PLCnext Technology - Security Info Center

Revision 017

February 10th, 2025

Phoenix Contact GmbH & Co. KG

Contents

Welcome to the PLCnext Technology - Security Info Center!

Product range

Industrial Security Guideline

PLCnext Security Guideline

PLCnext Security amd Safety Guideline

PLCnext Control

Appendix

Legal information and imprint

Welcome to the PLCnext Technology - Security Info Center!

In this offline version of the information platform you find all information about security in the context of PLCnext Technology:

- Generic security information
- Information on secure operation including starting up
- Information on IEC 62443-4-1 and IEC 62443-4-2 certification, prerequisites and validity for the different controllers
- For general information on the WBM, refer to the Web-based Management reference in the main PLCnext Technology - Info Center

How to get in touch

Do not hesitate to connect with other PLCnext Technology users around the world and our PLCnext Technology team at Phoenix Contact in Germany. Your questions, hints and feedback are always welcome.

- If you need further information, contact your local subsidiary of Phoenix Contact .
- For feedback to the PLCnext Technology - Security Info Center, please send an email to the author.

Product range

Products

The following devices are certified according to IEC 62443-4-1 and IEC 62443-4-2 Full ML3 Process Profile and therefore subject of this information platform:

Note: If you are using older firmware versions with security certification, you must update to firmware version 2024.0.x LTS.
An update to the current LTS version is also essential, as many security vulnerabilities (CVEs) in Linux components are fixed in every LTS version.

Product	Product Type	Firmware version	Item no.
AXC F 1152	PLCnext Control	2022.0.4 LTS or newer	1151412
AXC F 2152 with AXC F XT ETH 1TX extension module and AXC BS L 2 bus base module	PLCnext Control	2022.0.4 LTS or newer	2404267
	Extension module	-	2403115
	Bus base module	-	1064312
AXC F 3152	PLCnext Control	2022.0.4 LTS or newer	1069208
AXC F XT EXP	Extension module	-	1139999
AXC F XT SPLC 1000 (SPLC 1000)	Safety-oriented control for operating PROFIsafe® devices	01.01.0000 or newer	1159811
RFC 4072S	PLCnext Control for safety-related operation	2023.0 LTS or newer	1051328
BPC 9102S	Industrial box PC with integrated safety-related controller	2023.0.4 LTS	1246285

The procedure for safe commissioning is illustrated using the AXC F 2152 as an example. Information deviating from this can be found in the chapter of the respective controller.

Note: The AXC F XT SPLC 3000 (SPLC 3000, item no. 1160157) is developed in compliance with the IEC 62443-4-1 process and meets the requirements of IEC 62443-4-2, as detailed in the security and safety hardening guidelines.

Officially, the SPLC 3000 will be included in the forthcoming IACS Components PLCnext Control certificate for firmware 2025.0 LTS.

You can find the Functional Safety Certificate here: Functional Safety certificates

Documentation

Each product comes with its own documentation. In addition to the user manuals, there are other documents such as data sheets or change notes that you can download from the respective product page.

Device	Product documentation	Current change notes	Additional documentation
AXC F 1152	Product page	Change notes	"Axioline F: System and installation" user manual , "Axioline F: Diagnostic registers and error messages" user manual , "Industrial Security" user note (see download section on product page)
AXC F 2152	Product page	Change notes	
AXC F 3152	Product page	Change notes	
AXC F XT ETH 1TX	Product page		
AXC F XT SPLC 1000 (SPLC 1000)	Product page	Change notes	
AXC F XT SPLC 3000 (SPLC 3000)	Product page	Change notes	
RFC 4072S	Product page	Change notes	
BPC 9102S	Product page	Change notes	
PLCnext Engineer	Product page	Change notes	Online help

Revision history

We keep adding to and elaborating this information platform. The following changes have been made to this information platform (reverse order - most recent changes at the top):

Rev.	Release date	Changes	Approved by	Approval date
017	2025-02-10	Updated IEC 62443-4-1 ML3 certificate	Boris Waldeck	2025-02-06
016	2024-12-16	Updated IEC 62443-4-1 and IEC 62443-4-2 certificate for devices of the PLCnext Control series.	Boris Waldeck	2024-12-16
015	2024-12-09	Updated hyperlinks	Boris Waldeck	2024-12-09
014	2024-12-04	Publication of the released version – Added information on AXC F XT SPLC 3000 – Changed wording: "PLCnext Technology - Security Info Center" instead of "PLCnext Security Info Center" – Protection against physical access: added information on shipping packaging – Integrity check of downloaded software or firmware files: added example for a PLCnext Technology App from the PLCnext Store – Activating App Manager: added security note on integrity check of the downloaded files – Added new topic: Controller-specific information on the 62443-4-2 compliance list – Added information on OpenSSL 3.0 – AXC F 3152 topic: added information on Trusted Platform Modules (TPM) – Updated PROFINET firewall configurations – Minor corrections and changes in various topics	Boris Waldeck	2024-12-04
013	2024-06-17	Preliminary version for certification – Added information on the service interface of the AXC F 3152 (firewall configuration) – Updated information on backup and restore – Updated product range – Protection against physical access topic: updated image of sd card packaging – Creating users topic: added information on the default password notification – Updated IEC 62443-4-2 compliance list – New topic Device certificates	Boris Waldeck	2024-06-17
012	2024-06-04	Preliminary version for certification – Adjusted information due to hardware changes of the AXC F 3152 with hardware revision 04: – The mode selector switch on this device is omitted. – The service interface (USB-C interface) can be used for service purposes. – Information about security seals. – Additional controller: – AXC F XT SPLC 3000 (SPLC 3000) – Additional information on the security seals of each PLCnext Control – Added information on handling (encrypted) SD cards – Updated information on backup and restore – Added information on OpenSSL – Minor corrections and changes in various topics	Boris Waldeck	2024-06-03

Rev.	Release date	Changes	Approved by	Approval date
011	2023-11-02	– Added instructions on how to perform backup and restore to the navigation and to the overview page. – Changed wording: "certified" (mostly American English) instead of "certificated" (mostly British English).	Boris Waldeck	2023-11-02
010	2023-09-15	– Remodelling the user interface, general restructuring of content and navigation: – Different typeface – Dimmed background – Contents panel and navigation: Clicking on a facet title now opens the first topic of that facet right away. – Several feature enhancements	Boris Waldeck	2023-09-15
009	2023-08-22	Publication of the released version – Additional controller: – BPC 9102S – Several feature enhancements	Boris Waldeck	2023-08-21
008	2023-06-21	Preliminary version for certification – Additional controller: – BPC 9102S	Boris Waldeck	2023-06-21
007	2023-04-17	Additional details to the SafetyEngineer user role in combined safety use cases.	Boris Waldeck	2023-04-17
006	2023-03-20	Additional controller: RFC 4072S	Boris Waldeck	2023-03-20
005	2023-01-13	Publication of the released version for the firmware release 2023.0 LTS of PLCnext Control AXC F 1152 and AXC F 2152	Boris Waldeck	2023-01-13
004	2022-10-24	Preliminary version for certification – Additional controller: – SPLC 1000 – New folder: PLCnext Security and Safety Guideline – Several feature enhancements	Boris Waldeck	2022-10-24
003	2022-05-24	Content added in the folder Industrial Security Guideline including Generic security concepts	Boris Waldeck	2022-05-24
002	2022-04-12	Publication of the released version	Boris Waldeck	2022-04-12
001	2022-04-06	Preliminary version for review	Boris Waldeck	2022-04-06
000	2021-11-16	Preliminary version for certification IEC 62443-4-1 and IEC 62443-4-2	Boris Waldeck	2021-11-16

Industrial Security Guideline

Phoenix Contact industrial security guideline

Introduction

The increasing interconnection of systems, components, and devices as well as the growing amount of data to be transmitted and stored (in a word: the achievements of Industry 4.0) result in a higher risk of cyber attacks. This is also promoted by the increasing spread of open industrial standards. Therefore, the best possible protection against cyber attacks, threats, and abusive or erroneous data misuse/manipulation must be the logical and highly prioritized consequence of this digital development.

Last but not least, in addition to the financial, business and customer interests in smooth and undisturbed operations and data with integrity, there are also legal requirements in terms of security , such as the European NIS Directive (EU 2016/1148) or the German IT Security Act (V2.0 valid from May 28, 2021). Refer to Security-relevant laws and industrial standards for details.

According to current directives and relevant laws, it is primarily the operator of relevant facilities who is required to implement appropriate protective measures. To do this, he needs a consistent security concept that defines uniform and sufficient protective measures. This concept must include the manufacturer of the industrial automation components, the system integrator who integrates these components into the asset (i.e., the plant manufacturer) as well as the plant user/operator.

The IEC 62443 standard defines such a security concept which holistically covers all the roles in the ICS area. In order to securely operate a company or plant, an ISMS (Information Security Management System) needs to be implemented to address the cyber-security risks and implement and improve the technical and organizational counter measures. This is the subject of this manual.

The purpose of such an ISMS is to establish the greatest possible level of cyber-security while taking economic aspects into account. This means that all security-related measures must be defined and implemented at a required and justified level.

"Cyber-security" is generally understood to mean the protection of information and systems against theft and deliberate or accidental manipulation. Cyber-security has the goal to ensure the

- integrity
- availability
- confidentiality

of data and IT systems or OT systems, i.e., Industrial Control Systems (ICS) in our current context.

Our support on your way to security

The present document contains the information that is necessary to integrate and use Phoenix Contact components within your plant in a secure way.

The guideline is aimed at

- system integrators,
- plant owners, and
- plant operators

who integrate, configure, parameterize, and use components supplied by Phoenix Contact.

Note: A basic assumption of the IEC 62443 is that security mechanisms must be implemented by all three roles (as defined by the standard), rather than by a single actor.

The present documentation is not specifically related to any specific device or software version. It is rather to be understood as generic information which has to be supplemented by the related product-specific information given in the respective device manual or software user guide.

Prerequisite level of knowledge

The information given in the present documentation is aimed solely at the group mentioned above who are familiar with the relevant concepts of automation technology as well as the applicable standards and other regulations.

Knowledge of the following is required:

- The devices used to build automation infrastructures and systems,
- The software tools used for device configuration and parameterization as well as
- The security-relevant regulations in the field of application, in particular the applicable parts of the IEC 62443 standard, and
- The safety and accident prevention regulations given by relevant safety standards, applicable sector standards and local safety guidelines in the field of application.

Qualified personnel

The information given in this guide must only be used and applied by qualified personnel: These are appropriately skilled personnel or persons instructed by skilled personnel who are familiar with the relevant IT/ICS security-concepts for automation and network technology as well as the applicable standards (IEC 62443) and other regulations.

Phoenix Contact assumes no liability for erroneous handling or damage resulting from disregard of information contained in this documentation.

⚠ **WARNING**

Improper modifications to devices can endanger safety and the system's cyber security, or damage devices

Within the scope of the information described in the present guideline, any modifications to the hardware and firmware of the devices in the system are not permitted.

About this documentation

Validity of this guideline

The present documentation is not specifically related to any specific device or software version. It is rather to be understood as generic information which has to be supplemented by the related product-specific information given in the respective device manual or software user guide.

Ensure you **always** use the latest documentation. You can verify with Phoenix Contact or refer to the Phoenix Contact homepage on the Internet, to see whether there are any modifications or additions to the documentation you are using: www.phoenixcontact.com

Additional documentation

You must observe the security-related information in the user documentation

- about the devices used to build automation infrastructures and systems (such as controllers, switches, gateways, I/O modules etc.)
- about any configuration or engineering software tool used to develop, commission or maintain your network/automation solution,
- about any additional standard technology (if applicable).

General terms of use for Phoenix Contact Technical Documentation

Phoenix Contact reserves the right to alter, correct and/or improve the technical documentation and the described in the technical documentation at any time and without any prior notice, within the bounds of what is reasonable for the user. This also applies to changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular data sheets, installation instructions, manuals, etc.) does not constitute any further obligation of Phoenix Contact to provide information about alterations to and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact. Please note that the documentation provided is a product-related documentation only. Thus, you are responsible to inspect and verify the suitability and the intended use of the in your particular application case, especially with regard to the compliance with applicable standards and regulations.

Although Phoenix Contact makes every effort to ensure that the information content is accurate, up-do-date and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact does not warrant that the provided information is accurate or complete. However, Phoenix Contact assures the development according to applicable standards. All information in the technical documentation is provided as is and without warranties of any kind, either express or implied.

Phoenix Contact accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, manuals, etc.).
The mentioned limitations and exclusions of liability do not apply if liability is mandatory, e.g. according to the Product Liability Act, in case of intent or gross negligence, in case of injury (of life, body or health) or in case of breach of contract. However, the claim for damages resulting from the breach of essential contractual obligations is restricted to damages that are foreseeable and typical for this contract type, as far as no intent or gross negligence exist or liability is mandatory due to injury of life, body or health. A change of burden of proof to the disadvantage of the user is not associated with this regulation.

Statement of legal authority

This manual, including all illustrations contained herein, is protected by copyright. Use of this manual by any third party is prohibited. Reproduction, translation and public distribution as well as electronic or photographic archiving or alteration requires the express written consent of Phoenix Contact. Violators are liable for damages.

Phoenix Contact reserves all rights in the case of a grant of patent or registration of a petty patent. External are always named without reference to patent rights. The existence of such rights shall thus not be excluded.

Note on usage of provided examples

The illustrations given by Phoenix Contact are mere examples which are intended to explain the general procedure a bit more clearly. We expressly point out that the examples do not represent complete solutions for practical problems or errors but are simply suggestions for an approach you can use as a basis for your specific implementations. Furthermore, we would like to stress that the examples make no claim of being complete, but are simply extracts.

Phoenix Contact has not performed any risk analysis, full-scale validation or respective tests for these examples, neither based on the error pattern nor following any troubleshooting.

Trademarks

Microsoft®, Windows®, Windows® 10, Microsoft.NET Framework are trademarks of Microsoft® Corporation.

All product and company names mentioned in this manual are possibly protected trademarks of the respective manufacturer and should be considered accordingly.

Why cyber security?

There are several definitions for cyber security, like

- Cyber security is the state in which the risks associated with the use of information technology are reduced to a tolerable level. Risks arise from threats and weaknesses to systems and products.
- Information security is the preservation of confidentiality, integrity and availability of information. (ISO 27000:2009)

Ignoring or neglecting cyber security risks in state-of-the-art, highly networked automation systems can at least lead to major disadvantages or even endanger the existence of complete business models and entire companies.

The most commonly experienced risks and damages from cyber-attacks include, for example:

- Plant downtimes: Due to security problems, production has to be stopped for hours or days. Such production downtimes result in considerable costs.
- Loss of know-how: A competitor can access your sensitive data (design, engineering,...). The quantification of the resulting economical damage is complex and expensive.
- Data loss. The reconstruction and recovery of the lost data may be very expensive.
- Damaged reputation: The consequences of a damaged reputation of your company after a cyber attack are often not foreseeable and even more difficult to represent financially. And what happens if data of your customers are affected by the attack?

Therefore, the importance of cyber security has increased massively during the last years in all areas of a company. The risk is further increasing due to two trends: On the one hand, the attack surface is becoming larger with increasing digitization and networking, and on the other hand, attackers and attack methods are becoming more efficient. Accordingly, measures must be taken to protect a company from cyber attacks. Only an integrated cyber security approach is suitable to protect production facilities and critical infrastructures.

The goal of all cyber security measures must be to protect the value creation as this is at the heart of every business.

From this basic principle, individual and specific security goals can be derived for your company. Such specific goals can be, for example, know-how protection (e.g., for development results or contract conditions) or the compliance with legal requirements, for example data privacy. In manufacturing companies, the ability to produce and deliver is of obvious importance.

Note: With regard to security, a distinction must be made between two types of technology or network: IT networks and ICS/OT (Industrial Control Systems/Operational Technology). See topic IT and OT/ ICS: A Comparison for details.

Note: An adequate security concept must include the technology involved, defined processes, and the people involved, i.e., it must specify both technological and organizational measures.
Refer to the topic Security as Holistic System Approach for further information.

Security-relevant laws and industrial standards

It is important to understand that IT security is not only a new "product feature" that a vendor can implement more or less well at its own discretion. Instead, the integration of security features into automation equipment, systems and components is now required by national and international laws.

Therefore, this topic gives a simplified overview on the most essential security-related laws, standards and regulations. In general, a distinction must be made between legal requirements, recommendations and standards that define the necessary steps for the implementation of security-related measures and procedures.

Security laws - what must be done...

IT Security Act (V2.0 valid from May 28, 2021)

Released by the German Parliament which has the central role in the protection of critical infrastructures in Germany.

According to the IT Security Act, plant owners of critical infrastructures **must** establish and certificate an ISMS (Information Security Management System) as well as fulfill a set of minimum technical requirements in order to protect and maintain the provision of its essential services. The act states that the information technology (IT) builds the basis of all security measures in a company.

> **Note:** Note that cyber security for IT and OT (Operational Technology also known as ICS, Industrial Control Systems) requires other measures and procedures. Refer to the topic IT and OT/ICS: A Comparison.

"Critical infrastructures" are facilities, installations, or parts thereof belonging to the sectors of energy, information technology and telecommunications, transport and traffic, health, water, nutrition as well as finance and insurance and are of great importance for the functioning of the community because their failure or impairment would result in considerable supply bottlenecks or threats to public safety. Since version 2, the municipal waste management sector is also considered as critical infrastructure. In addition, "companies in the special public interest" fall within the scope of the Act. These include, for example, defense manufacturers and manufacturers of IT components for use in critical infrastructures or for processing classified government information. This is intended to secure the entire supply chain. Also affected since version 2 are companies that are of significant economic importance to the Federal Republic of Germany. The same applies to their suppliers, which are relevant due to their unique selling propositions.
Therefore, the sectors mentioned must meet industry-specific minimum standards, including in particular the introduction of an ISMS. Moreover, they must report relevant incidents concerning IT security to the BSI. The BSI recommends suitable procedures for identifying and implementing security measures for the company's own information technology (IT). The aim of basic protection is to achieve a medium, appropriate and sufficient level of protection for IT systems. To achieve this goal, the "IT-Grundschutz" catalogues recommend technical security measures and infrastructural, organizational and staff-oriented protection measures.

NIS Directive

Put in place by the EU (with the participation of the European Union Agency for Network and Information Security, ENISA).
The NIS directive is the first piece of EU-wide cyber-security legislation which must be transposed into national law by all member states.

Its goal is to enhance cyber-security across the European Union by improving cyber-security capabilities at national level with better EU-crossing cooperation at the same time.

The NIS directive...

- extends the responsibilities of critical infrastructure operators (which include online service providers/marketplaces, domain registration authorities, search engines, and cloud providers) to include defined security and reporting obligations.
- requires the member states to establish a strategy for addressing cybercrime threats.

It defines and contains, amongst other:

- guideline for incident notification and reporting obligation
- identification criteria
- security requirements

European Cybersecurity Act (3/2019)

Released by the EU (with the participation of the European Union Agency for Network and Information Security, ENISA).

This act is a comprehensive set of regulations, technical requirements, standards and procedures for certification or conformity assessment of products. The act serves the following purposes:

- Strengthening of the ENISA by granting to the agency a permanent mandate, reinforcing its financial and human resources and overall enhancing its role in supporting the EU to achieve a common and high level of cyber security.
- Establishment of the first EU-wide cyber security certification framework to ensure a common cyber security certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g., Internet of Things) and services.
- Perspectively, the IEC 62443 standard will be placed as a certification framework.

Basic Security Standards - How to implement secure processes

Standards describe how precisely measures and procedures can be implemented to meet legal requirements. The basic standards in the context of industrial automation systems are the ISO 2700x series and the IEC 62443.

- IEC 62443: Security for industrial automation: Aimed at plant owners and operators, system integrators and device/component manufacturers/component suppliers. This standard refers in particular to industrial network and system security (OT systems like production and machine networks).
- ISO/IEC 2700X: Information Technology: Aimed at plant owners and plant operators. This standard refers in particular to information and managements system security (IT systems like office and factory backbone networks).

Further Information: For details on IT and ICS (OT) please refer to the topic IT and OT/ICS: A Comparison.

Sector-specific Security Standards

Based on national legislation, various specific security standards have been developed by industry associations especially for the requirements in their respective industries. The table below shows some examples. However, the international standard IEC 62443 is the only one with a cross-industry approach, addressing all participants in the value chain and also enabling certification procedures.

Standard	Target group	Main purpose	Geographical/ industry focus
BDEW White Paper	Device/component manufacturers, system integrators	Security requirements for suppliers	D, A, CH Energy & water sectors
WIB Security Standard	Device/component manufacturers, system integrators	Device/ component manufacturer certification	Oil & gas sector
ISO/IEC 27019	Asset owners, plant operators	IT security for control systems	Energy sector
NIST 800-82	Asset owners, plant operators	Technical security recommendations	USA
NERC CIP	Asset owners, plant operators	Increasing reliability of energy supply infrastructure	USA, Canada
IEC 62443	Device/component manufacturers, system integrators, plant operators	Requirements for secure products, secure solutions, and secure operation	General industry sector

Further information

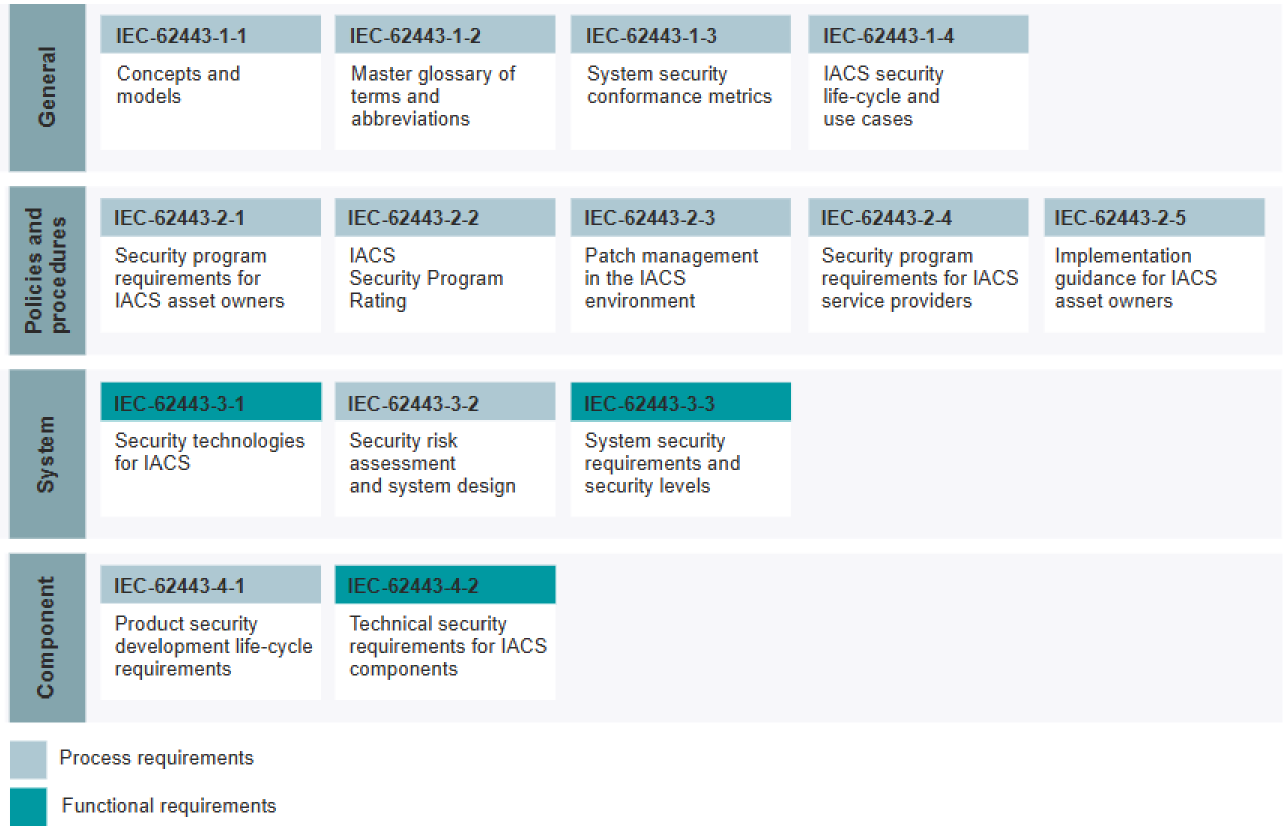
For further information, refer to these sources (some in German):

- IT-Grundschutz Compendium of the BSI
- BSI recommendations for ICS Operators
- Best practices of the US CISA (Cybersecurity & Infrastructure Security Agency)

IEC 62443 standard: security for industrial applications

Overview on the parts of the standard

The IEC 62443 standard series defines the necessary security processes and functional measures for device/component manufacturers, system integrators, and operators of machines and plants. It is a common security standard for industrial automation systems and consists of 13 parts which describe the security-relevant requirements for processes and functional measures as well as the technical state of the art. The following table summarizes the available standard parts:



General	IEC-62443-1-1 Concepts and models	IEC-62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics	IEC-62443-1-4 IACS security life-cycle and use cases	
Policies and procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS Security Program Rating	IEC-62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Security program requirements for IACS service providers	IEC-62443-2-5 Implementation guidance for IACS asset owners
System	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		
Component	IEC-62443-4-1 Product security development life-cycle requirements	IEC-62443-4-2 Technical security requirements for IACS components			

▨ Process requirements

■ Functional requirements

Roles definition in the IEC 62443 standard

The IEC 62443 standard defines three different roles. Depending on your role, different security-related requirements arise in order to fulfill the requirements of the IEC 62443 standard.

