#">Information &gt;&gt; Versions (CM WBM: 6.3.2 / CM CLI: 4.1.1.29)</a></p> <p><a href="#">Information &gt;&gt; I&amp;M (CM WBM: 6.3.3 / CM CLI 4.1.1.10)</a></p> <p>SNMP can be configured at:</p> <p><a href="#">System &gt;&gt; SNMP (CM WBM: 6.4.10 / CM CLI: 8.6)</a></p> <p><a href="#">System &gt;&gt; SNMP (CM WBM: 6.4.10 / CM CLI: 8.7)</a></p>