- Role 1: Manufacturer or Product Supplier. With regard to the devices used to build automation infrastructures and systems, for example, PLCnext Control devices, mGuard security appliance, switches etc., this is Phoenix Contact.
- Role 2: System Integrator
  As a system integrator, you are responsible for the standard-compliant integration and commissioning of components and systems involved into an automation solution.
- Role 3: Operator or Application/System Owner
  As an application owner/operator, you are responsible for implementing and following the standard-compliant policies, capabilities, and procedures that secure the operation and maintenance of the automation solution on-site.

> **Note:** A basic assumption of the IEC 62443 is that security mechanisms and processes must be implemented by all three roles (as defined by the standard), rather than by a single actor.

> **Note:** Phoenix Contact acts in all three roles: as a component supplier (product business unit), system integrator (VMMs) and as an operator (production). Refer to ICS Security Concept by Phoenix Contact for further information.

Target groups (roles) for the various standard parts

Part 1-1 describes the basic concepts, such as network segmentation, zones and conduits and provides an overview on suitable measures (process/functional/mix). Therefore, part 1 is intended for all target groups.

IEC 62443 parts 2-1 to 5 apply to plant owners with the exception of part 2-4 which addresses system integrators.

The parts 3-1 to 3 apply to system integrators and the parts 4-1 and 4-2 to device/component manufacturers.

Only the parts 3-1, 3-3 and 4-2 (marked with a dark green header in the figure above) describe actual "features". All other parts contain procedural definitions, descriptions, and technical reports on the current "state-of-the-art".

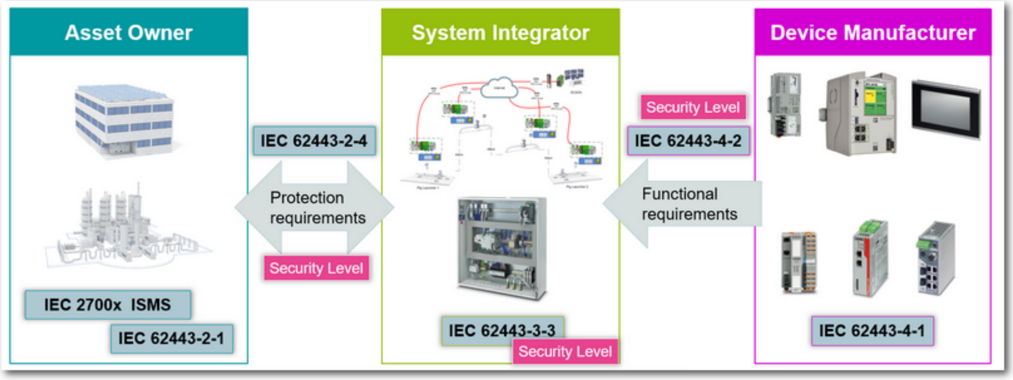
For device and solution providers, the following parts of the standard are relevant: part 4-1, 4-2, 3-3 und 2-4.

Example of roles and applying standard parts

In the context of planning and implementing new production plants or machinery, every party involved is now able to...

- act according to applicable legislation and have their individual parts and business contributions certified according to one and the same worldwide accepted standard
- specify protection requirements and implementation details to service providers and project partners and evaluate the results

All measures and procedures have to be performed in accordance with the individual roles and responsibilities in the current IT security context.



ISO/IEC 27001 standard: security for traditional IT systems

ISO/IEC 27001 is the leading international and most important standard regarding cyber-security of Information Technology (IT) systems. It describes the implementation of an Information Security Management System (ISMS) by providing clear guidelines for planning, implementing, monitoring, and improving your information security. These requirements are generally applicable and apply not only to private and public companies but also to non-profit institutions.

Starting point of an ISMS is basically the (risk) analysis of the situation in your organization. Based on the classified processes and data, the security risks identified for them, and the defined requirements and objectives, a customized security concept is to be implemented. The protection of your sensitive data and its simultaneous availability for authorized users and processes must be taken into account in equal measure.

ISO/IEC 27001 looks at your organization as a whole by including all hierarchical levels, departments and processes into the safety-related consideration.

An ISMS which complies to the ISO/IEC 27001 is not static but rather continuously adapted to changing conditions. It follows a Plan-Do-Check-Act (PDCA) cycle which results in a continuous optimization of the protection measures.

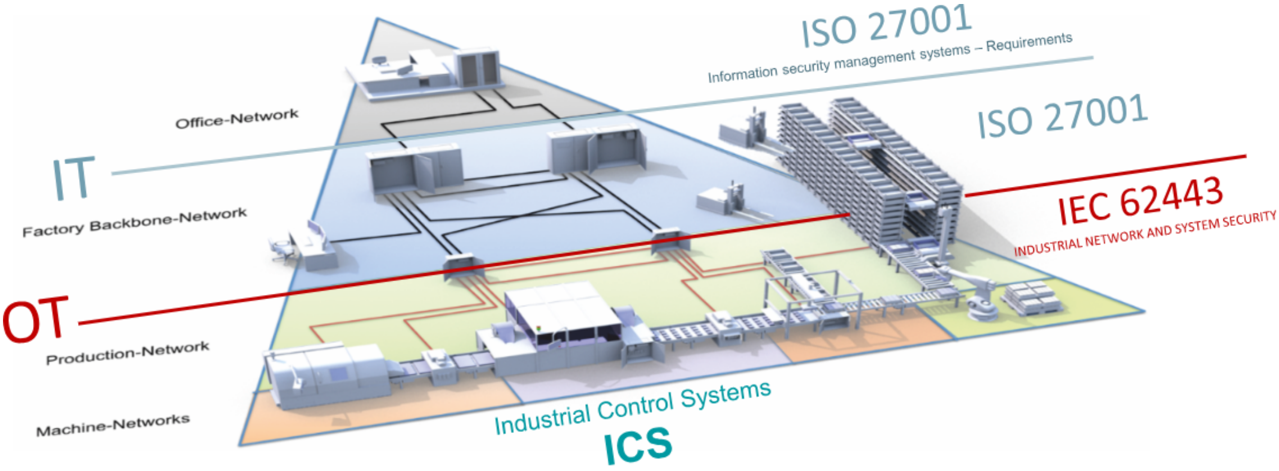
IT and OT/ICS: a comparison

Note: The abbreviation ICS stands for Industrial Control System.

With regard to security, a distinction must be made between different types of technology or networks:

- IT Information Technology Office (accounting, sales, management, ...).
  Here, the ISO 27001 standard for the plant owner is typically applied.
- "Intermediate Layer" Factory Backbone (inventory management etc.).
  Enterprise Resource Planning (ERP) or Product Lifecycle Management (PLM) domain, no classic automation.
  Here, the ISO 27001 standard is typically applied.
- OT Operational Technology Production area / Factory Floor with its machines and plants (ICS).
  Here, the IEC 62443 standard is typically applied.

The following figure illustrates the so-called "Automation Pyramid" with these network types:


ISO 27001
Information security management systems – Requirements
Office-Network
IT
ISO 27001
Factory Backbone-Network
IEC 62443
INDUSTRIAL NETWORK AND SYSTEM SECURITY
OT
Production-Network
Machine-Networks
Industrial Control Systems
ICS

In terms of security, these technology areas must not be considered separated from each other. Rather, they must be considered in conjunction. In order to completely serve security in OT, the measures defined by IT must be extended by additional relevant activities.

In the field of automation, the focus is on physical processes such as drilling, measuring, assembling, etc. Plants are operated as long as they allow economical production. The life cycle is much longer than in an IT environment. The broader challenges in automation are apparent: Any disruption leads to reduced productivity. In addition, the possibilities for eliminating vulnerabilities are limited, since restarts are only feasible to a limited extent and every change to an automation system entails the risk of further malfunctions.

Comparison: IT and OT

When comparing the areas of IT and the industrial automation world (OT/ICS), requirements apply as shown in the table below.

	ICS Security	**IT Security** [1]
Priorities	Availability Integrity Confidentiality	Confidentiality & Availability Integrity
Property: Availability	100 % required	99% sufficient [1]
Property: Restart	Difficult	Possible
Property: Patch Management	Significant challenge	Automated possible
Hardware life cycle	7 to 20 years	3 to 5 years

[1] *With regard to IT security, you may need to distinguish the requirements for the IT backbone and work places. Experience shows that 99 percent availability of the ERP system can result in the factory being inoperable 3.5 days per year.*

From this consideration it becomes evident: Besides an effective access control (user authentication, access restriction by user roles, etc.) to prevent unauthorized access to OT (ICS) systems, the availability of data (and thus the application) has a higher priority in industrial OT environments compared to office IT systems.

Any loss or corruption of data, caused by a malicious/intentional or negligent/unintentional act **must not** affect the functionality and availability of an automation application.

Conclusion: Even though the selection and implementation of security measures in IT and ICS environments differ, **all** elements are required for value creation. A holistic approach is necessary. This is because it is irrelevant in the economic outcome whether production comes to a standstill because of a cyber security incident in the manufacturing process or because of the failure of a central service (such as the ERP system).

360° security - the holistic approach

Comprehensive and sufficient security is not achieved by implementing only (one) technical measures in the system. An adequate security concept must include the technology used, defined processes, and the people involved, i.e., it must specify both technological and organizational measures.

Security must be understood as a mandatory system requirement. Any security-related measures must be integrated with general management structures and organizational processes. Furthermore, they must already be taken into account during the planning phase of processes, plants, and execution controls.

Many but not all threats can be defended against with appropriate technical measures, such as, for example, firewalls which filter the communication connections and only allow permitted and known connections. It is, however, important that **additional measures** are implemented that address personnel, procedures, policies and practices.

A basic assumption of the IEC 62443 is that security mechanisms and processes must be implemented by all three roles (as defined by the standard), rather than by a single actor.

Guiding principles

The following important guiding principles apply when developing an Information Security Management System (ISMS):

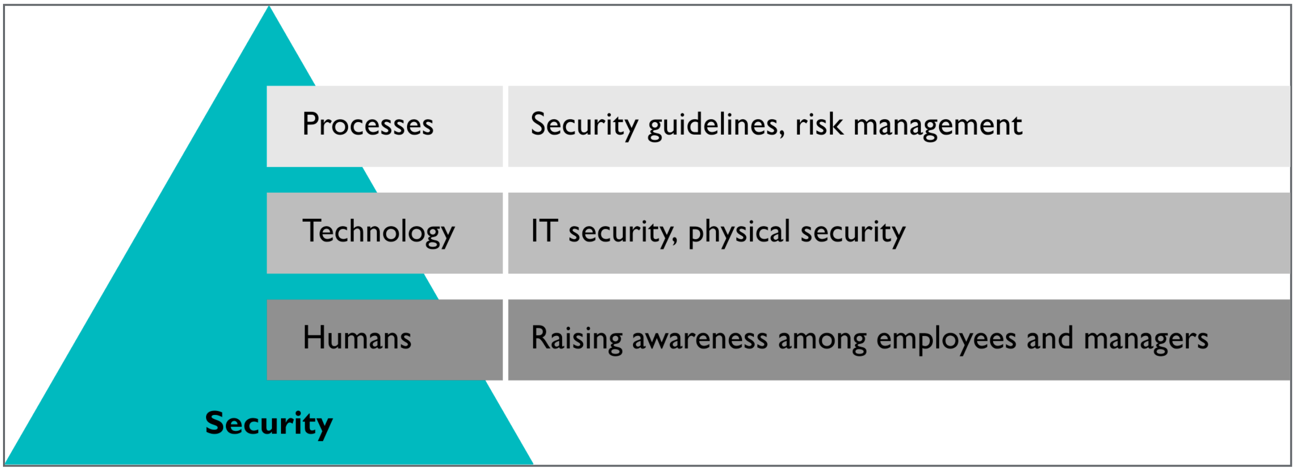
- Security arises from the systemic interaction of the components
- Security can only be economical if measures are taken in the right place. The principle of "equal shares for all" is just as ineffective as "a lot goes a long way".
- To implement technical security measures, the security-related capabilities of the devices used to build automation infrastructures and systems must be utilized as far as possible. To this end, knowledge of these functionalities is necessary as well as the application-specific correct parameterization and configuration.

Further information
For details on technical measures, please read Implementation by technical and organizational means.

Dimensions for a holistic protection

Security can only result, if all of the following three dimensions are considered in a sufficient way. Organizational and technical measures must be defined, implemented and applied/followed.

The figure below illustrates the dimensions of the holistic security measures and the following table explains details.


Processes
Security guidelines, risk management
Technology
IT security, physical security
Humans
Raising awareness among employees and managers
Security

Dimension	Offsite consideration (not ICS-specific)	Onsite consideration (specific ICS in operation)
Process	– How were the system components (devices used to build automation infrastructures and systems) involved developed? – Which security-related capabilities does the system integrator have? (Policies, procedures, competence of personnel, etc., regarding design, implementation, commissioning, maintenance.) – Which policies and procedures does the system integrator follow during the plant design? – Do the plant operation processes fulfill the security requirements regarding policies, procedures etc.?	Do the policies and procedures consider and include the necessary security-related aspect regarding the – design – operation – maintenance of the plant?
Technology	– Which security-related features are provided by the components used? – What is implemented in the plant?	– Which protection functions (functional security capabilities) are implemented in the plant? (Based on the requirements of the IEC 62443-3-3.)
People	– How does the system integrator personnel follow the security-related policies and procedures? – How is the life cycle of each component realized by the product supplier? Consider all aspects from specification to development, test, patch management, technical support, etc. – How are the operating personnel instructed, trained and guided with regard to secure plant operation?	– How strictly does the plant designers follow the security-related policies and procedures? – How strictly does the plant operators and maintainers follow the security-related policies and procedures?

Protection of safety-related data

The protection of safety-related data and therefore the integrity of the safety function is of particular importance.

The manipulation of the safety-related application program may result in:

- triggering the safety function without a request having occurred in the application
- the unavailability of the safety function so that it is no longer triggered when requested
- the unavailability of the safety function with a simultaneous deliberate causing of the request case

Concepts & tools based on IEC 62443

Concepts & tools based on IEC 62443

The following topics describe concepts and tools defined in the IEC 62443 standard:

- Least privilege concept
- Defense-in-Depth concept
- Zones and conduits (with protection needs analysis)
- Data classification & protection needs
- Security levels (SLs)
- Foundational requirements (FR) and system requirements (SR)

Further Information: Practical measures to follow these concepts are described in Implementation by technical and organizational means.

Least privilege concept

The concept of "least privilege" is a basic security concept: **Every** access and execution right to components and data in your ICS should be restricted to the maximum possible extend for **each** user. In doing so, care must be taken to ensure that the availability of the plant is limited as little as possible. This fundamental measure is so important because restricted access significantly increases the effort required for malicious data manipulation and reduces the risk of accidental manipulation.

Further Information: Refer to (Central) User Management for details.

Defense-in-Depth concept

Purpose of the Defense-in-Depth concept

A suitable approach to counter manifold cyber threats is a Defense-in-Depth strategy, for example in accordance with the IEC 62443 standard. This means that a holistic approach must include a combination of technological and organizational measures.

Furthermore, a defense system must not only rely on a single measure. Instead, staggered countermeasures should be implemented, each of which represents one layer of protection. All measures should complement and reinforce each other. If an attacker succeeded in leveraging one (i.e., the outermost) measure, he would be stopped by the subsequent protection mechanism.

Example: In case of an external cyber attack via the network, one or more firewalls must first be overcome before the attacker can reach the target component. There, he must defeat a user logon, only to be stopped by internal security mechanisms. If one protective mechanism in a Defense-in-Depth system fails, the security model does **not** immediately collapse and exposes the target to the attacker.

Consequently, the Defense-in-Depth concept is realized through the interaction of the various security mechanisms. It is therefore also important to consider all security mechanisms in the system.

The IEC 62443 standard defines all aspects of a Defense-in-Depth strategy and addresses all stakeholders involved.

Note: Each stakeholder must contribute to a suitable Defense-in-Depth strategy by

- implementing suitable protection measures for his role/area, and
- avoiding to create potential vulnerabilities when further developing his business (part).

Note: The weakest link in the defensive chain must determine the strength of the entire strategy.

Outer defense layer: organizational measures...

...to be implemented by the **plant owner** (acc. to IEC 62443-2-1). To this end, security policies and procedures are to be defined by the plant owner.

Topics of these policies are among others:

- General security-related behavior
- Awareness and training of personnel
- Definition/review of responsibilities of plant users
- Definition/review of (user) roles
- Definition/review user access rights
- Regulations of physical access
- Implementation of an incident response plan. Such a plan contains the instructions to be carried out after an attack in order to continue the business.
- Definition of a patch management system (IEC 62443-2-3) for rolling out security patches.

Further defense layers: protection measures...

...to be implemented by design in the plant/ICS by the **system integrator** (acc. to IEC 62443-2-4, 3-2 and 3-3).

Examples for such defense measures are:

- Network segmentation into zones and conduits
- Protection of networks by firewalls
- Access control by means of authentication
- Restriction of user actions to necessary operations only
- Secured communication using certificates
- Data protection by encryption
- Suitable procedures and policies regarding commissioning, maintenance and operation. This includes, for example,
  - User management,
  - Security patch management,
  - Anti-malware system,
  - Password policies (acc. to part IEC 62443-2-4).

Inner defense layers: functional security capabilities...

...of the components and systems used: **security by design**, implemented by **product suppliers** (addressed by the IEC 62443-3-3 and 4-2 as well as 62443-4-1 which describes the quality of the development process and includes the security by design).

Examples for such defense features of components and devices are:

- Use of signed software/firmware
- Anti-malware features, such as scanners
- Whitelisting features
- Authentication and authorization mechanisms for human users and software processes on all communication channels including wireless channels. Refer to the topic User Management for details.
- Hardware protection measures for private vendor keys stored on a device, e.g., Trusted Platform Modules (TPM) which provide enhanced security functions thus ensuring the integrity of a hardware/operating system
- Implementation of a encrypted storages for certificates, keys and identities of system integrators and operators
- VPN (Virtual Private Network) communication interfaces
- Device management interface for updating firmware components (Plant Management)
- Logging mechanisms with a synchronized time base
- Secured communication protocols, e.g., TLS communication (Transport Layer Security), also available for wireless links.
- Support of the built-in interface with Security Profiles
- Use and configuration of the integrated firewalls

Zones and conduits (with protection needs analysis)

What is a zone?

A complete plant is difficult to grasp or categorize in terms of possible threats and necessary security measures. For this reason, the IEC 62443 standard divides a complete system into so-called zones. In terms of the standard, a zone can be a **physical and/or logical group** of system components to which the same security requirements apply.

Zones are useful to consider critical components separately and thus to isolate them from the overall system. This way, a segmentation of the network takes place, whereby individual zones can be shielded from the "outside world", e.g. by firewalls. In addition to this shielding, it is recommended to additionally harden individual components and subsystems.

What is the demilitarized zone (DMZ)?

The so-called demilitarized zone (DMZ) plays a central role. It acts like a "buffer zone" between the public network (Internet) and the internal ICS network thus decoupling them. Any communication between the external and internal networks must pass the DMZ which strictly controls the information flow: When accessing the DMZ from outside the ICS, communication connections are only possible to explicitly permitted components such as authentication servers, application gateways or webservers. By restricting external access to these appropriately configured components in the DMZ, other ICS-internal components remain invisible from outside. Thus the ICS network is protected from attacks from public networks.
This information flow control is usually realized by one or several DMZ firewalls.

What is a conduit?

Zones communicate with each other or/and with external networks. The IEC 62443 standard designates the technical means of communication and/or controlling the communication flow between zones as conduits. Consequently, a conduit is a logical grouping of cyber assets dedicated exclusively to communications between two or more zones, and which share the same cybersecurity requirements.

A conduit may consist of a single service (e.g., an Ethernet network) or multiple data carriers. Thus conduits control the access to a zone and they must secure the integrity of the network traffic thus providing protection to the zone.

Conduits must control the information flow and they should separate the ICS from public networks

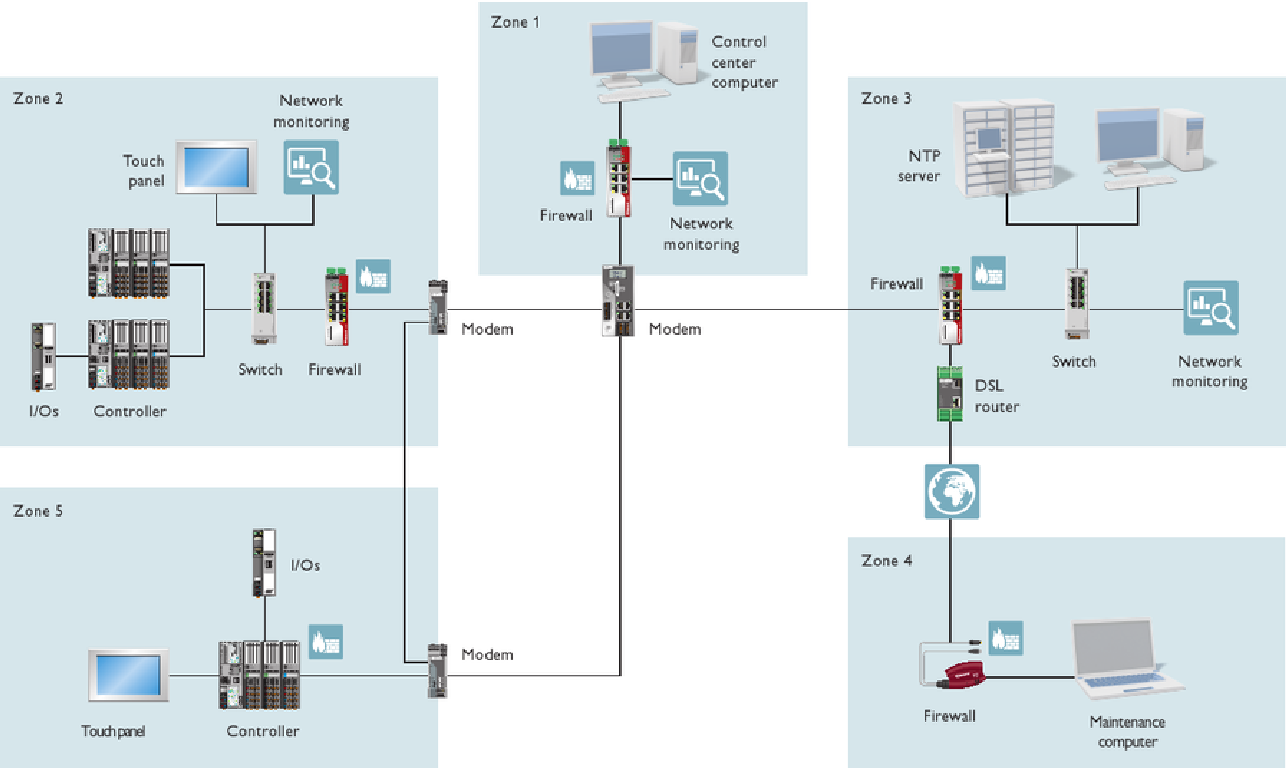
According to the standard, a conduit may cross a zone as long as the cyber security of the channels running in the conduit cannot be compromised by the zone.

Security level (SL) of zones and conduits

For each zone/conduit, a security level (SL) has to be determined depending on its protection needs. By means of their SL, zones and conduits can be compared to each other with respect to their security capability. The SL can be considered as the zone's/conduit's qualitative degree of security.

To each zone/conduit, a target SL (SL-T) should be assigned. This is the SL, the zone/conduit must achieve according to your risk assessment. After having implemented the required security measures, the resulting SL-A of the zone/conduit can be determined. SL-A is the level, this zone/conduit actually **achieves** with the taken measures.

A detailed description of the following example is contained in the section Threat-Risk-Assessment.



The division into zones and conduits supports the Defense-in-Depth concept according to the IEC 62443 standard.

Note: In the context of this manual, network segmentation takes into account the definition of zones according to IEC 62443. However, here we form only zones that correspond to physically connected components (technically considered a cell). Logical component groups are not formed here. Please refer to the chapter Network Segmentation for further information.

Threat-risk-assessment for zones and conduits

Each security-related consideration has to start with a threat-risk-assessment. Actually, a first threat and risk analysis is needed to initially determine the layout of the zones and conduits.
As part of such an analysis, you must identify zones and conduits that require protection, classify the data stored/ processed in and transmitted between these zones, identify potential threats, and determine vulnerabilities. Based on these values, you determine the protection needs and finally develop a protection concept.

In the following, you will find an exemplary description of how to proceed with the threat-risk-assessment. The example shown above of a division into zones and conduits is used as a concrete basis for this procedure.

Further Information: This example is based on a certified Blueprint by Phoenix Contact (Blueprint "Remote Monitoring & Control"). Refer to the respective Blueprint Integration Manual for detailed information.

Note: Proceed for your plant in the same way as described for this example.

1. **Segmentation: available zones**

   In the example figure shown above, a plant has been divided into 5 zones:

   - Zone 1: Control center (SCADA).
   - Zone 2: **Main process zone**, which we will look at as an example in this context. See description below this list.
   - Zone 3: Management zone.
   - Zone 4: Sub-process zone.
   - Zone 5: Remote maintenance zone.

     We will look at zone 2 as an example in this context. Its function is to collect and process data from the process and the sub-process. It consists of a network monitoring (no. 1 in the figure), PLCnext Technology controllers each with I/O devices connected to the field bus (2), a WebPanel for controlling and visualization purposes (3), and an Ethernet switch (4). A firewall (5) handles the communication with the other zones (conduits).

2. **Data identification**

   Based on this zone definition, the data worthy of protection must be identified which are
   1. stored/processed within each zone, and
   2. transmitted between zones via the identified conduits.

   Further Information: Refer to the topic Data Classification & Protection Needs for an overview on data classes.

   In the example, the following data is relevant in zone 2:

   - Configuration data (CD) stored on the devices used to build automation infrastructures and systems.
   - Log data onboard (LO) stored on the devices involved.
   - Application data (AD) on the devices involved.
   - Process data (PD) which are transferred between and processed by the devices.
   - System data (SD) such as access credentials, keys and certificates stored on the devices.

3. **Data classification: protection need analysis**

   Based on the identified data classes, the protection needs can be determined. This classification is made under three aspects:

   - A = Availability
   - I = Integrity
   - C = Confidentiality

   Further Information: Refer to the topic Data Classification & Protection Needs for an overview on protection classes.

In our example zone 2, the following protection needs have been identified (excerpt from all classes):

Data class	Objective: Protection need	Justification
Application Data (AD)	Availability: 3	System cannot start or stop. Shared Libs are on the SD card and can no longer be loaded.
	Integrity: 3	The loss of integrity can result in high damage.
	Confidentiality: 2	Know-how protection. Necessary but not mandatory.
Process Data (PD)	Availability: 3	Process data are mandatory for the plant.
	Integrity: 3	Corrupted process data may cause high damage.
	Confidentiality: 1	Not interpretable by uninvolved parties or interpretable only with high effort. 90% of applications do not require confidentiality of process data. Performance is more important.
System Data (SD), in particular private keys and user credentials	Availability: 2	Failure/expiration of system data only leads to failure of e.g., remote access capabilities while the process continues to run.
	Integrity: 3	Intentional or unintentional falsification of system data can cause medium damage (failure of a component or system part).
	Confidentiality: 4	Highly sensible data.

4. **Zone classification**

   Based on the data classification, the protection needs of each zone can be determined. The **maximum principle applies**, i.e. the highest protection need of a data class must apply to the entire zone (in each case for A/I/C). In our example, the following values have been determined for **zone 2** (main process):

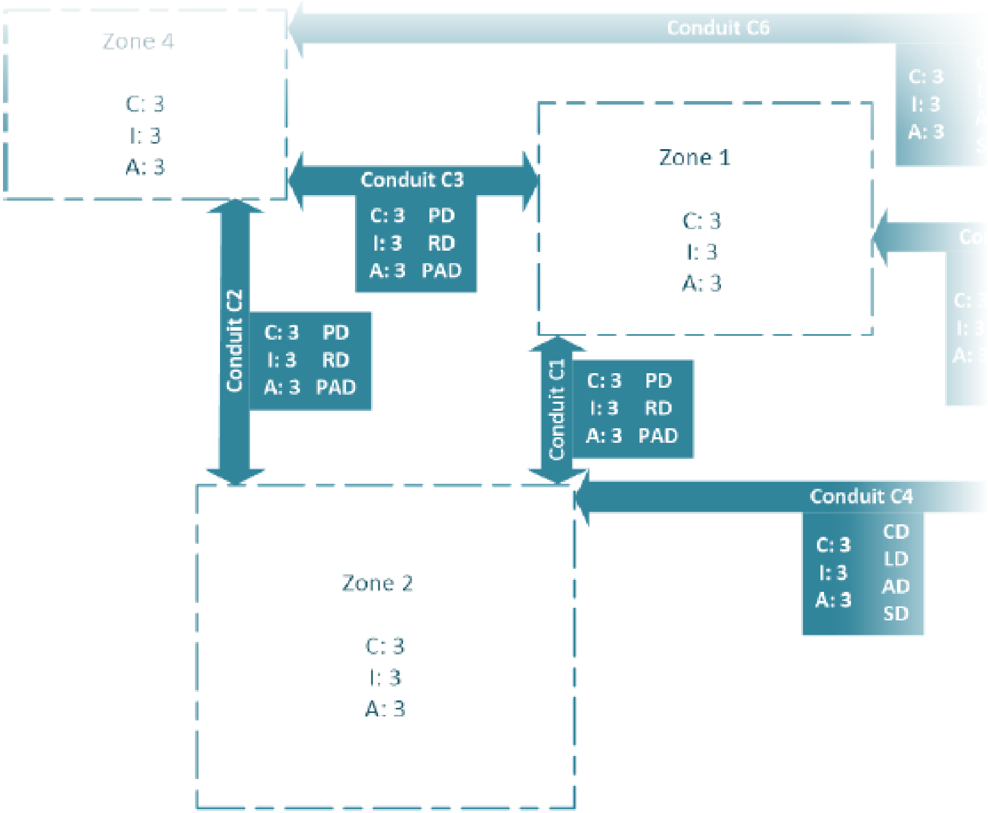
   – Protection need A for zone 2 = 3
   – Protection need I for zone 2 = 3
   – Protection need C for zone 2 = 3

5. **Conduit classification**

   For the necessary communication channels between the previously defined zones and conduits must be identified. In the same way as for the zones, the data transmitted via each conduit must be classified and their protection need (A/I/C) must be determined.

   Example: determined protection needs as schematic representation

   For our example plant, finally the following schematic representation results which shows the zones, conduits as well as the classified data with their protection needs:



6. **Specification of protective measures**

   Based on the evaluations in the steps 1 to 4, you can now specify the protection measures.
   A protection need of 3 (A/I/C) for zone 2, for example, can be fulfilled by

   - segmentation of the network
   - the connection of the main process in zone 2 to the system via a ring topology to increase availability
   - encrypted communication with other zones
   - firewalls, routing & VPN for securing the interfaces outside the zone boundaries
   - hardening measures of the devices in the zone, such as deactivation of unused device interfaces
   - implementing an Intrusion Detection System which monitors all data flows and generates an alarm in case of an unknown participant or an unusually high data transfer volume
   - installation of uninterruptible power supplies (UPS)
   - implementing protection measures regarding the environment of the plant (access control, lockable rooms and cabinets, installation of a fire alarm system, monitoring of the room climate
   - sensitization and training of employees on the subject of information security

   In particular for **zone 2** which contains a PLCnext Technology controller with periphery, the following measures are suitable:

   - SSH (certificates, user credentials) for securing Configuration Data and System Data.
   - HTTPS and user credentials for securing the communication with the Web-Based Management (WBM) of the controller.
   - TLS and user credentials secure the Log Data and Application Data transfer.
   - HTTPS and user credentials and cryptographic strong token for securing eHMI.
   - TPM (supplier root of trust) for secure storage of user credentials, keys, certificates (System Data).
   - Certificates secure the OPC UA communication.

7. After having implemented suitable security mechanisms (in accordance with the results of your assessment), the residual risk should be determined.

Data classification & protection needs

The central task for a threat-risk-assessment is the classification of data which is stored/processed in a zone and transmitted between zones via conduits.
This classification is done in two steps:

1. Identification of the data available in your system.
2. Classification of the data, i.e., determination of the protection needs of the identified data classes.

Data identification

Data class	Abbrev.	Description
Configuration Data	CD	Configuration data is located on the devices used to build automation infrastructures and systems
Log Data central	LD	Log data stored on a central Syslog server
Log Data onboard	LO	Log data available on the device, logging can be configured
Application Data	AD	Application data is located on the devices
Process Data	PD	Process data transferred between the devices and processed there
System Data	SD	System data (access data, keys, certificates) located on the devices
Recipe Data	RD	Recipes (which may also include proprietary data and trade secrets)
Parameter Data	PAD	Variable values (e.g., min, max)
Backup Data	BD	Backed-up data

Data classification (protection needs)

Based on the identified data classes, the protection needs can be determined. This classification is made under three aspects:

- A = Availability
- I = Integrity
- C = Confidentiality

Note: The data classification may vary from company to company. The classes listed below are examples.

Protection objective: **Availability**
To what extent must the information and processing functions be accessible to authorized users / resources, or what downtime is tolerable to the maximum?

Level	Description
1 - Negligible	The processing of the information can be postponed for up to several days or can be carried out manually for this period of time without significant damage being incurred.
2 - Moderate	The processing of the information may be up to one day or may be performed manually for that period without major damage.
3 - Serious	The processing of information may fail only rarely and for short periods of time (up to 4 hours). Otherwise, high damage is to be expected.
4 - Critical	The processing of the information must basically be continuous and may only fail for a very short period of time, not exceeding one hour. Otherwise (in case of failure for more than one hour) very high damages are to be expected.

Protection objective: **Integrity**
To what extent must uncontrolled changes and deliberate manipulation be prevented, or must the (machine) processing work flawlessly and reliably? To what extent must the actions of the users or the generation of the information be traced?

Level	Description
1 - Negligible	Deliberate or unintentional falsification of the processed information or information loss does not result in any significant damage. If the processed information is incomprehensible, no significant damage is to be expected.
2 - Moderate	Intentional or unintentional falsification of the processed information or loss of information can cause only medium damage. If the processed information is not bindingly traceable or provable to third parties, only medium damages can occur.
3 - Serious	Deliberate or unintentional falsification of the processed information or loss of information can cause serious damage. If the processed information is not legally binding or provable to a third party, it can cause serious damage.
4 - Critical	Intentional or unintentional falsification of the processed information or loss of information can cause very high damage. If the processed information is not legally binding or provable to third parties, it can cause very high damages.

Protection objective: **Confidentiality**
To what extent must unauthorized access to information and unauthorized disclosure and disclosure be prevented?

Level	Description
1 - Negligible	The processed information can be brought to the attention of anyone without significant damage or are explicitly intended for publication.
2 - Moderate	Information is processed whose access is restricted to authorized persons. If the information is disclosed to unauthorized persons, only moderate damage is to be expected.
3 - Serious	Information is processed whose access is restricted to authorized persons. If the information becomes known to unauthorized persons, high damages are to be expected.
4 - Critical	Information is processed whose access is restricted to authorized persons. If the information becomes known to unauthorized persons, I can expect very high damages.

Security levels

Security levels according to IEC 62443-3-3

To categorize the severity of potential threads, protection classes are available for the various data classes a zone stores/processes or a conduit transmits. This is the basis for the required level of protection of an entire zone or conduit.
In response to these protection need levels, the IEC 62443-3-3 standard defines Security Levels (SL). Furthermore, the standard maps SLs to system requirements by mentioning specific protection measures the system shall provide at each level.

The standard defines the SLs as level of confidence which indicates whether an industrial automation system is free of security vulnerabilities and operates in the intended manner. Thus, the SL can be considered as a qualitative degree of security. This way, an SL provides information by a single number about the severity of the threat scenario.

Note: By means of their SL, zones and conduits can be compared to each other with respect to their security capability.

The SL could be compared to the Safety Integration Level (SIL) in the field of safety engineering. The main difference between safety and security engineering is that the safety SIL can be calculated based on measurable system/component failures, malfunction or outages as well as on calculated probabilities of human misconduct during setup, operation, or maintenance. In terms of security, the threat reasons and incidents may be manifold: from operator carelessness to mistaken data tampering to malicious attacks by various means or via different channels. Therefore, the determination of the SL is more complex.

What does an SL refer to?

An SL relates to a zone or a conduit which was identified in your plant/ICS. Or put the other way around: the SL indicates the threat level of a zone/conduit, that has been assigned during the threat and risk analysis. Depending on the SL of a zone/conduit, the components involved must be selected.

Defined SLs

The following table describes the SLs defined in the standard (as they might be understood with practical examples):

SL	Profile	Description
SL1	– **Who?**: Operators, maintainers or any Internet user – **Means**: n/a – **Resources**: n/a – **Skills**: n/a – **Motivation**: none - rather carelessness/misuse	Accidental/(co)incidental violation/manipulation – "Accidental", for example, by a plant operator or maintenance personnel due to disregard of regulations or guidelines when handling facilities or data. – "(Co)incidental" by an external threat with the aim to misconfigure your system or the unauthorized disclosure of information.
SL2	– **Who?**: Individuals and companies with generic security knowledge – **Means**: simple – **Resources**: limited/common – **Skills**: basic/common – **Motivation**: low	Intentional but low-motivated violation using simple means: – Attacks with low motivation. – Attacks may be executed by any Internet user with generic skills who does not have specific knowledge to attack systems. – Attackers without detailed knowledge about your plant. – Attacks relating to this SL are often executed using automated tools. – Attacks often targeted to a wide range of plants instead of specifically one (your) system.
SL3	– **Who?**: Experts (incl. companies) who develop and use targeted attack means/scenarios for the purpose of profit – **Means**: sophisticated – **Resources**: moderate – **Skills**: plant-specific – **Motivation**: moderate	Intentional and moderate-motivated attacks with sophisticated means: – Attackers have expert security knowledge (high level hackers), – and/or advanced knowledge about your field of industry, your plants, weak interfaces or vulnerabilities in the hardware/software/protocols involved. – Attacks using tools specifically adapted to your plant as target. – Attackers with a higher degree of criminal energy than mentioned for SL2.
SL4	– **Who?**: Government organizations targeting specific targets, regardless of the costs incurred in doing so. – **Means**: highly sophisticated and aggressive – **Resources**: extended – **Skills**: plant-specific – **Motivation**: high	Intentional and aggressive attacks with highly sophisticated means: – Attackers have security knowledge of an expert group, – and/or expert knowledge about your field of industry, your plants, weak interfaces or vulnerabilities in the hardware/software/protocols involved. – Attacks using tools specifically adapted to your plant as target combined with high performance equipment. – Attackers with a higher degree of criminal energy as mentioned for SL3.

Ongoing security considerations

Security vulnerabilities can arise not only during the development of a plant or ICS. They can also result, e.g. by applied patches or changed guidelines during the plant's life cycle of after changes in the environment or new elements have been added to the plant.
Example: The change of a regulation for the user accounts management leads to security vulnerabilities. Additionally, when the inappropriate new account management is implemented, old user accounts are not deleted.

Therefore, the changing threat situation must be continuously monitored and analyzed. New attack methods as well as the overcoming of existing security mechanisms (e.g., an encryption technique) must lead to a corresponding defense reaction, i.e., the appropriate further development and optimization of security measures.

Types of SLs

Security levels do not only show the level of confidence in a zone or conduit. They can also be used to select the devices and components to implement technical security measures. Ideally, the SL-C (C = capability) of the selected components corresponds to the SL-T (T = target) to be achieved in the zone/conduit to be protected.

To be able to map the view on SLs from the different roles (plant owner, operator, system integrator, device supplier), three different types are distinguished.

- Target SLs (SL-T): Target security level according to the requirements resulting from the threat-risk-assessment you have performed.
- Achieved SLs (SL-A): Actual security level resulting from the operational and technical measures that are already implemented and applied.
- Capability SLs (SL-C): Security levels, each component/device to be involved in your ICS can provide.

Foundational requirements (FR) and system requirements (SR)

Foundational requirements (FR)

The IEC 62443 standard defines seven foundational requirements (FR). These are basic requirements regarding the security of an ICS. They are addressed to all stakeholders of a plant and used throughout the standard.

- **FR1:** Identification and authentication control (IAC)
  Protection by verifying the identity of any user before enabling communication
- **FR2:** Use control (UC)
  Protection against unauthorized actions by necessary privileges before performing
- **FR3:** System integrity (SI)
  Preventing modifications of information by unauthorized persons and systems
- **FR4:** Data confidentiality (DC)
  Preventing disclosure of information to unauthorized persons and systems
- **FR5:** Restricted data flow (RDF)
  Protection via zones and conduits to limit unnecessary data flow
- **FR6:** Timely response to event (TRE)
  Collecting, reporting, preserving automatically evidences to ensure timely corrective actions
- **FR7:** Resource availability (RA)
  Ability of device functionality in case of demand also during DoS attacks

System requirements (SR)

For each FR, part 3-3 of the IEC 62443 standard defines several system requirements (SRs). Each SR describes concrete requirements for the plant and thus describes the respective FR in detail. The example below shows details for FR4.

To comply with the standard, you must map the relevant SRs to the subsystems and components of your automation system.

Requirement enhancements (RE)

An SR can be supplemented by so-called requirement enhancements (REs) that have to be fulfilled for higher Security levels.

Example: FR4 with its SRs and REs

According to "FR4 - Data confidentiality", communication channels and data repositories must be protected against unauthorized disclosure. Depending on the security level (SL 1 to 4), the disclosure must be prevented with the means, resources, skills and motivation as defined in the SL classification table.

The following three SRs are defined for FR4, some of them with REs:
(The list also mentions which SR and RE must at least be fulfilled to achieve a particular security level (SL).)

- **SR 4.1:** Information confidentiality.
  Protection of the confidentiality of information for which explicit read authorization is supported.
  SR 4.1 (without any RE) must be fulfilled to achieve SL-C 1.
  - SR 4.1 RE 1: Protection of confidentiality at rest or in transit via untrusted networks.
    SR 4.1 + RE 1 must be fulfilled to achieve SL-C 2 or 3.
  - SR 4.1 RE 2: Protection of confidentiality across zone boundaries
    SR 4.1 + RE 1 + RE 2 must be fulfilled to achieve SL-C 4.
- **SR 4.2:** Information persistence.
  Purging all information for which explicit read authorization is supported before taking them out of service.
  To achieve SL-C 1, it is not necessary to fulfill SR 4.2.
  - SR 4.2 RE 1 – Purging of shared memory resources
    SR 4.2 + RE 1 must be fulfilled to achieve SL-C 3 or 4.
- **SR 4.3:** Use of cryptography
  Use of state-of-the-art cryptographic tools for key establishment and management.
  SR 4.3 must be fulfilled for any level SL-C 1 to 4.
  - No REs defined for this SR.

Security from the operator's view

Introduction

> **Note: Many requirements are listed in both standards IEC 62443-2-1 and ISO/IEC 27001**
> From a plant operator's point of view, many requirements apply that are defined in both ISO/IEC 27001 (which deals with IT system security) and IEC 62443-2-1 (draft edition 2.0). Even more: the two standards complement each other. The information in this topic can therefore be seen as a kind of mapping of particular relevant requirements which are defined in both standards.

The IEC 62443-2-1 standard defines the elements to establish a cyber-security management system for owners and operators of ICS. For that purpose, it lists specific security requirements with a special focus to ICS/OT the implementation of which is intended to protect the systems against unwanted access or attacks. These requirements are aimed to achieve the needed and best possible security according to the existing protection needs.
What "needed and best possible security" means in a specific plant must be assessed individually by each operator. Accordingly, the requirements defined in the standard must also be assessed and implemented individually by each operator for the respective plant. This is, because the general measures defined by the standard must be comprehensive enough, but should not be too restrictive (and in line with the available budget).

The requirements in the part 2-1 of the IEC 62443 standard series are organized into **Security Program Elements (SPEs)** that contain measures for establishing, implementing, maintaining, and continuously improving an SPE.

The present chapter summarizes those SPEs which relate in particular to the functionality of a plant and above all which correspond to the viewpoint of the plant operator. It therefore contains in a condensed form information from the previous chapters with the special focus of the plant operator. Details can be found in the standard.

SPE 1 – ORG 1.1

The plant operator must coordinate the Security Program (SP) with the ISMS (Information Security Management System) to ensure integrated Defense-in-Depth strategies for the ICS and coordinated operational (OT) and information (IT) security. SP and ISMS security administrators must collaborate. Common ICS network interfaces (such as firewalls or remote access) as well as a cross-interface user management should be designed and managed.

The plant operator should identify, investigate, and address areas of potential conflict.

A holistic security approach (360° security) for a plant can only result from the combination of personnel, hardware and software. To comply with the IEC 62443-2-1, SPs must therefore consider all of the following:

- Organizational measures (including organization-wide policies and practices) must be taken, **and**
- technical security functions provided by the hardware and software components involved must be configured and used, **and**
- security-related processes must be implemented for the secure setup/configuration/operation of the ICS and for maintaining its technical security functions.

SPE 2 - CM 1.1

The operator of the ICS must document, verify and maintain all included devices used to build automation infrastructures and systems, software components, communication protocols and ports in a verified inventory list (e.g., managed in a database).

This is the only way to ensure that the operator is aware of all components of the ICS and that all components are authorized and configured to meet the security requirements. The verified inventory list should also be used to record all changes to devices, components and communication paths.

SPE 3 - NET 1.1

The operator of an ICS must ensure that segmentation and communication policies are established and implemented for the interconnection of networks from the ICS and other networks. This is because external networks are a threat to the ICS as they allow access from potentially unknown sources.

The segmentation of networks allows to restrict data and control flows as well as the visibility between the ICS and external systems.

- All connections between the ICS and external networks/systems must be identified (as trustworthy or non-trustworthy), managed, authorized and documented.
- Only necessary data flows should be allowed.
- Connections between segments must be examined for threats.

SPE 4 - COMP 1.1

The plant operator must ensure that all hardware and software components included in the ICS are sufficiently protected against cyber attacks. Attacks can occur via internal interfaces (e.g., USB or configuration ports) and external interfaces (e.g., inter-process communication interfaces or APIs).

Devices used to build automation infrastructures and systems must be hardened prior to installing them in an ICS. Hardening includes, for example, removing or disabling unneeded functions, applications, network addresses and interfaces.

SPE 5 - DATA 1.1

To protect data from disclosure, tampering, loss, or loss of use, the system operator must perform a risk assessment. The goal of the risk assessment is to understand which data needs to be protected from which threats. See topic Threat and Risk Assessment.

SPE 5 - DATA 1.2

Data must be protected from threats according to its classification. The following protection mechanisms are possible:

- User access controls: Only users with appropriate permissions are allowed to access specific data or software.
- Permissions for the transmission of data: Restrict what data is transmitted and validate data and parameters to determine if they were changed during transmission or if invalid values were transmitted.
- Encryption: Protect data from disclosure.
- Digital signatures: Enable authentication and change detection based on a secure checksum.
- Physical access controls: Especially when the above options cannot be realized or if additional protection is desired. Access controls restrict physical and network access to computers and communication connections.

SPE 5 - DATA 1.4

If normal operation of the ICS cannot be maintained due to an identified security breach, the ICS must be brought into a predetermined secure state in order to limit further risks to the ICS (incl. health, safety, and environmental risks). This state is referred to as "fail-secure" (similar to the "fail-safe" from the functional safety area), into which the system is brought to protect itself from the hazard. Since this state is ICS specific, the operator must define it individually based on the risk to the ICS.

SPE 5 - DATA 1.6

After removing devices and components from the ICS and/or decommissioning them, the system operator must delete all confidential data that requires protection.

SPE 6 - USER 1.1

The plant operator must ensure that there is a plant-specific procedure for assigning identifiers, authenticators, and roles to users. Users in this context may be human users, software processes, and the devices used to build automation infrastructures and systems.

- Human users must be authenticated by their login data and will be given access to programs/data according to their role. Refer to the topic User Management for details.
- Software processes must be authenticated when connect to any process within the ICS.
- Devices connected to any device in the ICS must be identified and verified as authorized.

SPE 6 - USER 1.2

User accounts that are no longer needed must be removed or deactivated immediately. For this purpose, the operator must set up a separate procedure, in close coordination with Human Resources.

SPE 6 - USER 1.3

The user IDs, authenticators, roles and associated access rights must be configured so that they cannot be automatically disabled. This could result in the inability to perform essential operations (those that ensure health, safety, environmental and system availability). A risk assessment is required in which the plant operator identifies essential operations, their software dependencies, and associated user accounts.

Policies should be established and implemented for the identified user accounts to ensure that they automatically expire or are automatically terminated.

SPE 7

The operator must implement suitable measures for the timely detection, logging, analysis, and management of security-related events and hazards. Such measures serve to identify security-related problems, initiate actions, and record responsibilities.
Security-relevant events must be reported and written to protected event or audit logs. These logs must be retained for an appropriate period of time.

The system operator must ensure that the appropriate capabilities are in place to restore the system to its previous state if needed. For this, a site disaster recovery plan (DRP), business continuity plan (BCP), or both must be deployed and kept up to date. These plans must include disaster scenarios, error handling procedures, and processes to maintain the required level of business continuity.

ICS security concept by Phoenix Contact

This topic describes how Phoenix Contact solves the requirements regarding cyber-security.

Note: This description and the illustrations in this chapter are schematic and exemplary in nature. They do not claim to be complete. Details on technical implementations and practical realization can be found in the respective product-related security guides.

General considerations and Phoenix Contact certifications

Phoenix Contact understands and implements security holistically: as a device/component manufacturer and as a system integrator and keeps a close eye on plant owners (as end customer). This is possible because Phoenix Contact is familiar with the challenges of plant owners since production is also the core element of Phoenix Contact business processes.

In practice, this means that Phoenix Contact has to decided to comply with the IEC 62443 standard as this is the comprehensive standard for OT (ICS networks) security.
Phoenix Contact is active on all three levels of the IEC 62443: device/component manufacturer, system integrator and plant owner. Therefore, our customers can rely on our security expertise as well as on the fact that Phoenix Contact products are developed securely according to the IEC 62443 standard. Many of the measures described here are direct answers to the general requirements in ISO 27001 which is the recognized and applicable standard for security processes in plant IT networks. Both standard are complementary to each other.

To prove this, Phoenix Contact has been certified according to the following parts of the IEC 62443 standard:

- Part 4-1 certified product development process. This certificate confirms that Phoenix Contact has completely defined security processes and applies them for certain product developments.
- Part 3-3: Certification of the security system building capabilities.
- Part 2-4: Certification of the system integration services. This certificate covers system development at Phoenix Contact as well as at the premises of the plant owner.

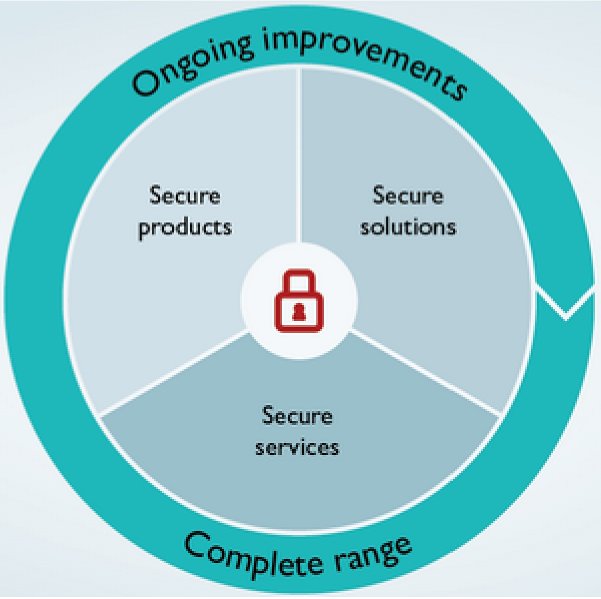
Further Information: Refer to the topic IEC 62443 Standard: Security for Industrial Applications for further information on the standard and the division of its parts.

360° security: our portfolio

As mentioned before, Phoenix Contact considers cyber security holistically. The basic idea of what we call 360° security is that an adequate security concept must include the technology used, defined processes, and the people involved, i.e., it must specify both technological and organizational measures.

Refer to 360° Security - The Holistic Approach for further information.

Transferred to us as a supplier of products, solutions and services this means:



Phoenix Contact...

- operates a secure development process. Security measures are implemented, verified and documented based on a threat analysis. Phoenix Contact products implement various security functions. Regular checks ensure the identification of any security vulnerabilities. Security updates then close the security gaps.
- offers various services to support you: from assessing your individual security level and providing advice on how to improve your security to training your staff. All services conform to the highest security standards.
- provides you with secure automation solutions and security architectures for a wide range of requirements and industries.

Technical and organizational security measures

Technical and organizational security measures

To achieve security, a holistic approach is necessary: An adequate security concept must include the technology used, defined processes, and the people involved, i.e., it must specify both technological and organizational measures.

Many but not all threats can be defended against with appropriate technical measures. These technical measures must be supplemented by organizational measures that address personnel, procedures, policies and practices. Please refer to 360° Security- The Holistic Approach for details.

From the systemic point of view, further requirements and interfaces arise regarding the following:

- Network architecture of the automation solution
- Configuration of the automation solution
- User account management
- Certificate management
- Firewall settings management
- Device and patch management
- Remote Maintenance

The following aspects can help to fulfill these requirements:

- Network segmentation: Data exchange between different internal plant parts (zones) can be configured.
- Use of firewalls.
- Encrypted data transmission: Incoming and outgoing communication can be encrypted using VPN, for example via IPsec or OpenVPN.
- Authentication of any human user or software process that request the establishment of a communication connection within your network (for example using certificates).
- Implementation of a secure certificate management/PKI system.
- Integration into user administrations: By configuring users network-wide, each employee can be assigned and managed individual access.
- Secure remote access: For remote maintenance of machines via insecure networks, it makes sense to use additional security appliances (e.g. mGuard from Phoenix Contact). Here, it is important that the configurations of the devices used to build automation infrastructures and systems are matched to each other. Secure remote access is also mandatory for wireless connections (mobile access).
- Implementation of a powerful (new generation) anti-malware inspection tool on all network components for which a tool is available and can be installed. Other components (if no anti-malware tools can be installed) should be protected by alternative measures.
- Implementation of NAT/PAT devices which protect the devices located in your internal (private) networks from being visible from the external (public) network.
  In addition, individual device ports in the internal network that can be accessed, for example, via connected laptops or mobile storage media should be protected and report an alarm in the event of a local attack.
- Implementation of a suitable logging and monitoring system which allows the continuous evaluation of events, accesses etc. in your plant network.
- Realization of suitable PC hardening measures that reduce the risk of compromized engineering/configuration PCs in your network which in turn could influence the application running on controllers or the configuration of any network device or field device.
- Implementation of a suitable data backup system that enables the data recovery after a data loss or a necessary attack-related reconfiguration/setup of system components.
- Integration with device and patch management: Intelligent and efficient device and patch management is provided as a solution or interface for managing multiple devices in the automation solution. It enables the central creation and administration of all security-relevant device settings and supports firmware upgrades.

Network segmentation

It is difficult to determine the protection needs of an entire plant and to implement protective measures on this basis. If an office network, factory network and, for example, production line networks are directly connected to each other, malfunctions and viruses can be spread directly over all network parts. Network segmentation eliminates the risk that any data can directly be transferred between external networks or, e.g. the office environment and the production area/ ICS networks.

The IEC 62443 standard divides a complete system into so-called zones and conduits. In practical implementation this means that the network to be protected must be segmented. The resulting network segments (cells) as well as the data paths between them can then be protected by targeted security measures.

> **Further Information:** Basic information on the definition of zones and conduits according to the IEC 62443 can be found in Zones and conduits

Zones, cells, segments

In terms of the standard, a zone can be a physical and/or logical group of system components to **which the same security requirements apply**.

However, for the purposes of this manual, we look at segmentation a little differently: We divide the entire plant into segments/cells that are physically connected to each other and form a physical zone, so to speak. Each of these cells has a specific protection need.

Deviating from the IEC 62443 standard, we consider only such cells to be zones, although the standard also defines purely logical groups as zones.

If we look at the specific (technical) security measures to be implemented, these are generally limited to physical network segments (cells). Since we equate cell = zone, the required protection measures are easier and more clear to implement. As a result, we may get several cells (= zones) with the same protection need (security level) although the standard would comprise them into one zone.

Requirements and general considerations

The operator of an ICS must ensure that segmentation and communication policies are established and implemented for the interconnection of networks from the ICS and other networks. This is because external networks are a threat to the ICS as they allow access from potentially unknown sources.

The segmentation of networks allows to restrict data and control flows as well as the visibility between the ICS and external systems. The plant operator should identify, manage, authorize, and document all connections between the ICS and external systems.

Only the data flows that are necessary should be allowed. In the context of network segmentation, the connections between segments must be examined for threats and the associated risks. The documentation to be prepared must note these security risks and their designation as trustworthy or non-trustworthy. For non-trusted connections, a high level of protection is required. Identifying the non-trusted connections is a fundamental step in establishing network access controls.

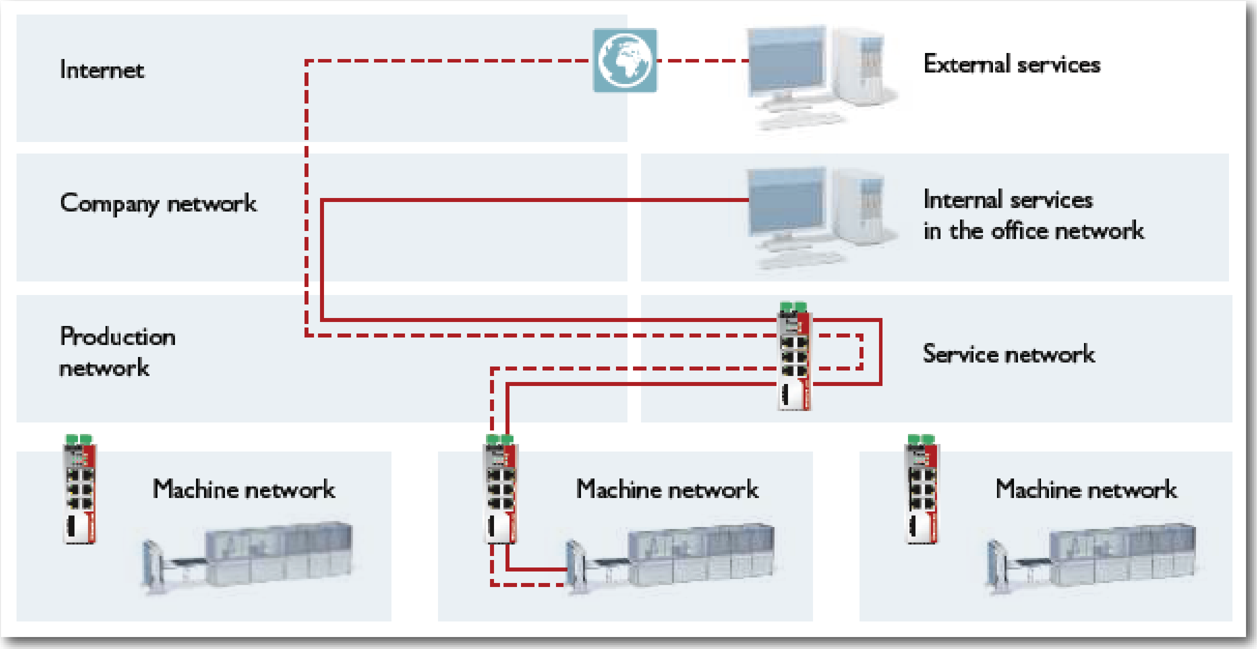
If a functional safety system network is integrated in the ICS, the plant operator must ensure that the safety system is not affected by non-safety (i.e., standard) system networks and devices. To protect the safety system from interference, for example, firewalls or gateways can be used to manage access to the safety system. This way, a certain separation between the (standard) control system and the safety system can be realized.

The resulting segments can be separated using VLANs or firewalls. Routers or Layer 3 switches then need to be used for communication between the individual network segments. These devices intercept typical network errors, preventing them from spreading further to the rest of the network.

Separation: OT (ICS), IT and cloud

Details on the differences between IT and OT (ICS) networks can be found in IT and OT/ICS: A Comparison.

The following figure shows an example where mGuard security routers handle the communication between network segments.



Rules for network segmentation

According to the IEC 62443 standard, the following rules apply when segmenting the ICS into zones and conduits:

- According to "FR5 - Restricted data flow", zones and conduits must be defined in such a way that unnecessary data flow is prevented.
  Depending on the security level (SL 1 to 4), the casual/coincidental or intended circumvention of the defined zone and conduit segmentation must be prevented with the means, resources, skills and motivation as defined in the SL classification table.
- Conduits should control the information flow and separate the ICS from public networks.
- Network components which represent a zone border must be able to protect the zone.

  At zone borders, which represent the transfer point between a zone and a conduit, only network devices should be used which are able to protect the zone border by monitoring and controlling the inter-zone communication (represented by a conduit).
  These are mainly devices with managed interfaces such as firewalls, encrypted tunnels, routers, proxies, (unidirectional) gateways.

Note: Also dual-homed devices (PCs, controllers etc.) should be considered. Such devices have two network interfaces and they are part of two networks at the same time. In this architecture, these devices can form (unintentional) conduits and become (undetected) security risks.

Possible measures for implementation

Possible measures to protect zones and secure interzone communication:

- Firewalls
- Determine communication relations according to the least privilege concept: The default is "deny" and only needed communication relations should be explicitly allowed.
- Routers or Layer 3 switches handle the communication between network segments
- Prohibition of uncontrolled access
  (e.g. mobile routers)
- Isolation/separation from the Internet
  - No routing of DNS requests to the Internet
  - No default route
  - Use of a Web Proxy
- Locks with exceptions (for pass)
- Network Address Translation (NAT)
- Port Forwarding

Remote access/remote maintenance

Consideration: risks and benefits

The increasing network capabilities of devices used to build automation infrastructures and systems enable a variety of new opportunities. Remote access to systems and data facilitates monitoring and maintenance of plants via the Internet. This saves costs, shortens the response time to problems that arise during operation, and can significantly reduce the risk of a production stoppage. Specialists no longer need to be on site to avert damage or loss.

However, where remote access is possible, misuse is also possible. Devices that are connected to a network via Ethernet are generally at risk of unauthorized network access. To prevent unauthorized third parties from accessing devices (controllers, switches, etc.) and making changes or corrupting/stealing data, appropriate access control measures must be taken.

> **Note:**
> Devices with communication interfaces (e.g., controllers) but without any built-in network security functions should never be used in security-critical applications without a suitable security appliance.
> Note that unauthorized access can also occur, for example, via the following device interfaces: USB ports, PCI express interfaces, Ethernet interfaces, bus interfaces (e.g. Axioline or Profinet), SD card slots, device HMI (such as touch panels and other operating elements).

Making remote access controllable

Basically, remote access should only be possible "on demand". For this purpose, the plant can be switched to a special maintenance mode, for example, by means of a key switch. In maintenance mode, the equipment may only operate with special attention to operational security and safety.

An implemented firewall should provide an appropriate configuration for this mode, e.g. by blocking (retroactive) effects to the production network. Furthermore, access must be restricted to actually required interfaces. If, for example, only access to the desktop transfer is enabled, the risk of malware infection is significantly reduced.

> **Note:** In addition to remote access via Ethernet, "real access" on site must also be controlled and restricted if necessary.

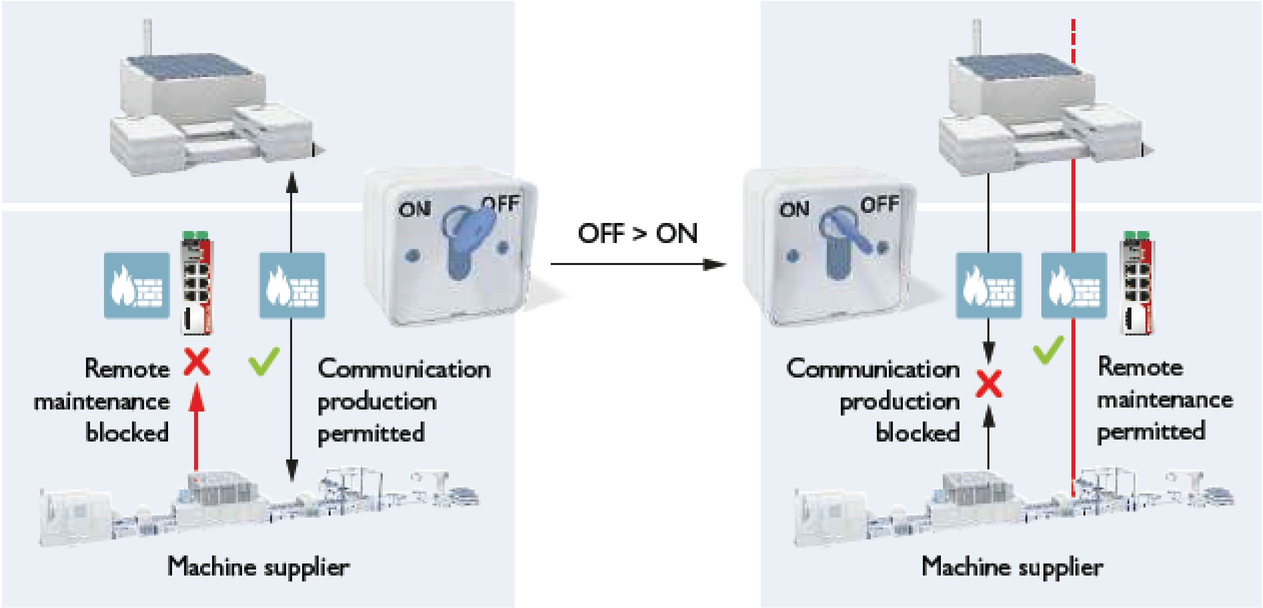
For your use case, check the possibility of disabling active communication channels (e.g. SNMP, FTP, BootP, DHCP, HTTP, HTTPS etc.) or assigning passwords.

Take further protective measures according to the IT security requirements and the applicable standards for your area of operation to prevent unauthorized access to your network. Such measures can be:

- Virtual networks (VPN) to ensure encrypted communication.

  Note that the establishment of (encrypted) VPN connections directly to the remote maintainer must be viewed particularly critically, since there is no control over the actions performed via the VPN connection.

  For securing networks for remote maintenance via VPN, Phoenix Contact offers the mGuard product line as a security appliance. Refer to the current Phoenix Contact product catalog (phoenixcontact.net/products).
- Use of secured communication channels. For example, data is transmitted encrypted using HTTPS (Hypertext Transfer Protocol Secure). Furthermore, the communication partners involved may have to authenticate themselves with certificates when establishing the connection.
- Installation of a key switch on the machine to initiate or inhibit remote access. The figure below shows an example. A key switch ensures that only intended changes can be made to the machine. At the same time, the key switch also enables the communication rules in the network to be blocked while remote maintenance is being carried out.
- Secure passwords for all access ways to ICS devices. This should also include access from mobile end devices via WLAN.


ON
OFF
Remote maintenance blocked
Communication production permitted
Machine supplier
OFF > ON
ON
OFF
Communication production blocked
Remote maintenance permitted
Machine supplier

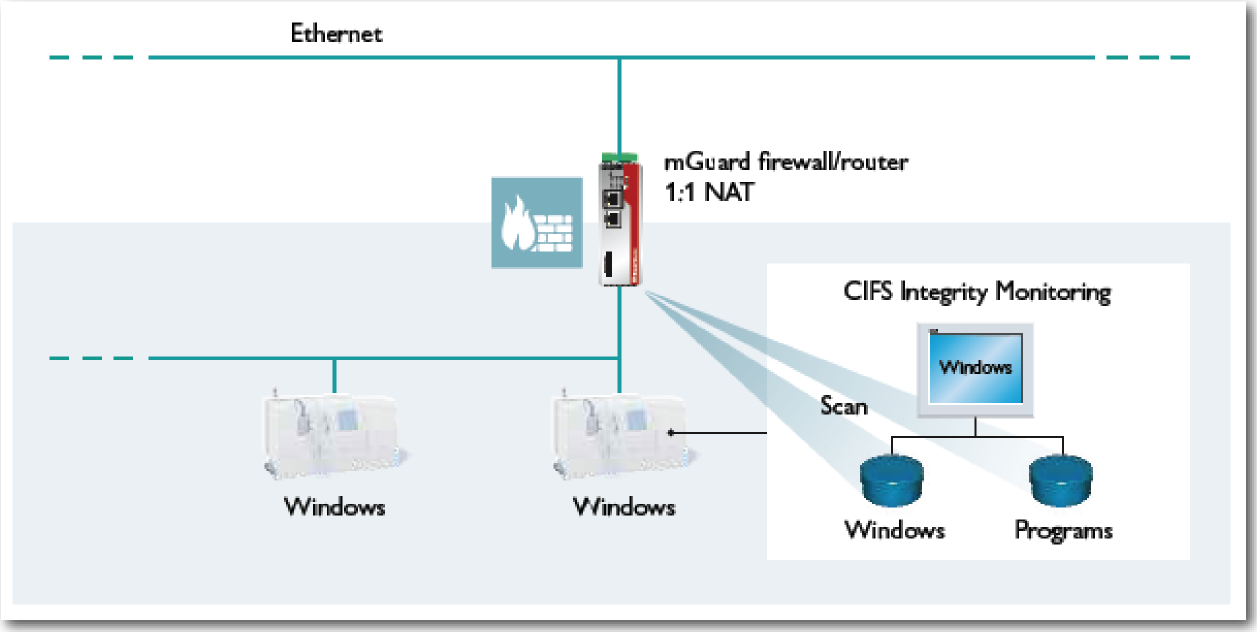
Firewalls

General information on firewalls

A firewall is a system component which protects individual computers, IT systems and ICS networks from attacks and data corruption/misuse. Firewalls can prevent or restrict the spread of malware.
The firewall is installed at a suitable system boundary. i.e., zone boundary in our context. It analyzes the inbound and outbound data traffic and detects unauthorized access based on the properties of the network packet. Network packets that are not allowed are blocked by the firewall.

By eliminating all of the communication options that are not technically necessary, many attacks to your network would not even be possible. In addition, industrial integrity monitoring helps you detect and halt the impact of changes and manipulations to Windows®-based systems, such as controllers, operator interfaces or PCs, in good time.

The following figure shows an example with an mGuard firewall/router and 1:1 NAT as well as integrity monitoring.



Configurable firewall features

For configuration purposes, each firewall offers a corresponding user interface where rules and exceptions for blocking and passing must be defined. Such rules are, for example:

Note: Some of the feature mentioned below are only supported by so-called Next Generation Firewalls (NGFW).

- **Packet Filtering**: Which network packets are allowed to pass? To determine this, the firewall evaluates the IP-related information such as the packet's IP source and destination address and the ports used by the communication connection.

  Firewalls that support **Stateful Packet Inspection** also evaluate the condition of the IP connection involved. See section Stateless and stateful firewalls for details.

  If **Deep Packet Inspection (DPI)** is supported, dynamic packet filtering also takes place. The information contained in the data packets is read, analyzed and evaluated. The firewall recognizes the type of user data (text, graphics, audio, video). In this way, different types of malware can be detected, which can prevent DoS attacks, for example. In addition, unwanted data traffic (e.g. Spam) can be detected and filtered out (reduction of data traffic load).

  > **Note:**
  > - DPI works only for plain (unencrypted) traffic.
  > - Since the content of the data packets is read, compliance with applicable data protection guidelines must be ensured when using DPI.

- **Network Access Translation**: A NAT function hides the resources behind the firewall from the public network thus making them unavailable from external. See topic Network Access Translation for details.
- **Proxy**: If a firewall supports the proxy function, it can be parameterized to forward requests to the external network coming from inside the protected zone. This way, the firewall appears as source for outbound data packages. A proxy handles vicariously the entire communication and it is able to analyze and block (if required) transmitted content. This way, participants inside the protected zone can be prevented from loading unauthorized content outside. **Configurable content filters** may enhance this functionality. **Note:** In addition, the proxy may be able to provide the same services for inbound traffic.
  The most common type of proxy is an HTTP proxy for web traffic.
- **URL Filtering**: URL filters are typical functions of HTTP/web proxies. By defining a list of URLs of forbidden websites or services (black list), the access to potentially harmful data sources can be blocked for participants inside the protected zone. In the same way, a white list can define permitted sites that have been verified as non-hazardous. See section Black/white lists for details.
- **Antivirus and Malware Inspection**: All system components for which anti-malware software is available should be protected with a modern (next generation) malware prevention tool. For details, refer to Antivirus and malware inspection.

Stateless and stateful firewalls

Firewalls that support Stateful Packet Inspection are referred to as stateful firewalls. The difference between stateless and stateful firewalls is described in the following.

A "classical" **stateless firewall** inspects ingoing network packages based on filtering rules which have been defined for inbound and outbound traffic by an administrator. For that purpose, it inspects, for example, only the source and destination IP address of network packets. Since the permitted data traffic must be configured for both transmission directions, it is not possible to determine which of the communication partners (peers) initiated the connection. As this is static information, such a firewall is referred to as stateless firewall. If an inbound data packet matches the conditions for passing, the stateless firewall guides it into the network (according to defined rules). Otherwise, i.e, if a packet cannot be identified, it is rejected.

In contrast, a **stateful firewall** controls the network traffic on a more comprehensive basis and is therefore more restrictive. For that purpose, it inspects the entire state of the existing network connections by considering state information from past communications.
For example, a stateful firewall also considers the connection state by analyzing the data transfer on the transport layer (which is the 4th layer of the OSI model). This way, it inspects the complete context of the network and decides dynamically on each current communication attempt.

Usually, a stateful firewall inspects five properties of IP headers: source address, destination address, source port, destination port, protocol. On this inspection basis, it is able to detect the following:

- Addressing anomalies (IP source and destination address identical, broadcast/multicast source address, etc.)
- Packet anomalies (incorrect IP address, bad IP header checksum, incorrect IP options, etc.),
- Fragmentation anomalies (IP length errors, etc.),
- Protocol anomalies (e.g., incorrect TCP flags and TCP sequence numbers)

A stateful firewall works according to the handshake principle and takes the times into account at which data packets are expected and received (timeouts are possible).

Any permitted connections (packets) are entered in a dynamic state table allowing connection tracking. Since NAT gateways must assign port numbers dynamically, they require state tables and are therefore always stateful.

Conclusion: Stateful firewalls provide a higher level of protection than stateless firewalls. Therefore, they are the current state of the art. Stateless firewalls are hardly available on the market anymore.
However, they require a higher hardware performance due to their operating principle. This makes them more vulnerable to DDoS attacks.

Integrated and dedicated firewalls

A firewall can be installed on a separate hardware unit (which is then referred to as "dedicated firewall") or it can be a software component which is installed within the unit to be protected ("integrated firewall").

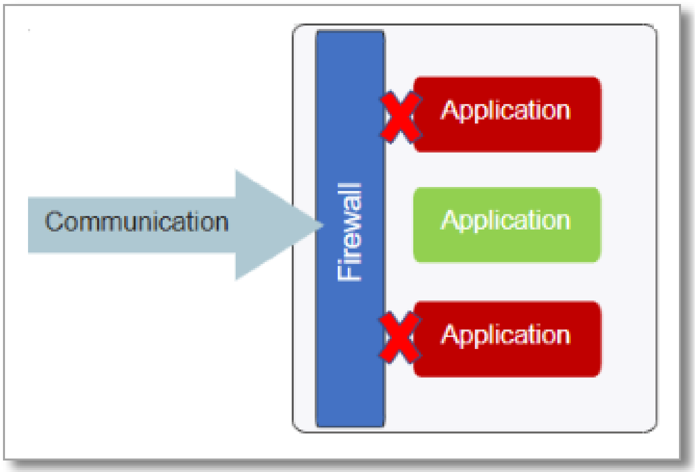


Figure 1: Integrated firewall

An integrated firewall, as shown in *Figure 1*, offers cost advantages but is more vulnerable to attacks, depending on the quality of the main system implementation. If many different components with integrated firewalls are to be used, all possible variants must be administered and maintained. If the main system is successfully attacked, the firewall can be infiltrated as well.

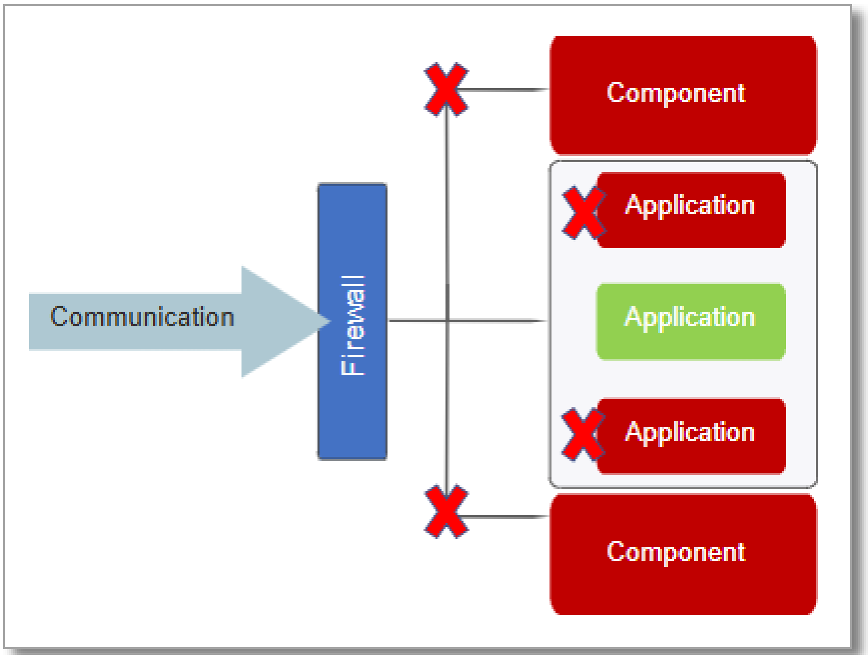


Figure 2: Dedicated firewall

A dedicated firewall as a stand-alone device (*Figure 2*) requires a targeted investment but allows selection independent of the other automation components. In addition, there are the following advantages of dedicated firewalls over integrated firewalls:

- Central administration is possible.
- Component is more robust against vulnerabilities in other automation components.
- Patches and updates are possible without affecting the function of the overall system.
- In the event of a network overload, the firewall can absorb the load thus protecting the automation components behind it.

Firewall(s) protecting the demilitarized Zone (DMZ)

The DMZ is a buffer zone between the ICS and other networks. This other network can be a public one or, for example, an internal office network. See section Special zone: DMZ for details.

A DMZ can be protected by one or two firewalls:

- When implementing a single firewall (e.g., for cost reasons), this firewall should at least provide three network ports for connecting the external network, the DMZ and the ICS-internal network.
- When implementing two firewalls, one could be located between the external network and the DMZ, another firewall between the DMZ and other ICS-zones.

The DMZ firewall(s) must control the data flow as follows:

- Accesses from external networks (Internet) must only be possible to components (authentication servers, application gateway, etc.) in the DMZ. No direct access from external networks to resources within the ICS network is allowed.
- Accesses from the ICS-internal network must not directly access resources located in external networks. Instead, an intermediate point such as a proxy server in the DMZ must be interposed.
- Data packages must only leave the DMZ (in direction internal network and Internet) if they are authorized accordingly.

Blacklists and whitelists

Blacklists and whitelists pursue opposing strategies. Therefore, usually only one of the two lists is used, but not both together.

- A **whitelist** is a "positive list", or in other words a list of all exceptions to a general prohibition. This means that no connections are allowed through the appropriately configured firewall except those explicitly listed on the whitelist. A prerequisite for the use of a whitelist is that all permitted connections must be known. The list must be updated for each new communication connection that is classified trustworthy.
- A **blacklist** is a "negative list", i.e. a list of all exceptions to a blanket permission. It contains all connections that are considered untrustworthy and should therefore be prevented. A prerequisite (and a disadvantage) for using a blacklist is that all prohibited connections must be known.

Further information: For detailed information on the management settings for the firewall used refer to the respective user manual or the online help of the corresponding configuration software.

Anti-malware inspection

The list of security incidents in industry is growing longer all the time: Stuxnet, Industroyer, TRITON, or WannaCry are examples of malware/ransomware which attacked SCADA systems, safety controllers etc.

While anti-virus/anti-malware software is common and widespread on IT systems, OT components are often still unprotected. Often, the corresponding tools for OT components are not available or are more complicated or, depending on the component, cannot be installed at all.

Components to be protected

All system components for which anti-malware software is available should be protected with a modern (next generation) malware prevention tool. These system components include:

- Plant management systems/server.
- Patch management systems/server.
- Engineering systems (PCs, tablets).
  Malware could modify or destroy controller/PLC applications developed on an engineering PC with an engineering/programing system. If not detected, infected or malfunctioning applications could be written to the controller/PLC. In addition, malware could use debug/remote control functions of the engineering software to take control of connected controllers/PLCs (change the operating mode, stop the controller etc.)
- Parameterization/configuration systems for network/field devices (PCs, tablets).
  Malware could modify or destroy device configurations/parameter sets. If not detected, wrong parameter/configuration data could be written to the network devices.
- Visualization and HMI systems (PCs, tablets).
  Malware could modify or prevent the visualization display. In addition, malware could use HMI control functions to take control of connected controllers/PLCs (change the operating mode, stop the controller etc.)
- Logging and monitoring systems (PCs, tablets).
  Malware could modify or delete log data or prevent external monitoring.
- Data backup systems and media, including cloud storages
  Malware could modify, delete or encrypt data backups.

Configuration/operation rules for anti-malware tools

- Access to the configuration settings of the anti-malware software should be restricted to specially authorized persons (administrator).
- The configuration settings as well as the results of the scans should be documented and logged.
- Configure the installed anti-malware software to achieve the best possible balance between security and availability of your plant. Especially for time-critical applications, a system scan must not affect the performance of the system.
- After the initial installation and configuration of the anti-malware software, run a full system scan. Make sure that the signature database is up-to-date.
- Configure regular automatic scans. When partial or full scans can be done depends on your application (workload, performance).
- Manual scans (especially complete ones) should only take place outside regular production operation (e.g. during shutdown, maintenance or setup operation) to avoid causing performance problems.
- Any access to data and applications should trigger an automatic scan (in addition to regular automatic scans). Take other appropriate protective measures if such continuous scanning on access is not possible due to performance reasons (refer to the next section).
- If you include network drives in the scanning process, make sure that they are not scanned by multiple instances of the anti-malware software and that no performance problems can occur (e.g. due to network overload).
- Update the anti-malware software regularly, in the shortest possible intervals that your application or production process allows.
- Update your anti-malware systems (e.g., virus signatures databases) automatically and from a central location (e.g., via a local update service in the DMZ). Never download updates directly from the Internet.
- Take into account the possibility that updating the anti-malware software (for example, due to an incorrect signature database) may cause problems in the application. Therefore, divide the systems into "update groups", assigning redundant systems to different groups. Then update the databases of the groups in sufficient time interval. This allows you to respond (without complete system downtime) to problem-causing updates.

Alternative measures if no anti-malware tools can be installed

Especially on controllers or smart field devices, anti-malware tools may not be available. Even on computer systems, application-related scenarios are possible in which only limited malware protection is possible (for example due to performance problems or lack of possibility for regular updates). The following measures should then be taken as an alternative:

- Separation of the affected component into a separate zone.
- Application whitelisting.
- Regular scanning of the affected component from a connectable device (e.g., laptop with installed anti-malware tool).

Next generation anti-malware software

Next generation anti-malware tools offer improved endpoint protection compared to traditional antivirus programs. They not only detect known file-based malware using a signature database and heuristic methods, but also protect against unknown malware (zero-day attacks, file-less non-malware attacks). They are also able to detect malicious behavior and respond to TTPs (Tactics, Techniques, and Procedures) from unknown attackers.

Thanks to new technologies, next generation malware protection programs are able to respond to previously unknown threats. For this purpose, comprehensive data is collected on attacks that have taken place. This data provides information on how the threat originated, other potential points of attack in your plant, how to potentially recover affected areas, and how to close the vulnerability. Furthermore next generation anti-malware tools may support machine learning and cloud-based, configurable behavior detection. Ideally, these tools will be able to share information gained in this way with other entities in your company or community.

Especially in networked systems (zones and conduits), it can be crucial that the malware protection program is able to immediately stop network activities for the affected zones or processes, isolate (quarantine) and clean affected systems in the event of an attack.

NAT and port forwarding

General information

Network Address Translation (NAT) separates internal (private) and external (public) network areas. A NAT device (which is usually located at the network or zone border) exchanges public and private IP addresses. This way, all internal network addresses are hidden behind the external address and private addresses can be used in the delimited internal network.
Outgoing connections are mapped to different port numbers on the outside. For ingoing connections, one entire private network can be addressed via one "common" external IP address.

Devices in local internal networks can thus be connected to the external network (Internet) without these having public IP addresses and without these addresses having to be known in the external network.

1:1 NAT

1:1 NAT is always a 1:1 IP address replacement, i.e. to each public address relates exactly one private address. This means IP addresses are mapped and ports numbers are not changed. 1:1 NAT does not strictly need connection tracking as the mapping is static. Both directions, ingoing and outgoing are equal.

Example for 1:1 NAT: 10 machines have the internal network address 192.168.1.0/24. This could not be routed. The 1:1 NAT-device maps each machine to a different network 10.0.1.x, 10.0.2.x etc such that from outside the machines all components can be distinguished.

NAT with port forwarding

The term NAT is typically used to describe the mapping of an internal network to **one** external IP address. While 1:1 NAT is always a 1:1 IP address replacement, with NAT, multiple IP addresses share one single IP address after translation.

Port numbers are used to ensure unique assignment of data packets. Consequently port numbers of outgoing connections need to be mapped to avoid conflicts. This requires connection tracking.
This type of address translation may also be known as PAT (Port and Address Translation).

Since incoming connections do not know which internal IP (and port) the connection should be connected to, such a connection must be configured in advance. This is called port forwarding.

As there is an automatic assignment of outgoing connections, no connections to the internal network are possible. Port forwarding allows to specify for external ports to which internal component a connection request should be forwarded. This allows the internal services to be used from the outside.

Security aspect of NAT

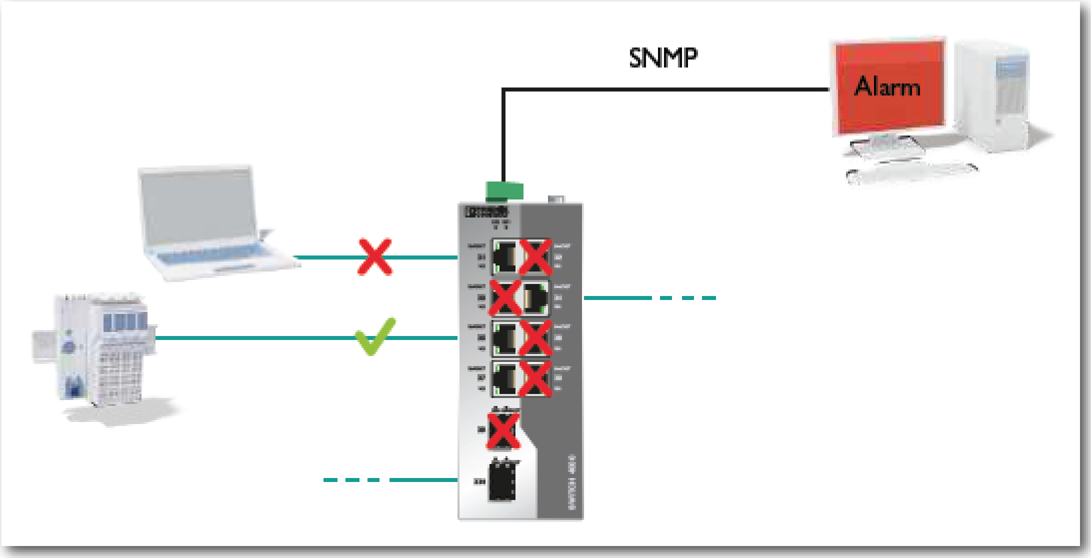
As address translation interrupts the end-to-end connectivity of the communication, this technology also provides a way to protect the internal network: The devices in the internal network are located behind the NAT router and cannot be accessed from the public network. Only the end device can establish a connection.

Note: Although this protection effect is similar to that of a simple firewall, NAT cannot substitute a dedicated firewall with packet filtering.

Port protection and port alerts

Infected hardware, like USB sticks or laptops, can transfer malware to the network. The following measures can be taken to prevent this:

- Configure the port security function of the devices involved in a way that unknown devices cannot exchange data with the network.
- Switch off any available ports that are not required.
- Activate any alert functions provided by the devices involved. For example, alerts via SNMP and signal contact can be sent if an unauthorized access to the network is detected.
- Protect wireless connections (mobile access) via WiFi/WLAN networks against unauthorized use.



(Central) User management

General considerations on user management

If communication is allowed through a firewall or possible via local access, access should be protected by a user login. Users in this context may be human users, software processes, and devices used to build automation infrastructures and systems.

- **Human users:**
  They must be authenticated when logging on and will be given access to run programs under the account used to log in.
  According to the IEC 62443 standard, the authentication of human users is necessary "on all interfaces capable of human user access". This includes local human-machine-interfaces (touchscreens, keyboards and further command devices), and network protocols designed for human user interactions (HTTP, HTTPS, FTP and SFTP) as well as open and proprietary protocols which are, for example, implemented with device configuration tools.
- **Software processes:**
  Processes must be authenticated when they are automatically started by the operating system and run under the account under which they were started.
- **Devices:**
  While a device is connected to the system, its identity must be verified. This ensures that devices are authorized to participate in system operation.

Note: Exceptions can be considered for display-only or basic machine operation. All administrative access should be protected.

This topic relates to the identification and authentication of human users.

User management can be done locally, but is then difficult to administer. Central user management systems, as shown in the example below, are more practical

Note: If a system does not support access control, a dedicated firewall can help by permitting predefined connections only if the user has previously logged on to the firewall.

Roles (e.g., operator, process engineer, maintenance engineer or administrator) are groups of access rights that can be assigned to human users. If identifiers, authenticators, and roles are used, user access controls can be managed more easily. Furthermore, this reduces the potential for errors and omissions in the corresponding processes.
Depending on how the users will use the system, the roles for the ICS will be defined. A user may have one or more roles.

Each user needs "credentials" (password, smart card holding a private key) and the system needs "authenticators" (hashed password, certificate issued for the smart card and/or its user). Furthermore, authorizations must be assigned, i.e. it must be defined which operations the user may perform, which resources he may use and which data he may access.

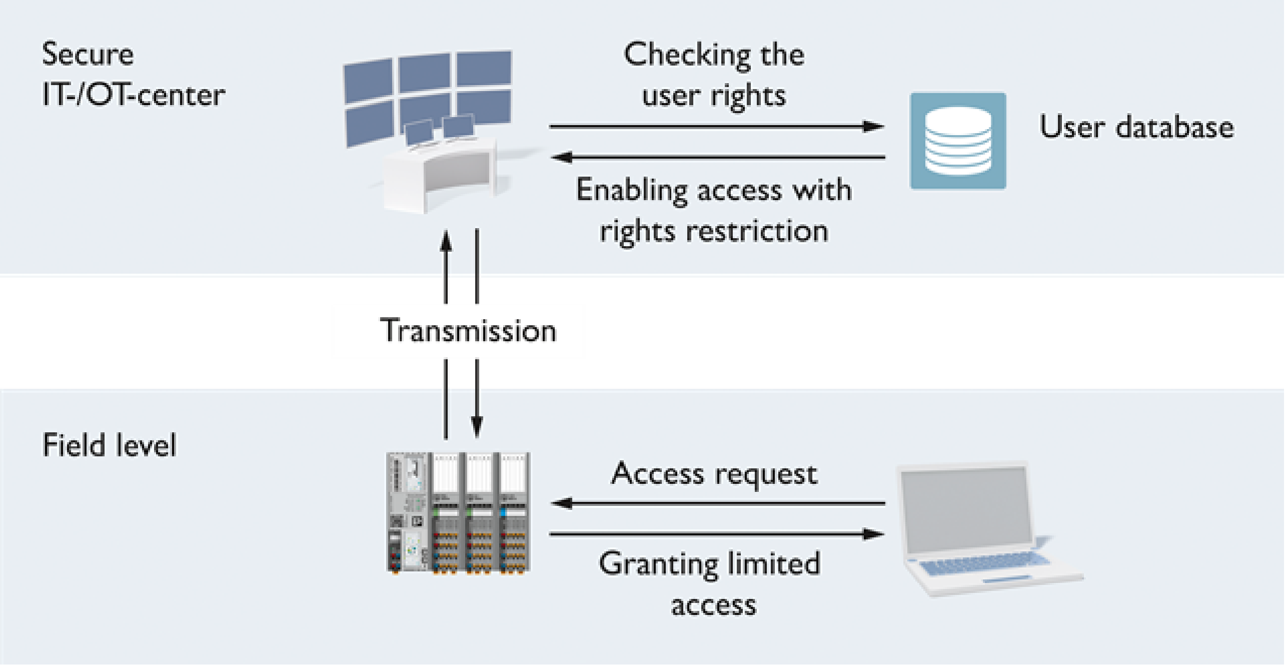
Required: password protection of devices in the ICS network

Password protection is necessary when logging on to both devices and applications in your ICS:

- Logon to the network-capable devices with a particular user role ensures that the user is known and authorized to access/control/configure the device.
  Example: When logging on to a PLCnext Technology controller from PLCnext Engineer to write a project, debug the application or control the PLC, you must enter a user role and password.
- When launching a server application from a client, a login page must be called first.
  Example: When launching an HMI application running on the internal HMI webserver of a PLCnext Technology controller from any HMI client (e.g. web browser on any computer), a login page should request authentication.

Why using a central user account management?

This question can already be answered by one simple example: In ICS networks, group passwords are often used for user access. The collective password is therefore known to many users. However, when employees leave the company, passwords are not changed or access is not blocked and can be abused. To solve such problems, a central user management should be used in which individual access rights are assigned to each employee.



The IEC 62443 standard (part 4.2) requires that the components involved in an ICS should "provide the capability to support the management of all accounts". This means it should either provide the management of all accounts directly according to part 3-3 or should be able integrate into a higher-level user account management system.

Integration into a higher-level user management means that the evaluation of the user authentication is performed in the higher-level user management system but not in the component itself. Many Phoenix Contact devices support this integration.

For such remote authentication, special network protocols are available which are referred to as "dial-in user services". Examples are RADIUS or LDAP both of which are briefly described below.

General rules for user management systems and user accounts

- Every user management server (e.g. RADIUS, LDAP - see below) that evaluates user/login requests and subsequently grants or denies access to the network must be protected by suitable firewall services. A firewall used there should only allow valid dial-in requests to pass.
- Strictly separate and distinguish highly privileged (e.g. overall domain administrator), privileged (server/ workstation administrator) and non-privileged (normal daily work) accounts.
- Reduce the number of privileged accounts to the minimum necessary.
- If there are multiple administrators, each should have their own privileged user account, if possible. Otherwise, the responsibility or accountability is not always clearly assignable.
- Even for the same person, administrative tasks and "day-to-day" operations should be under separate accounts. Follow the two-user rule to ensure security over convenience.
- The IEC 62443 standard explicitly allows role-based and group-based identification and authentication. However, avoid group accounts as much as possible and use individual accounts instead wherever possible. If a group of users use the same account, correct and unique identification is not possible.
- Make sure that (access) rights are restricted to the maximum possible extend for each user account. Refer to the topic Least privilege concept.
- Only administrators should be authorized to modify the user data bases or access right configurations. Other user must only have read-only permission to this data.
- Delete temporary and outdated user accounts (which were, for example, been used during the design or commissioning phase of the plant/ICS).
- Delete accounts that are no longer used.
- Implement user identification and authentication in a way that does not impede rapid, local emergency response.
- If supported, implement multifactor authentication.
  According to the IEC 62443 standard, ICS network components should implement multifactor authentication for all human users who will have access. For implementing multifactor authentication, several authentication methods can be combined. Combine the request of the user password with, for example, the evaluation of biometrics (e.g. finger print scanner, face recognition), tokens, physical keys, key cards or the geographic location of the user.

Note: Central user management with username/password implies that the same credentials can be used to access other systems, probably even IT systems. Therefore, both the user/application interface and the communication channel between the device/application and the central user management system should be implemented via secure network connections and/or strong encryption. For further information, see Secure Communication by Encryption and Authentication.

RADIUS

RADIUS is a mechanism which allows network devices to authenticate users. It is less complex as, for example, Active Directory with LDAP as authentication mechanism (see next section). Therefore, it is particularly suitable when using devices that are not members of an Active Directory domain and which implement a simple authentication process.

Note: RADIUS is already an older protocol. In its documentation (RFC 2865, June 2000), the mechanism for hiding the user name and password is not considered state-of-the-art. Consequently, RADIUS cannot be considered strongly encrypted today. It should only be used for central authentication services if the communication can be additionally protected by other network security measures.
RADIUS can be used securely in conjunction with Extensible Authentication Protocol, such as EAP-TLS. EAP-TLS is a commonly deployed authentication protocol which uses X.509 certificates. RADIUS with EAP-TLS is often used in port security applications.

The RADIUS standard is based on a client-server-architecture. The client has to be available on the device which initiates the login and generates a corresponding request. This request is routed via the network to the RADIUS server via a Network Access Server (NAS) which is also referred to as Authenticator. The server is connected to a user database where each user is registered with a unique name, password and the assigned user access rights. The user database can be a RADIUS internal one or the server queries other directory services or databases.

The login request is evaluated (username and password or security token value correct?) and, if the authentication was successful, the server initiates the establishment of the requested connection using all parameters belonging to the user. These user data also include authorization information which define the access rights to resources, services and data in the network. This means, RADIUS supports both authentication and authorization.

Active Directory and Lightweight Directory Access Protocol (LDAP)

Active Directory (AD) is a directory service in Windows®-based networks and part of the Windows® Server operating system. The term "directory" in this context is not an equivalent to a folder in a file system, but rather corresponds to a register. It stores devices, users, resources and other relevant objects where each contained object is described by specific information (object type, class, attributes).
This way, AD allows the detailed modelling of organization structures or, if suitable, of your plant. The structure may contain several hierarchically structured domains. Each contained object can be uniquely identified. The Active Directory service supports the search for objects, e.g., devices, users etc.

AD allows the management of administrable resources such as network services, access rights to memory space, use rights for applications, access to peripheral devices or network printers and network services. In terms of cyber security, the administrator of the AD must authorize or can restrict each user from using individual services, network devices/resources or objects.

For that purpose, Active Directory implements the LDAP which is described in the following. (LDAP is one of four main components of AD).

Lightweight Directory Access Protocol (LDAP) is an authentication mechanisms implemented in AD (besides other ones like, for example, Kerberos). From a technical point of view, LDAP is a network protocol that enables queries and changes in a decentralized directory service. This means the directory may be distributed over several servers/ computers. Each system involved must allow to communicate via a particular port (636 for TLS communication).

Note: LDAP should not be used without TLS protection as otherwise credentials (username, password) will be transmitted in unencrypted text.

Note: LDAP support is not only available in MS Active Directory. Various other software systems also implement an LDAP server, for example, Apache Directory Server, Novell (eDirectory), Sun (Sun Java System Directory Server) and many others. Furthermore, several different LDAP clients are available from various manufacturers.

In AD, the LDAP directory provides the information about users, computers and their group membership and it stores the certificates of the particular computer.

The directory is structured hierarchically below a fixed root directory which corresponds to the directory name. The hierarchy schema below the root must follow strict rules and can reflect your organization as it may contain countries, locations, departments, resources (servers, printers, services etc.) and persons. The LDAP data model defines for each directory service entry (i.e., for each object) a list of attributes such as Common Name (CN), localityName (L), User ID (UID) and more. They form the Distinguished Name which is the unique object identifier.

This way, the **LDAP server enables central management** of the users in a network. Or, to put it another way, user authentication can be connected to an LDAP server. It allows to manage user accounts, their passwords and group memberships at a central level. With an LDAP server there is no need to setup user accounts and passwords on every single controller.

The benefits are:

- If a password change is necessary, it only needs to be changed once inside the LDAP directory and not in every component.
- New users can be added without the need of configuring every component.
- New user rights and permissions can be granted and distributed in a very simple way.
- A blocked user is blocked in the whole system and not only for a single component.

Further Information: Refer to the main **PLCnext Technology - Info Center** where the file-based configuration of an LDAP connection is described.

Passwords

Each (human) user of a system component needs to be identified and authenticated for all access. For that purpose, passwords can be used. Further authentication methods can be, for example, biometrics (e.g. finger print scanner, face recognition), tokens, physical keys, key cards or evaluating the geographic location of the user.

> **Note:** According to the IEC 62443 standard, ICS network components should implement multifactor authentication for all human users who will have access. For implementing multifactor authentication, several authentication methods can be combined.

You must set up a User and Role Management accordingly. There, authorizations are granted to each user role which define the access type and permitted operations to system components or data.

Password rules

Definition of a password policy

A policy which rules the definition and handling of passwords should be defined and implemented for your ICS. This policy should fulfill the following requirements:

- Users are forced to define strong passwords by technically preventing the definition of weak passwords. Strong passwords result from their complexity: a combination of upper and lower case letters, numbers and special characters and a minimum length should be mandatory.
  Especially with regard to **brute force attacks**, the length of a password is decisive. (Brute force attacks refer to the software-supported "finding out" of a password by trying out all possible combinations of letters and digits.)
  Example: A password consisting of, for example, 7 lowercase letters corresponds to 26^7 possible combinations. A powerful software tool may determine such a password within only a few seconds. By using all uppercase and lowercase letters plus digits and special characters and extending the password by one character to 8, the same attack needs up to a day. When using 15 characters, a "successful" attack may take years.
- Passwords should have a time-limited validity, i.e. they must expire after a reasonable period of time. Before a password expires, the affected user must be prompted to change the password. At this point, the change algorithm should not accept the same password again.
- The number of incorrect password entries can be limited. If the defined value of goodwill logins is exceeded in such a scenario, the user can be blocked and must contact the administrator.

> **Note:** This measure may not be suitable for all ICS types. Blocking after a brute-force attack would prevent the user from logging on (even in an emergency case where a quick reaction is necessary).

Handling of default user names/passwords

- If possible, delete or at least deactivate (factory-set) default users/passwords from any component involved. If not deletable, change preset passwords to secure passwords which comply to your above mentioned password policy.

Note: Prior to modifying, deleting or deactivating default user names/passwords, make sure that the plant is still operable/controllable afterwards.

Note: Never transmit passwords unencrypted (see topic User Management for details). Even without central user management, users tend to use the same password for multiple applications. As a result, a compromised password could have security consequences in multiple systems.

Note: Passwords are usually stored "self-encrypting" on systems and servers, so they cannot be decrypted, but only disclosed through systematic guesswork or brute force. Also read the remarks in section Pre-shared Keys (PSK).

Use cases

Practical use cases for authentication using passwords

- Password protection of PCs with ICS-related software tools
- Password protection of devices in the ICS network
- Restricted mobile access: protecting a WLAN by password

Secure communication by encryption and authentication

Main goals: integrity and authentication

The implementations described in this chapter serve to pursue two main objectives of security engineering: to achieve data integrity and to authenticate users and data sources.

- **Integrity**: is the data unchanged?

  Checksums indicate the integrity of data thus allowing tamper detection. By verifying checksums, manipulations and data corruption can be detected.

- **Authentication**: where does the data come from/go to or who accesses the system/data?

  In communication networks, certificates can be used for authentication purposes. Here, private and public key pairs are relevant.

  By requesting a user role and password, users can be authenticated. Since each user has been granted authorization for certain operations and accesses (in the central user management), access to both data and system components (e.g. network-capable devices such as a controller) can be restricted.

  Furthermore, signing certificates with a private key can be used for distributing data (e.g., releasing libraries). The resulting signature is used to verify both the integrity and the authenticity of the released data.

Secure communication

Communication connections between participants in your ICS must be secured. Participants can be, for example:

- Server or client applications, such OPC UA, HMI, etc.
- Engineering tools, such as PLCnext Engineer
- Devices used to build automation infrastructures and systems, such as PLCnext Technology controllers, switches, etc.

For protection purposes, certificates can be used for authentication of such connections.

To secure the communication between devices and applications, certificates must be provided (installed) on these devices or in the applications.

When establishing a communication connection between two communication partners, both have to provide authentication to each other by means of their certificate which exclusively belongs to the particular participant. The respective other participant then verifies the validity of this certificate.

In many cases, only the server authenticates itself with its certificate (HTTPS, LDAPS etc.), so the client can be sure that the data provided for login (username, password) cannot be intercepted. Mutual authentication via client certificate eliminates the risk of password disclosure.

This authentication allows the establishment of a secure channel (within one so-called security domain) and the connection is only established if the certificate is valid. If the authentication fails, no secure communication connection can be established.

By securing a communication connection this way, also potential man in the middle attacks between the participants can be recognized.

Example: PLCnext Technology controller

When establishing a communication connection between a PLCnext Technology controller and PLCnext Engineer, the controller has to provide authentication to PLCnext Engineer by means of this certificate which exclusively belongs to this particular device. PLCnext Engineer then verifies the validity of this certificate.
The user authenticates himself to the controller with a user role and password: He has to log on to the controller via the engineering tool when initiating the connection between PLCnext Technology controller and PLCnext Engineer. The authorizations (permitted operations and data accesses) for each user role are stored in the controller.

If such a man in the middle attack is detected between PLCnext Engineer and a connected PLCnext Technology controller, you have the choice to stop the connection or to continue if the communication breach is intended and needed to support the chosen network architecture.

Owner-specific certificate instead of Phoenix Contact certificate

Some devices may come with a preinstalled manufacturer-defined certificate.
PLCnext Technology controllers by Phoenix Contact are equipped with a manufacturer-defined certificate issued by Phoenix Contact (in accordance with the IEEE 802.1AR standard).

This manufacturer-defined device certificate should be replaced in the device by an owner-specific device certificate which can be configured and issued by the device owner (Certification Authority). Installing an own certificate increases the degree of security as the device is "customized". The replacement ensures that your automation system can only be controlled by your software tools (e.g. your particular PLCnext Engineer instance).

After implementing an owner-specific device certificate in a device (or a hierarchical certification structure), the relevant certificate(s) (at least the root certificate) must be provided to the potential communication partners to enable it to validate the controller as trusted device.
Example: PLCnext Engineer must be adapted accordingly after installing an owner-specific device certificate on a PLCnext Technology controller. You have to deposit the corresponding certificate for validating the customer-specific controller certificate in PLCnext Engineer.

Note: If you have implemented a **hierarchical certification structure** in your application, at least the Trusted Anchor (root certificate) of the certificate path must be provided to the communication partners. Based on the Trusted Anchor, it will then be able to validate the entire certification path including all Issuer Certificates.
Installing only the Trusted Anchor (but not the Issuer Certificates of the path) avoids unnecessary subsequent installations for the communication partners when modifying the certification hierarchy of the device certificate (for example, by inserting or replacing any Issuer Certificate (signed by a sub-CA).
Refer to the topic "Certificates" for details.

Available measures

Possible measures and technical means are described in the following topics:

- Passwords
- Checksums and signatures
- Pre-shared keys
- Certificates

Implementations

- VPN
- TLS/HTTPS

Checksums and signatures

Checksums

Checksums indicate the integrity of data thus allowing **(accidental) modification detection**. By verifying checksums, manipulations and data corruption can be detected.

Checksums are calculated over valid, verified and non-corrupted data. When calculating the checksum again with the same algorithm (e.g., after a data transmission) the same checksum must result if the data is unaltered.

While checksums like CRC-32 are designed to detect simple communication errors, cryptographic checksums are designed to detect changes in large data sets. Such cryptographic checksums are called "hashes". Examples are SHAs (Secure Hash Algorithms).

A different checksum indicates that the data has been changed, for example due to manipulations, transmission errors, or memory errors (hardware failures).
Such a checksum comparison can be performed, among others, to verify the integrity of ...

- data loaded from the Internet (e.g., manufacturer's download portal) or via ftp. This also includes libraries, software/firmware patches, and setup files for Windows® application.
- data received as attachment via email (e.g. a library sent by colleagues).
- the integrity of software installations.

Signatures

A signature signs a hash which allows to verify the authenticity of the origin of data.

After calculating the checksum over a set of data, the hash can than be signed using a private key. The correctness and authenticity can then be verified at any time using the respective public key/certificate.

Example: When releasing a library in PLCnext Engineer, the engineering tool calculates checksums over the contained components which are then used as signature. If the library is later included in a project, the signature is verified each time the project is loaded. This way, any modifications (e.g., new version) or data corruptions are recognized.

Use case: integrity check of downloaded setup/firmware file

To comply with the IEC 62443 standard, the tamper protection of downloaded setup/firmware files is mandatory.

After downloading a setup file for any Windows® application or a firmware file for a controller from the Internet and prior to its installation, you must verify that the downloaded setup/firmware file has not been corrupted/tampered. To do this, you need to find out and write down the checksum of the download file from the provider before downloading it. After downloading the setup file, use a suitable tool to calculate a SHA256 checksum over the downloaded file. Only if the checksum you determine is identical to the providers's specification should you install the software.

Use case: integrity check of software installations

When installing software tools that have been developed according to the IEC 62443 standard, checksums are calculated over the installation.

By verifying these checksums, manipulations of the installation and data corruption can be detected.

To comply with the IEC 62443 standard, you must continuously check the integrity of relevant software installations. For that purpose, use primarily a **standard Windows® tool**. Alternatively, you can use the ChecksumCalculator tool provided by Phoenix Contact or any other suitable tool.

Further Information: Phoenix Contact supports this, for example, for PLCnext Engineer. Refer to the PLCnext Technology Security documentation for details.

Certificates

What are certificates used for?

Certificates can be used for the following:

- Securing communication connections between participants in your ICS. Participants can be, for example:
  - Devices used to build automation infrastructures and systems (such as PLCnext Technology controllers, switches, etc.).
  - Server and client applications (such as HMI application, OPC UA etc.).
  - Engineering or configuration tools connecting to the devices to be configured (such as PLCnext Engineer etc.).
    During a logon to a device, the identity of both the engineering software instance used to logon and the device must be verified and they must match. This can be done by means of certificates.
    Example: When logging on to a PLCnext Technology controller from the software PLCnext Engineer, both parties must authenticate themselves using a certificate. A secured connection is only established, if the certificates are valid.

  Refer to the topic Secure Communication for details.

- Verifying the integrity and origin/authorship of data, such as a provided library, or the authenticity of software/firmware.
  When creating the data (for example, releasing the library), a signature certificate (file) as well as the relating issuer certificates and the corresponding private key (signature key) are required. The private key is used for generating the signature in the inventory of the data to be published. As a result, this inventory signature then contains the signature certificate including the relating issuer certificates and can be used to prove the integrity of the library and the authorship of the data releaser (library supplier in our example).

What is a certificate?

A certificate is an electronic, digitally signed and forgery-proofed identity document (data structure).

A certificate...

- is specifically created and only valid for the particular owner.
  The owner of a certificate is referred to as **subject**. This could be, for example, a server or a client application instance.
  The creator of a certificate is referred to as **issuer**.
- describes the capabilities the subject has.
  For example, the certificate can only be used for authentication purposes, or a subject may become an issuer and act as CA.
- contains (quotes) the public key of the subject which exclusively belongs to the private key of the subject.
- is signed by the issuer with a signature. For creating the signature, the issuer has used its private key. The signature attests that the public key belongs to the subject.
  See the section "CA-signed certificates vs. self-signed certificates" below for details.
- does **not** contain the private key of the subject.

Authentication using certificates

- A subject (application) can authenticate its identity to other applications by means of its certificate in combination with its private key.
- The recipient of the certificate verifies the signature of the certificate (and thus the identity of its owner) with the public key of the issuer.
- The verification is done as challenge response authentication procedure. For example, the subject is asked to sign a random number with its private key. The signature is then verified with the public key.

Following the mutual verification of applications, a secure communication channel between the authenticated applications can be established.

Certificates do not contain encrypted content but plain text. Due to their signature, they do not need to be protected. Therefore, they can be distributed (to involved applications/administrators), for example, by email.

CA-signed certificates vs. self-signed certificates

A Certificate Authority (CA) is an administrator, organization or application that issues certificates, i.e, that creates certificates for other subjects and signs them using the private key of the CA. Subject (owner) and issuer (creator) in this certificate are not identical. The issuing CA writes the public key of the subject for which the certificate is going to be created into the certificate, instead of its own public key when "self-signing".

A self-signed certificate results, if an application creates its own certificate and signs it with its own private key. In a self-signed certificate, the subject (owner) and issuer (creator) are identical. For securing the communication between a small number of applications, the use of self-signed certificates may be practicable. Since there is no common trust basis in such a scenario, each application involved must be manually configured for each relevant self-signed certificate.
To secure the communication in large distributed networks with many applications, certificates issued by a Certificate Authority (CA) are recommended. This is because using the CA certificate(s) as a common trust anchor makes management much more scalable. Also hierarchical certification structures are possible with one or several issuers and sub-issuer levels.

Note: For the communication between PLCnext Control and PLCnext Engineer, no self-signed certificates can be used.

Certificate Signing Request (CSR)

A Certificate Authority (CA) generates and signs a certificate only on request. This request is called Certificate Signing Request (CSR). With the CSR, the CA receives detailed information on the subject that requests the certificate (subject/owner attributes) as well as the subject's public key in order to include these data in the certificate.

Certification hierarchy, certification path, and trusted anchor

When a CA issues a certificate for a particular subject it has to define the future capabilities of the subject. Possibly, the certificate can only be used for authentication purposes, or (by granting further capabilities) a subject may become an issuer and is also able to issue certificates for other subjects. This way, a hierarchical certification structure can be created.

In a hierarchical certification structure, the CA is considered as **root node**. The CA certificate (root certificate) is called Trusted Anchor. In the next lower level, further issuers (sub-CAs) can follow, each of them with the right to issue certificates. Their own certificates are called issuer certificates. Further sublevels with subsub-CAs are possible. The certificates on application level (e.g., controller and PLCnext Engineer, or OPC UA server and clients) are called application certificates.

In a hierarchical certification structure, a certificate (for example the device certificate of a PLCnext Technology controller, or the application certificate of an OPC UA client) can only be verified by authenticating the entire **certification path** from the particular certificate up to the Trusted Anchor (root certificate).

Example: PLCnext Technology controller and PLCnext Engineer

For the communication between PLCnext Technology controller and PLCnext Engineer, this is done by

- installing the entire certification path in the PLCnext Technology controller starting with the controller certificate via all issuer certificates involved up to and including the Trusted Anchor (root certificate).
  and
- providing the certificate for validating the Trusted Anchor in PLCnext Engineer.

> **Note:** Installing only the Trusted Anchor avoids unnecessary subsequent installations in PLCnext Engineer when modifying the certification hierarchy of the device certificate (for example, by inserting or replacing any issuer certificate (generated by a sub-CA).

Certificate Revocation List (CRL)

A Certificate Revocation List (CRL) is a list which describes the invalidity of certificates. A CRL specifies certificates that must not be accepted by application instances or devices. A certificate can be revoked if the relating private key (which is the property of the certificate subject) has been compromised or if the certificate contains content that is no longer valid (e.g. an outdated application instance URI after migrating the application to another computer).

CRLs can be created by any issuers (CA or sub-CA) which are endowed with the rights for issuing CRLs ("Sign CRL"). To revoke a certificate, the CA adds the respective serial number of the certificate (and potentially more) to the CRL. To secure the CRL, it is also signed by the CA using the private key of the CA and it contains a time stamp. This way, applications can verify the authenticity, integrity and validity of a CRL before evaluating its content.

Because usually authentication only happens during connection establishment, an application instance only evaluates the CRL each time when authenticating a certificate.

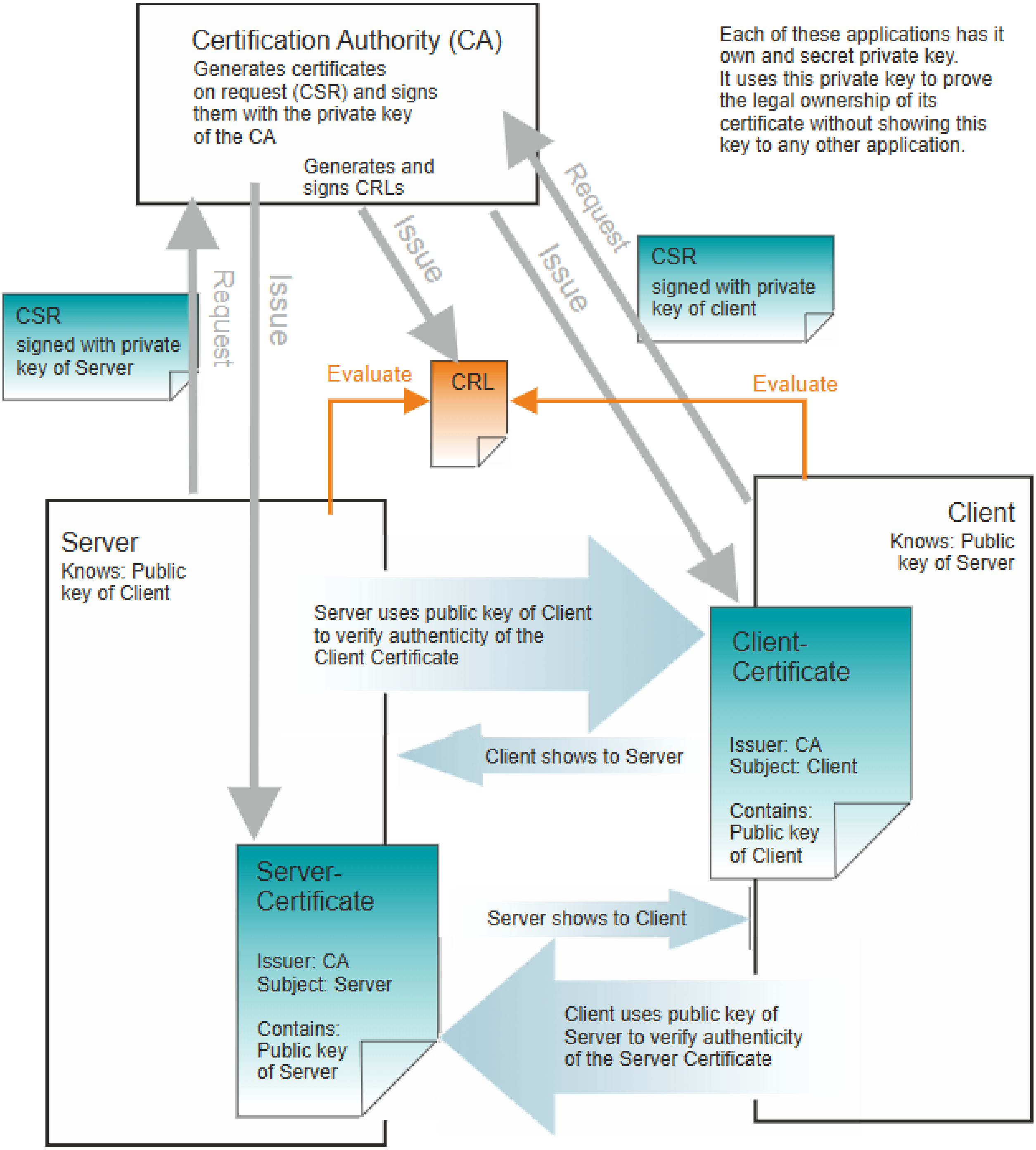
Consequently, existing connections are **not** disconnected if a certificate, which was used during connection establishment is revoked later. Such connections must be disconnected manually, for example, after a private key has been compromised or stolen. The disconnection may also be done by restarting the affected devices or application instances.

Example illustration

A CA has issued certificates for a server and a client application on request. This represents a two-level certification hierarchy.

Mutual authentication: To authenticate their identities, each application verifies the certificate of the other application using the public key of the other application. Following the successful authentication, a secure communication channel can be established.

The CA has additionally issued a CRL. The application can use this CRL during authentication to ensure that a certificate that to be authenticated is not revoked. Communication is only established if the involved certificate is not listed in the CRL.


Certification Authority (CA)
Generates certificates on request (CSR) and signs them with the private key of the CA
Generates and signs CRLs
Each of these applications has it own and secret private key. It uses this private key to prove the legal ownership of its certificate without showing this key to any other application.
Request
Issue
Issue
Request
Issue
CSR signed with private key of Server
CSR signed with private key of client
Evaluate
CRL
Evaluate
Client
Knows: Public key of Server
Server
Knows: Public key of Client
Server uses public key of Client to verify authenticity of the Client Certificate
Client-Certificate
Issuer: CA
Subject: Client
Contains: Public key of Client
Client shows to Server
Server-Certificate
Issuer: CA
Subject: Server
Contains: Public key of Server
Server shows to Client
Client uses public key of Server to verify authenticity of the Server Certificate

Secure certificate management

Trusted networks may have a large number of certificates in use. To maintain smooth and secure communication, each of these certificates must be checked for the following aspects.

- Are all certificates valid, i.e. compliant with the directive? If not, this certificate should be checked and revoked if necessary, for example, by listing it on a Certificate Revocation List (CRL).
- Has the expiration date been exceeded for a certificate? If yes, this certificate must be extended or replaced.
- Have certificates been revoked/blocked? See Certificate Revocation List (CRL) above.
- Are there legitimate certificate signing requests from participants in the network? If so, new certificates must be issued by the CA. See Certificate Signing Request (CSR)
- Does an endpoint (application/device) report a certificate error?

Expired, forgotten or invalid certificates in most cases lead to security problems, communication or even production downtime. Therefore, a secure certificate management is essential. As certificates contain public keys, such management is also referred to as Public Key Infrastructure (PKI).

If possible, use an automated certificate management system (or PKI) that covers the following tasks or contains the following components:

- Certificates search tool: The automatic search in the network should produce a clear log of all the certificates found. All details of each certificate should be listed, such as subject (owner) and expiration date etc.
- Adding (client) certificates to the trust list of the endpoints (devices or applications) involved. This should be able to be done automatically if possible, possibly with subsequent manual confirmation. If possible, running processes or services should be able to continue running.
- Ability to schedule: all tasks should be regular and at appropriate time intervals (e.g., several times per week).
- Define clear personnel responsibilities and unambiguous authorizations for certificate/PKI management.
- Administrators and users of the management system must be trained according to their roles.
- The certificate/PKI management system should have a notification function that informs about all events and necessary action steps. This includes detected (soon to be) expired certificates, certificate errors in endpoints, pending signing requests etc.
- Approve Certificate Signing Request (CSR) as soon as possible.
- Ensure that no outdated keys or other obsolete technologies are used when issuing certificates.
- Permit/enable the automatic extension of the validity period provided that the performed threat risk assessment allows it.
- Fix certificate errors on endpoints as soon as possible.
- Maintain a Certificate Revocation List (CRL) and evaluate it continuously.

Keys: PSK, private/public

This topic introduces basic knowledge on keys.

Pre-shared Keys (PSK)

Pre-shared keys (PSKs) can be used for authentication purposes. When establishing, for example, a VPN or WLAN connection, the PSK is used for exchanging the (symmetric) session key between the applications involved.
PSKs can also be used for symmetric encryption, where one individual key is used for encrypting and decrypting data.

In both cases, for authentication and symmetric encryption, the same key is used on both communication end points. Therefore, the key must be available for all participants before the authentication or encryption/decryption - it must be pre-shared.

With this symmetric method, only one key needs to be distributed (in contrast to the asymmetric encryption with private and public keys - see below). However, it requires a secure distribution medium, because anyone in possession of the PSK can authenticate themselves or decrypt data. For this reason, all peers involved must protect the PSK accordingly. The key must not be disclosed even if a participant is compromised. Consequently, if the PSK becomes accessible to an unauthorized person, it must be modified, redistributed to all authorized participants, and set up accordingly.

> **Note:** While passwords are typically stored "self-encrypted", PSKs are stored in plain text in all systems involved. Therefore the risk of being compromised is significant. Whenever possible, public key methods should be used (see section below).

Typical application area for PSKs are those, where the key exchange is possible because the participants are known. Examples are WLAN networks, VPNs, or IoT connections.

To prevent brute-force attacks, PSKs should be suitable long combination of characters, numbers and special characters ("brute force" designates a method which tries to determine keys or passwords by automated and random trial and error).

Private and public key

Asymmetric cryptography is based on individual key pairs. Each communication party possesses its own unique private key which belongs to exactly one public key as counter part.

- Using its **private** key, a party can sign data (for example, a certificate). The signing party is referred to as signer (also referred to as "issuer" within CA-signed certificates).

  When realizing data integrity by data encryption/decryption, the receiver of encrypted data uses its private key to decrypt the data which where encrypted before by the sender of the data using the related public key.

  Private keys may be protected by special, security-related hardware like a TPM (Trusted Platform Module) or Smartcard/Integrated Circuit Card(ICC) which provides enhanced security functions thus ensuring the integrity of a hardware/operating system. Protected this way, private keys can provide a very high security level.

- Using the relating **public** key of the signer (which exclusively belongs to the private key), this signature can be verified by other parties.

  For encrypting data, a public key can be used. To decrypt this data, the related private key is required.

The private key must be kept secret by the party. The public key can be distributed in a certificate. By giving the certificate (with the contained public key) to other parties, these recipients are enabled to verify the identity of the subject.
See topic Certificates for details.

Protection of project data on the hard disk and during transfer

Engineering and parameterization tools (e.g. PLCnext Engineer) often store plain, i.e., unencrypted project data on the harddisk of your computer. The data is therefore unprotected against tampering and theft.

Use a suitable encryption method:

- to protect project data, archives, and libraries, etc. on your computer.
- to protect the transmission of project data, for example, by email.
- to authenticate the origin and authorship of transmitted project data with the recipient.

Suitable methods can be provided by encryption and signing tools according to the OpenPGP standard as defined by RFC 4880 (such as PGP, or GnuPG). For encrypting project data on your hard disk, for example, FDE (Full Disk Encryption) tools, such as BitLocker can be used. WinZip archives with password can help protect project files/archives or released libraries.

Note: The methods described here for encryption should be supplemented by the general protective and hardening measures for PCs.

Recommendation: encryption on the entire data path

- Encrypt data on each storage medium (local disks, your network, in the cloud, portable storage media).
- Only transfer encrypted projects parts or libraries, for example, by email.
  Suitable Tools (e.g., PGP) enable both the encryption as well as signing of emails: Encryption prevents the unauthorized reading of the mail content while the signature is used to verify the integrity and the authenticity of the mail.
- Transferred data should remain encrypted on its entire way from the sender to the receiver. This includes that the sent data are stored encrypted at the target system as well after the transmission.

VPN

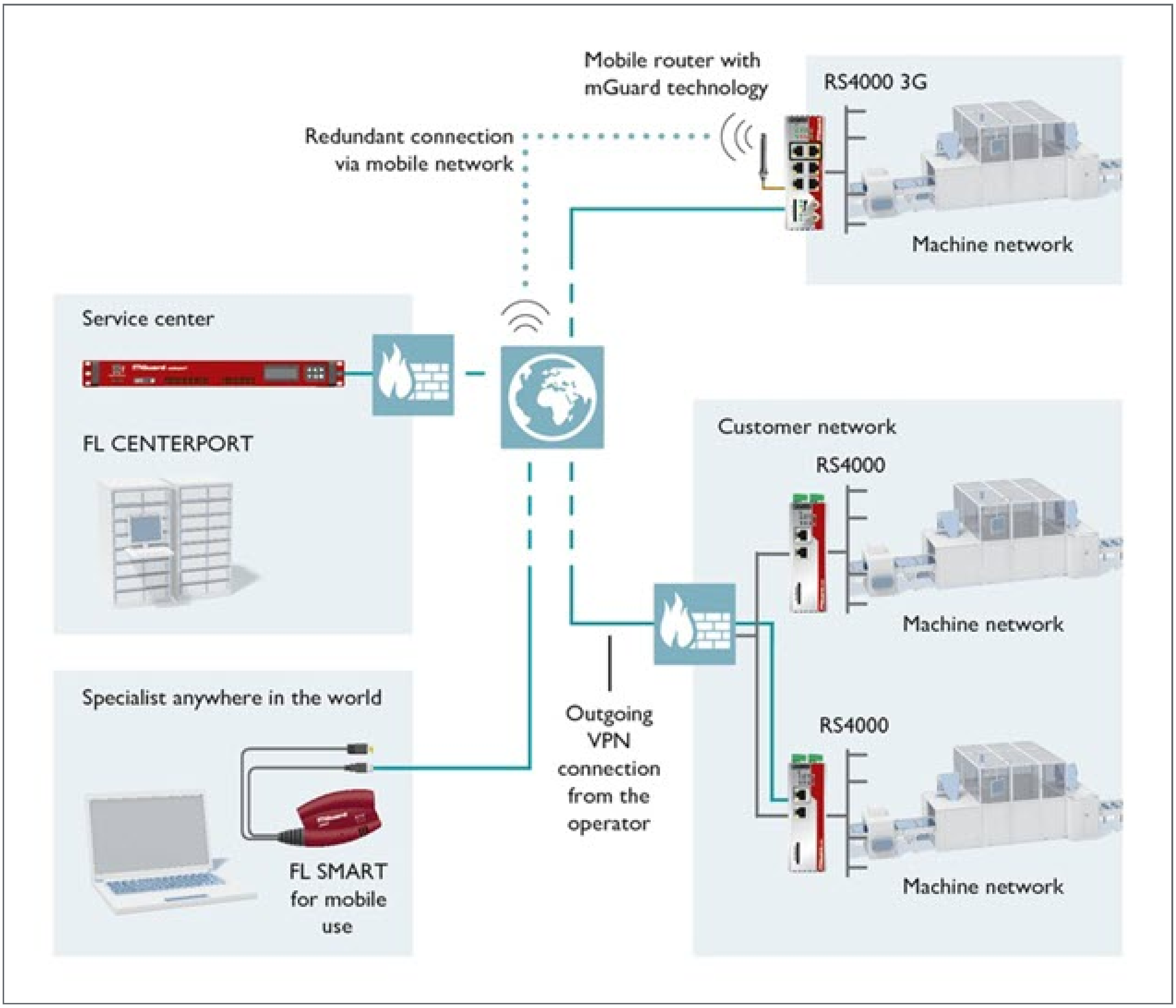
Via open Internet connections, criminals can copy data or make changes to the system. Using firewalls, the access to automation systems from the external networks can be restricted to authorized connections. In addition, remote connections via the Internet should always be encrypted, for example via a virtual private network (VPN).

VPNs are a protective measure to prevent unauthorized access to your network, e.g. for remote maintenance access. Protocols used to establish a VPN do not only secure against interception or eavesdropping, but also contain mechanisms to protect against manipulation.

For securing networks via VPN, Phoenix Contact offers the mGuard product line as a security appliance. Other products (e.g., PLCnext Technology controller) may also come with built-in VPN support. Refer to the current Phoenix Contact product catalog (phoenixcontact.net/products).

Note: The establishment of (encrypted) VPN connections directly to, for example, a remote maintainer must be viewed particularly critically, since there is no control over the actions performed via the VPN connection.

Note: VPN connections established using proven protocols established in the market and mutual certificate authentication can be considered as cryptographically strong connections. For further details please refer to the respective product documentation.


Mobile router with mGuard technology
RS4000 3G
Redundant connection via mobile network
Machine network
Service center
FL CENTERPORT
Customer network
RS4000
Machine network
Specialist anywhere in the world
Outgoing VPN connection from the operator
RS4000
FL SMART for mobile use
Machine network

TLS / HTTP(S)

To secure the transmission of data between network devices used to build automation infrastructures and systems (such as controllers), or between an engineering software and devices which you configure and commission via this software, you should use security-capable transmission wherever they are supported. Such protocols are, for example:

- TLS (Transport Layer Security): encryption protocol which secures the Internet data transfer. With Phoenix Contact products, the communication between the engineering software PLCnext Engineer and the firmware of PLCnext Technology controllers is handled using TLS.

  TLS is often called SSL (Secure Sockets Layer). SSL is the predecessor of TLS whose latest released version was 3.0. After this version SSL was further developed and released under the name TLS. Known implementations of the TLS/SSL protocol are OpenSSL and GnuTLS.

  > **Note:** To increase the network performance, some New Generation Firewalls (NGFWs) allow the deactivation of the SSL/TLS inspection. Nowadays, the proportion of encrypted data used to infiltrate networks is significantly greater than the proportion of unencrypted attacks. Therefore, this deactivation results in a limitation of the security function as it may allow unauthorized data traffic to pass.

- HTTPS (Hypertext Transfer Protocol Secure) is the secure version of network protocol standard HTTP. HTTPS is supported by TLS (SSL) which establishes an encrypted connection between two communication partners, authenticates the server and prevents manipulation of the transmitted data. It therefore ensures a tap-proof connection.
  Identification and authentication take place before the data is sent via HTTPS. For that purpose, a symmetrical key is exchanged in a handshake process. With this key, the data is encrypted by the sender and, after transmission, decrypted by the receiver. An SSL certificate from a public CA is only issued if the server and the domain can be uniquely identified. For this reason, certification authorities require the address data and verify the actual ownership of the domain.

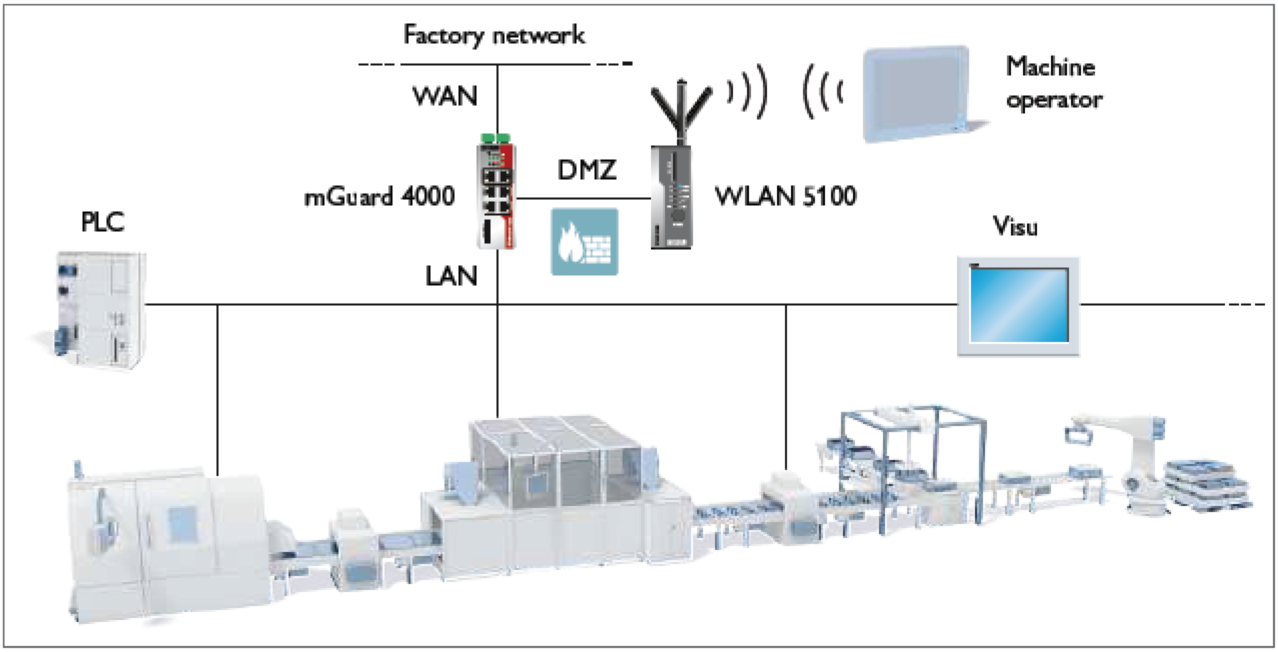
  Use secure access paths such as HTTPS or VPN for remote access.

  > **Note:** Data transmission with HTTPS protects data only during transmission, but data not protected after the transmission is completed on the receiving end. For complete protection, you should use end-to-end encryption or re-encrypt received data immediately after transmission. Never store plain data.

Restricted mobile access: protecting a WLAN by password

Unauthorized smart devices must not be able to connect themselves via the WLAN interface. For that reason, your strict password rules should also apply to all wireless access points in your ICS.

WLAN components from Phoenix Contact enable automated key management by the machine control system. This means that secure WLAN machine access can be easily implemented in the form of one-time passwords. In addition, WLAN communication can be protected and isolated from the rest of the network using a demilitarized zone (DMZ). The following figure shows an example of a secure integration of mobile end devices with one-time passwords and DMZ.



Technical PC hardening measures

Any engineering tool, such as PLCnext Engineer, can manipulate devices or processes in your ICS. To reduce the risk of manipulation, perform security evaluations regularly.

PC-based hardening and organization measures

Protect any PCs used in automation solution environments against security-relevant manipulations. This can be facilitated, for example, by taking the following measures:

- Boot up your PC regularly, and only from data carriers that are secured against manipulation.
- Set up restrictive access rights for any personnel that absolutely must have authorization.
- Identification of each user on the PC must be mandatory. For this purpose, passwords can be used or multifactor authentication can be implemented.
  Passwords should be defined according to a password policy (strong and time-limited passwords). Furthermore, user roles and user authorization should be managed in a (Central) User Management system.
- Activate the BIOS password protection to prevent unauthorized modifications in the BIOS settings.
- Only allow necessary boot options (BIOS setting) to make sure that the PC only boots from media which are considered secure (e.g., internal hard disk). Deactivate all other boot media (USB sticks etc.)
- Deactivate the autorun option if not required for the operation.
- Encrypt your project data.
- Deactivate unused services.
- Uninstall any software that is not used.
- Use a suitable and up-to-date virus/malware detection software.
- Use a firewall to restrict access.
- Use whitelist tools to protect important directories and data against unauthorized changes.
- Activate security-relevant event logging in accordance with the security directive and the legal requirements on data protection.
- Activate the update feature in accordance with the security directive.
- Activate the automatic screen lock function and automatic logout after a specified time.
- Perform backups regularly.
- Only use data and software from approved sources.
- Do not follow any hyperlinks listed that are from unknown sources, such as emails.

Keep software up-to-date

- Always use the latest software version of all tools (e.g., PLCnext Engineer) installed as well as the latest operating system version on your PC.
- Check for any software updates available on the respective product page from Phoenix Contact: phoenixcontact.net/product/1046008
- Observe the Change Notes for the respective software version.
- Pay attention to the security advisories published on Phoenix Contact's Product Security Incident Response Team (PSIRT) website regarding any published vulnerabilities.

Password protection of PCs with ICS-related software tools

Implementation of a suitable user authentication on the Windows® PCs involved must ensure that each user is known and authorized to use your ICS-related tools, such as the engineering software PLCnext Engineer.

- Users must log-on to Windows® (standard login mechanism).
- Separate account per user (no "group login").
- Corporate policies regarding user administration, password rules, etc., must be defined.
- Logged-on Windows® user is allowed to launch and use the software.
- Standard Windows® login must be supplemented by **multifactor authentication** tool: verification of the user identity, e.g. via a mobile app (push notification, biometric recognition, etc.), via a PIN or finger print, hardware/software token, etc.
- A suitable and up-to-date virus/malware detection software must be used, and a firewall is activated and configured.

Logging and monitoring

Log and status data as feedback for security improvements

The early detection of security-relevant incidents as well of system errors and performance "bottlenecks" during operation or data transmission depends to a large extent on adequate logging and monitoring.
In particular, log data and status information from the various areas, zones (processes) and conduits of your plant provide important information for all activities relating to security. They form the basis for decisions regarding the status of protection or necessary adjustments or extensions to security measures and policies.

A central function should consolidate and evaluate log data and status information from the entire plant. The results of this evaluation should be incorporated into the permanent risk management system so that a changing threat situation can be identified as quickly as possible and appropriate countermeasures initiated.

The evaluation of the log files and status information should be performed at regular intervals. A corresponding message/report should be generated as soon as a previously defined threshold value for a specific event is exceeded.

Logging: recording of events

The following list shows the events that should be logged.

> **Note:** All logged events should be reported to suitable recipients which evaluate and further process this notification.

- Operating system/firmware events an all PCs/devices in the network. This includes boot processes, state changes, CPU load, memory consumption as well as detected hardware errors (such as defective storage media) etc.
- Execution of applications.
- Events on all network devices, such as firewalls, switches, routers etc.
  This includes, for example, the loss of network connections, traffic load, performance etc.
- Intrusion/tampering attempts (detected, for example, by an Intrusion Detection System): Systems and components should log any attempt of unauthorized access or tampering.
- Security-related log data should include the user name, date and time of any login to any component in your plant. If possible, also the commands executed by the user should be logged.

  Phoenix Contact provides security-related logging on the PLCnext Technology controller: The user, data and time of the login to the controller as well as the executed commands, state changes, etc. are logged for evaluation/ monitoring purposes.

> **Note:** Logging must comply with the applicable data protection guidelines.

Each log entry should be composed of the following information:

- When? Date and time of the event.

> **Note:** The time signal for synchronization should come from a trusted source. Time synchronization through a dedicated Network Time Protocol (NTP) service or via Precision Time Protocol (PTP, acc. to IEEE 1588) is recommended. NTP and PTP are a worldwide industrial standards which enable the time synchronization of computers and other IT/OT components via an IP network, i.e., the Internet.

- What? Description of what happened.
- Severity? How critical is the event in terms of security, system performance, maintenance of orderly operations??
- Who reports? Specification of the device/application reporting the event.

Monitoring the system state

- SNMP monitoring: System status information relating to, for example, the state of communication channels should be collected and evaluated (such as VPN up/down, number of users logged in, resource status etc.). Furthermore, e.g. traps sent (pushed) by an SNMP agent without being requested by the manager can be used for this purpose.
- The state of antivirus/malware protection (i.e. database version used) should be logged and reported

Data backup and restore

General considerations on data backups

Data loss may not be the result of careless or erroneous actions of authorized users or defects in storage media alone, but may also be the consequence of malicious deletion or encryption of your data by unauthorized intruders. The consequences of data loss are usually manifold and very expensive, possibly even existential: from production downtime/standstill of your plant to the loss of proprietary data and essential know-how.

Backup strategy

- A common backup practice is "3:2:1". This means: create a triple backup to two different media, one of which you keep offline in a secure place (protected against theft and fire).
- Perform backups regularly or event-triggered.
  The required interval for regular (scheduled) backups depends on the change intensity of the data: Data which are modified often (such as application development) should be backed up daily. Configuration or system data that is changed/updated less frequently can be backed up either at reasonable longer intervals or on an event-driven basis.
- Create full backups and incremental backups.
- Depending on the requirement for the availability of backups for restoring systems, daily backups, for example, can be kept locally (e.g., on additionally installed hard disks or immediately available SD cards), while long-term backups can be stored externally.
- The ongoing operation of a plant must not be impaired by the backup process. Depending on the situation in your plant, backups should possibly be created during a production shutdown (e.g. after commissioning and before the start of productive operation or during maintenance phases) so that ongoing production is not affected.
- A backup should be able to recover a system/plant to a known (i.e. clearly documented) secure state (of operation).

What data should be included in the backup?

A backup should include data on user level as well as on system level.

- Operating systems and firmware
- Device configuration/parameterization/control data.
- Security-related data such as keys and certificates.
- Application programs running on, e.g., controllers.
- Production data including e.g., recipe data bases.
- Logging and monitoring data including e.g., data logger sessions of event log data bases.
- Current security settings of the component/system.
  After a recovery, the security-related state must be clearly determinable/readable.

Integrity and verification of backups

- According to the IEC 62443 standard, backups are to be considered as "information at rest". As a consequence, their integrity and confidentiality should be protected in the same way as for your entire plant.
- Encrypt backups, if possible.
- Each Backup should contain characteristic data (such as checksums) which allow to verify the integrity of the stored data. You must be able to detect modifications that have been made to the data as well as defects of the backup storage media.
- For each device, you should document when a backup was created and what type it is (full/incremental). In addition, backups should be informative and clearly documented. This includes that for each backup the time of creation, the contained data status and, if applicable, the backed up device can be identified.

Storage of backup media with regard to confidentiality and availability

Backup data must also be protected, i.e. its confidentiality, integrity and availability should be ensured at all times. Therefore, the storage location for backup media must meet some requirements:

- Physical access to the backup media should be restricted and controlled accordingly. For example, a fireproof safe can be used, to which access is only permitted after appropriate authentication.
- Clear authorizations must be defined for accessing and restoring backups and enforced by means of organizational and technical measures.
- In case of emergency, access to the backups must be fast and guaranteed.
- Backup media must be permanently protected from external influences (moisture, heat, fire, etc.). Climatic conditions must also be suitable for long periods of storage.

Restoring backups

Prior to initiating a restore process of backed up data,...

- the integrity of the backup data must be verified.
- you have to make sure that the backup recover a known and secure state (of operation) of the system/plant.

After you have restored a backup, you should...

- determine the current security-related state of the component/system/plant.
- thoroughly test and verify the correct function as well as the safety-related and secure operation of the entire application.

Plant management

Making (physical) on-site access controllable

In addition to the remote access, the "physical access" on site must also be controlled and restricted if necessary. To prevent damage due to unauthorized access:

- Make sure that only authorized access is possible.
- Protect the interfaces by mounting the devices in a control cabinet.
- Secure the control cabinet with a lock.
- Ensure that the control cabinet key is only accessible to authorized persons.
- Run cables in such a way that they are not accessible for unauthorized persons.

Security patch management

Following the release process, usually patches are provided. Features and functionality patches increase or enhance the product's range of functions or improve the plant operation or reliability. Besides these well-known feature/ functionality patches, security patches are important.

Security patches fix known vulnerabilities in a system/an ICS. These vulnerabilities relate to software and hardware likewise. Often, they result from improperly programmed software or device firmware, or from an improper configuration/parameterization of integrated system components. Consequently, the elimination of these vulnerabilities is the responsibility of the manufacturer or the system integrator, respectively.

Security patches are an important element when it comes to maintaining the operational capability of a plant.

Therefore, a suitable security patch management process must be established and reviewed, accompanied by a notification/announcement mechanism, that informs, for example, the plant users about vulnerability as soon it has been detected.

The patch/update management process should be defined as follows:

- Regularly evaluate vulnerability reports for both your own software and third-party tools.
- Perform data backups for the affected components prior to installing a patch.
- Only distribute patches which have been tested and released by the manufacturer.
- Install patches and updates in your plant sequentially (component by component), if possible, and consider the consequences of possible system failures after installing a patch when planning the sequence.
- Define a fixed patch interval in particular for security-critical systems. It is recommended to contractually define time periods for releases with third party software vendors,
- If possible, adjust patch management to match the plant's production cycles.
- Define clear responsibilities with regard to patching software (own as well as third-party).
- Determine the criticality of patches and consider it in your schedule. If, for example, a patch is non-critical but its installation results in a system reboot (e.g., with a following downtime), it may be postponed.
- If the installation of a patch is not possible due to any circumstances, suitable alternative measures should be taken for the affected component, for example:
  - (Temporary) separation of the affected component into a separate zone/network segment.
  - (Temporary) filtering the data traffic to/from this component using a specifically configured firewall.

Note: If the support for a component or its software has been discontinued (end of life cycle), a new thread risk assessment is required for the entire system to evaluate the changed threat situation.

List of abbreviations

CA	Certification Authority
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DMZ	Demilitarized Zone
FR	Foundational Requirement
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control System
ISMS	Information Security Management System
IT	Information Technology
NAT	Network Address Translation
OT	Operational Technology
PAT	Port and Address Translation
PKI	Public Key Infrastructure
PSK	Pre-shared Key
SPLC	Left-alignable, safety-oriented control for operating PROFIsafe® devices
SPLCProxy	A layer that is providing security extensions, dedicated safety roles and file system access rights to protect the SPLC (see Security and safety hardening).
SR	System Requirements
TLS	Transport Layer Security
VPN	Virtual Private Network

PLCnext Security Guideline

PLCnext Security Guideline and security measures - an overview

To achieve security in an automation system, a holistic approach is necessary. An adequate security concept must be drawn up that covers technologies used, the defined processes, and the people involved. Both technological and organizational measures must be taken into account.

Many threats can be contained by appropriate technical measures, but must be supplemented by organizational measures involving personnel, procedures, policies, and practices.

For details, please refer to 360° Security - The Holistic Approach.

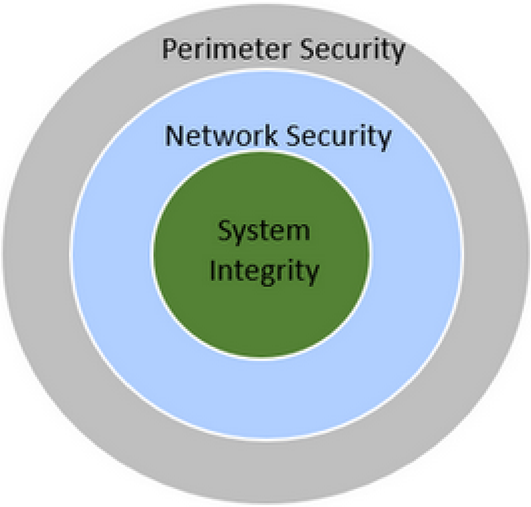
Technical automation solution measures are, for example:

- Network segmentation and architecture
- Firewall configuration, management of network segmentation, and device protection
- User management with Role-based Access Control (RBAC)
- Local and centralized (LDAP) user management configuration
- Transport Layer Security (TLS) for secure communication
- Certificate management for asymmetric cryptography and key management
- Local and centralized security logging
- Network-wide time synchronization
- Network-wide device and update management
- Secure configuration of the automation application
- Secure remote access via VPN (IPsec or OpenVPN)
- Local and centralized backup and restore

Generic security concept

Defense-in-depth design of automation systems is an important IEC 62443 process measure to achieve reliable security. The result is a generic layered architecture that leads step-by-step to a fully segmented network layer structure that describes the PLCnext Technology security architecture and the security use cases in the so-called *security context*.
The security context results from the combination of technological and organizational measures required by the IEC 62443 standard and the philosophy of a holistic security approach.

Defense-in-depth concept



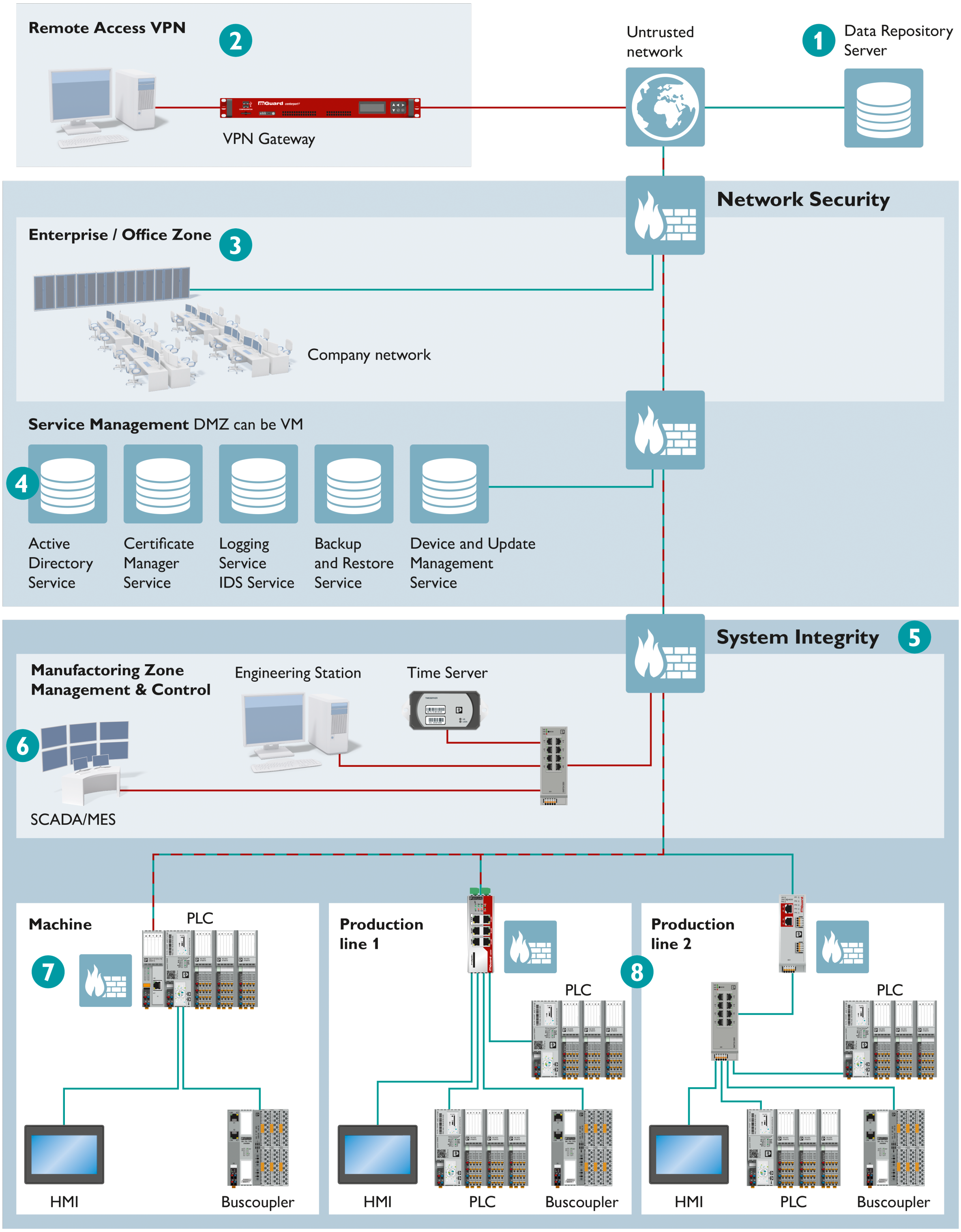
A generic defense in depth design results in three layers or zones:

- **Perimeter security**
  Perimeters are the outer boundaries of the network,
  protected by physical measures such as fences, doors, physical access controls, etc.
- **Network security**
  This layer contains the enterprise or office zone and a service management zone, protected by well-known IT security concepts.
- **System integrity**
  This layer contains OT devices and applications,
  to be protected by IEC 62443 concepts.

PLCnext Technology security context

The following figure shows the PLCnext Technology generic security context (zones and conduits) focussing on the OT security based on IEC 62443-4-2 requirements.

- *Blue-green connections (—) represent security mechanisms (e.g. TLS / HTTPS).*
- *Red connections (—)represent virtual private networks (VPNs).*

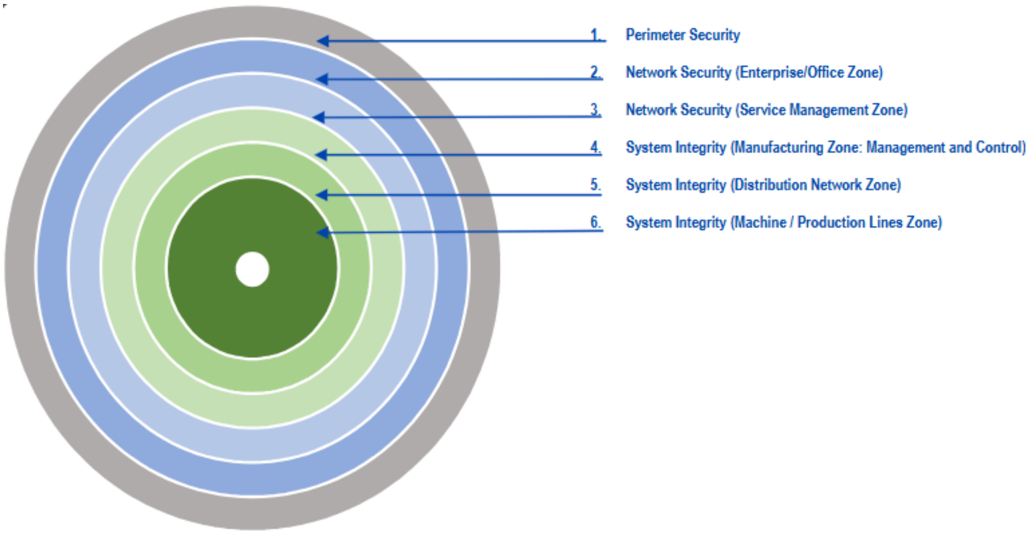


The different layers (zones and conduits) are marked by numbers:

No.	Description	Details
1	**Data Repository Server**	Provides data for patch management/asset management.
2	**VPN Server**	Remote maintenance access via VPN
3	**Enterprise / Office zone**	Factory IT; ERP (Enterprise Resource Planning) systems; production control systems. Protected by firewall
4	**Service management zone**	This zone can be considered as a Demilitarized Zone (DMZ) as it decouples the ICS networks (zones 5 to 7) from the external network by strictly controlling the information flow. Any communication between the external and ICS networks must pass this zone. Implements central user management, patch/update management, and logging. It contains the following infrastructure: – Active Directory/RADIUS server for authentication purposes – Firewall or VPN component (implemented, for example as jump host) handles the communication with the other zones (conduits).
5	**System integrity**	Factory OT, consisting of zones 6 to 8
6	**Manufacturing zone**	Management, monitoring and controlling of the main process and the sub-process. Implements SCADA, time synchronization and engineering. This zone is composed as follows: – Control center (SCADA = Supervisory Control and Data Acquisition) – NTP server which provides a GPS-based time base to the other devices involved – Ethernet switch – Engineering system (such as PLCnext Engineer) – Firewall which handles the communication with the other zones (conduits)
7	**Machine level** **Main process**	Collects and processes of data from the process and the sub-process. This zone is composed as follows: – PLCnext Control with I/O devices The controller integrates firewall and VPN server handling the communication with the other zones (conduits). – HMI for controlling and visualization purposes – Bus couplers
8	**Production line level** **Sub-process**	Performs a specific automation function in a peripheral unit (remote station). This zone is composed as follows: – PLCnext Control, each with distributed I/O devices connected to the field bus – HMI for controlling and visualization purposes. – Ethernet switch – mGuard VPN integrates firewall and/or VPN server handling the communication with the other zones (conduits) – Bus couplers

Six security layers

The PLCnext Technology security context is based on the Defense-in-Depth concept providing six security layers (zones/conduits):


1. Perimeter Security
2. Network Security (Enterprise/Office Zone)
3. Network Security (Service Management Zone)
4. System Integrity (Manufacturing Zone: Management and Control)
5. System Integrity (Distribution Network Zone)
6. System Integrity (Machine / Production Lines Zone)

Perimeter Security - the outer layer

Access protection for the enterprise network by the following measures:

- Physical isolation
- Digital isolation by network segmentation
- Logical access controls
- Use of specifically configured firewalls. The specified firewall must correspond to the identified threats and vulnerabilities.
- VPN or other security measures for remote access
- Documentation of all remote access points

Network Security layers

Protection of the factory network composed of the enterprise network zone and the service management zone which is considered as Demilitarized Zone (DMZ). Possible measures are:

- Identifying all network devices and hosts
- Analysis of protocols/traffic
- Auditing of wireless communication/traffic
- Analysis of switch/router configurations

Measures in the DMZ:

- OS check for vulnerabilities
- OS patch management
- USB or removable devices prevention from use inside control room
- Foreign computers restricted from connecting

System Integrity - the inner layers

Measures for SCADA applications:

- Monitored network for clear text transfer and use of encryption
- Ensured use of individual user accounts
- Restricted access to desktop

Measures for control subnetworks layer at machine/production line level (main process and subprocesses):

- Wired vs. wireless communications
- Ethernet vs. serial communications
- Capture traffic on Ethernet connections

Measures for field controllers:

- Ethernet vs. serial connected devices
- Ethernet devices tested in lab for vulnerabilities
- Removed vendor default passwords

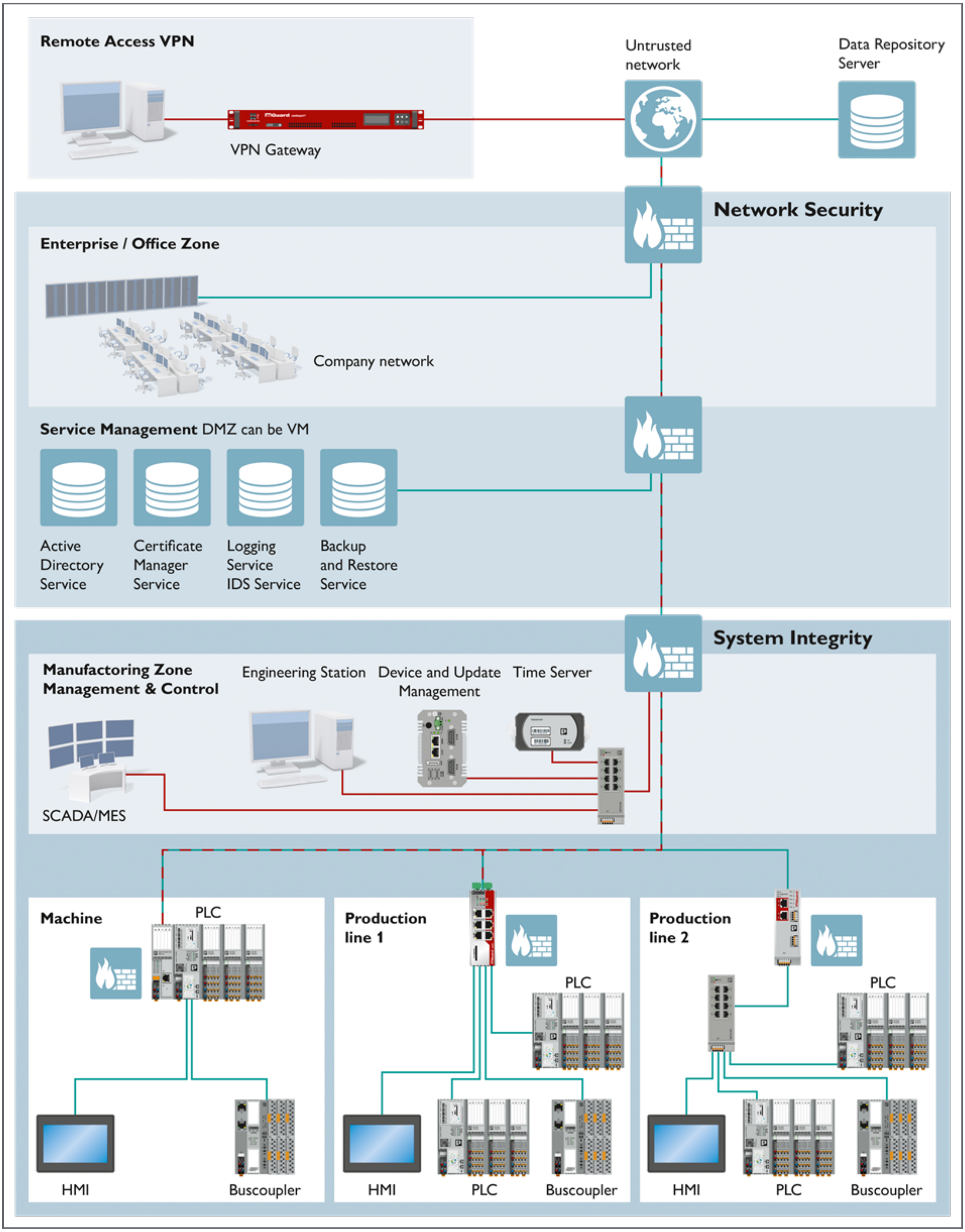
Further Information:
Details on the possible measures can be found in the Security measures topic.

Use cases and security context

PLCnext Technology is supporting different security use cases:

1. Openness is the leading approach, security is not a leading requirement:
   - Industrial Security application note (AH EN INDUSTRIAL SECURITY) must be considered
2. Security is an overall system design requirement, and is ensued by the system design:
   - WBM offers support by User Management, Certificate Authority, Firewall, Syslog, etc.
   - No security certification of the device is provided.
3. A PLCnext Technology device is an IEC 62443-4-1/4-2 certified component:
   - Security Profile must be activated.
   - Security context described in this PLCnext Technology - Security Info Center must fit the required automation system use cases.
   - IEC 62443-3-3 and IEC 62443-2-4 system design and installation/maintenance processes are supported.
   - Centralized security functions like Device and Update Management (DaUM), logging, backup and restore or OT PKI might be combined on an Edge Device and moved from the Service Management zone (IT) to the Manufactoring zone (OT) to separate IT and OT more strictly.

...continuation see next page...


Remote Access VPN
VPN Gateway
Untrusted network
Data Repository Server
Network Security
Enterprise / Office Zone
Company network
Service Management DMZ can be VM
Active Directory Service
Certificate Manager Service
Logging Service IDS Service
Backup and Restore Service
System Integrity
Manufactoring Zone Management & Control
Engineering Station
Device and Update Management
Time Server
SCADA/MES
Machine
PLC
HMI
Buscoupler
Production line 1
PLC
HMI
PLC
Buscoupler
Production line 2
PLC
HMI
PLC
Buscoupler

PLCnext Technology secure-by-design features

PLCnext Technology was developed according to the secure-by-design procedures from the beginning.

The next formal step was to certify the development process according to IEC 62443-4-1, and to prove the PLCnext Technology Security Level 2 feature set by an IEC 62443-4-2 certification.
To build an automation solution with PLCnext Technology based on the IEC 62443-4-1/4-2 certification the definitions described in this PLCnext Security Info Center must be fulfilled.
The activation of the Security Profile (Link) is mandatory.

The following features are building the base of the PLCnext Security.

Hardware measures

- TPM-protected Phoenix Contact device certificate
- Integrity check of devices while booting (depending in part on the controller model)
- Network segmentation by independent intefaces (e.g. the use of left-aligning AXC F XT ETH 1TX, depending on the controller model)
- Use of an SD card with encryption

Firmware measures

- Basing on Yocto Linux with secure-released components and automatic vulnerability supervision
- Secure communication via TLS 1.2, TLS 1.3, HTTPS, OPC UA®, SFTP, SSH, VPN
- User Manager supporting roles, permissions, credentials, and LDAP connection
- Certificate store for manufacturers, system integrators, and asset owners
- Firewall with management of different interfaces, levels for chains and rules
- Syslog-ng for secure message management and central storage
- Time synchronization via NTP
- Backup and restore via rsync
- Device and Update Management (DaUM) for e.g. firmware updates

PLCnext Technology security hardening

To use PLCnext Technology as an IEC 62443-4-1/4-2 certified component, the activation of the Security Profile is mandatory. In addition, the automation system design must fit the security context and the generic use cases described in this PLCnext Technology - Security Info Center.

With activated Security Profile PLCnext Technology supports the following functions:

- Clean device (Reset type 1)
- Integrity check on boot
- Least functionality
  - Limited PLCnext Technology openness
  - Only dedicated PLCnext ARP modules loaded
  - No root access, no SSH access, `admin` user switched off
- Authorization
  - Password complexity rules, lifetime restrictions and timeouts (*brute force* protection)
  - Specialized `SecurityAdmin` and `SecurityAuditor` user roles for device configuration and security monitoring
  - Central User Management systems support via LDAP
- Zone and *denial of service* protection
  - Firewall configuration for each dedicated Ethernet MAC address via WBM
  - Validation of incoming and outgoing data via external interfaces
  - Netload Limiter pre-configured and configurable
- Certificate Authority (CA) manages device identity and trusted partners
- Integrity and authenticity of data in rest and data in transmission
  - SD card with encrypted partition
  - Secure communication TLS 1.2, TLS 1.3 and OPC UA® (signed & encrypted)
- Security logging
  - Protected security logging
  - Connection to a central server
- Explicit activation of PLCnext Technology features via WBM
  - eHMI, or OPC UA®
  - App Manager for using the PLCnext Store might be activated (according to the security context, a threat analysis required)
- Local Axioline I/Os are supported
- PROFINET can be activated after threat analysis and protection measures from the security context
- Cabinet supervision (must be locked) via an application which generates security notifications

For more information on these features, please refer to the IEC 62443-4-1/4-2 Security Level 2 (SL2) feature set described in the IEC 62443-4-2 compliance list.

Security architecture

To fulfill the IEC 62443-4-1 requirements a threat analysis of the PLCnext Runtime System and PLCnext Technology hardware is an important task. The PLCnext Technology threat analysis is based on the *STRIDE* model which consists of the identification of these security threats in these categories: spoofing, tampering, repudiation, Information disclosure, denial of service, elevation of privilege.

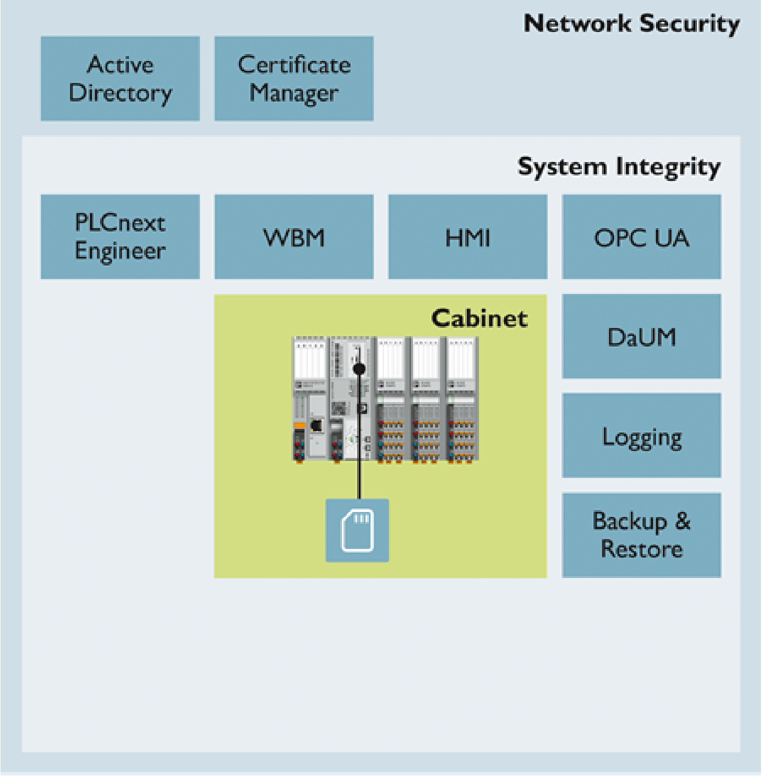
As a prerequisite the security context defined in this PLCnext Technology - Security Info Center and the implemented Security Level 2 (SL2) feature set are used.

One key element of the threat analysis is to review the integrity and authenticity of the data in rest and data in transmission. Another key element is the authorization of human users and software components to access the data. In addition, the firewall protects the access to the communication interfaces, or supports *denial of service* protection.

PLCnext Technology provides TLS 1.2 or TLS 1.3 based communication on necessary communication interfaces (e.g. HTTPS, OPC UA®, PLCnext Engineer).

For other communication channels like LDAP or Syslog-ng, TLS can be activated according the users' needs.

The authorization is handled by an RBAC user management for human users, and/or certificate management for software components.



Security measures

Data in rest

PLCnext Technology's data is stored on an internal (non-removable) SD card. The detailed description of the data and directory structure can be found in the main PLCnext Technology - Info Center at the Directories of the firmware components.
The storage capacity of a PLCnext Control can be enhanced with an external (removable) SD card. Activating the Security Profile is deactivating the external SD card usage because additional security measures are needed to protect the external SD card against unauthorized physical access.

In addition to the extra space for automation project data, the external SD card enables an easy device replacement with licenses transferred via that storage medium. From firmware version 2022.0 LTS special SD cards are available supporting the distribution of licenses:

- SD FLASH 8GB PLCNEXT MEMORY **LIC** (item no. 1151112)
- SD FLASH 32GB PLCNEXT MEMORY **LIC** (item no. 1151111)
- SD FLASH PLCNEXT MEMORY **LIC CFG** (item no. 1308064)

From firmware 2024.0 LTS, these special SD cards provide data protection, and therefore can be used together with the Security Profile.

For further information about protecting the sd card, refer to the topics Protection against physical access and Secure disposal and the topic of the respective controller (e.g. AXC F 2152).

Data in transmission

To support secure communication e.g. via TLS, different options of cryptographic keys can be can be configured in the Certificate Authentication WBM page.

1. PLCnext Technology self-signed certificates are preconfigured for HTTPS and OPC UA®. Additional self-signed certificates can be configured according to the user's needs.
2. Certificates are installed from an asset owners PKI. To configure dedicated asset owner identities, keys and certificates generated by a PKI can be installed in the identity store on the PLCnext Control device.
3. PLCnext supports TPM-generated keys and their related certificates. TPM-generated keys are currently usable for the TLS function block in the PLC application. Further use cases will be available in the future. TPM-generated keys are only valid in relationship with the dedicated TPM.

Use case 1 and 2 offer more flexibility for device replacement but less strict security as the private keys are stored in the PLCnext Control's file system. Additional system security measures might be needed to protect the device against physical access of the internal SD card.

Use case 3 offers high security as the private keys are not stored in the file system but the key generation is more complex. As well the device replacement is more complex because the keys are only valid on the device which contains the specific TPM which has generated the key.

User Management

PLCnext Technology’s User Management provides authentication and authorization on each communication interface. Only authorized users can access (read/write) data via a communication interface.

Software information integrity and authenticity

Software information security is provided by different mechanisms:

1. Boot integrity check (software based partial; see Checking the integrity state)
2. Signature of firmware container
3. Each PLCnext Technology-related software provided for download from the Phoenix Contact website provides an SHA256 value. It can be used to check the integrity of the software after download before installation on the PC or on the PLCnext Control.

Mobile and malicious code protection

Authentication and authorization are provided by the User Management: Only authorized users get access (read/write) to the PLCnext Control's data.

PLCnext Engineer enforces the user to enter his credentials before accessing the controller. Only authorized users can download an application to the PLCnext Control device. An integrity check is performed in PLCnext Engineer (see Checking project data integrity).
PLCnext Engineer or toolchains generating code must be installed on secure managed PCs only. In the security context, one especially supervised engineering PC is installed in the Manufacturing zone for engineering access to the PLCnext Control devices during maintenance phases.

Periodic security maintenance activities

You must check regularly:

- user roles and permissions
- password complexity rules and password changes
- firewall settings
- all security-related settings
- the product download area for firmware updates
- the PSIRT webpage for known security vulnerabilities

Security functionality verification

As a system integrator and asset owner, you must use a tool to automatically test interfaces and ensure that security measures are successful. The tool must check:

- user and certificates
- activated system services
- firewall settings (active rules can be exported and be used to check the measures, for further information refer to the topic Configuring extended firewall settings)
- extern SD card (encrypted)

Please check the notifications of the security logging, for further information refer to the topics Security logging and Configuring central logging.

IDS tools

IDS tools (intrusion detection systems), e.g. port scan, vulnerability scans:
It is advisable to use these tools only when the plant is shut down to avoid negative influences on production.
Whether IDS tool checks are possible during operation must be clarified by the asset owner or the system integrator on the basis of a risk analysis.

Secure operation

Secure operation

The secure operation of PLCnext Control in your specific application context requires a defined procedure. You will find all necessary steps in the following sections:

- PLCnext starting up: Everything you need to know when starting up your PLCnext Control in a security context.
- PLCnext environmental requirements: All environmental requirements you need to consider when operating your PLCnext Control in a security context.
- Account management: When operating a PLCnext Control in a security context, you need to consider some points in the account management.

PLCnext starting up

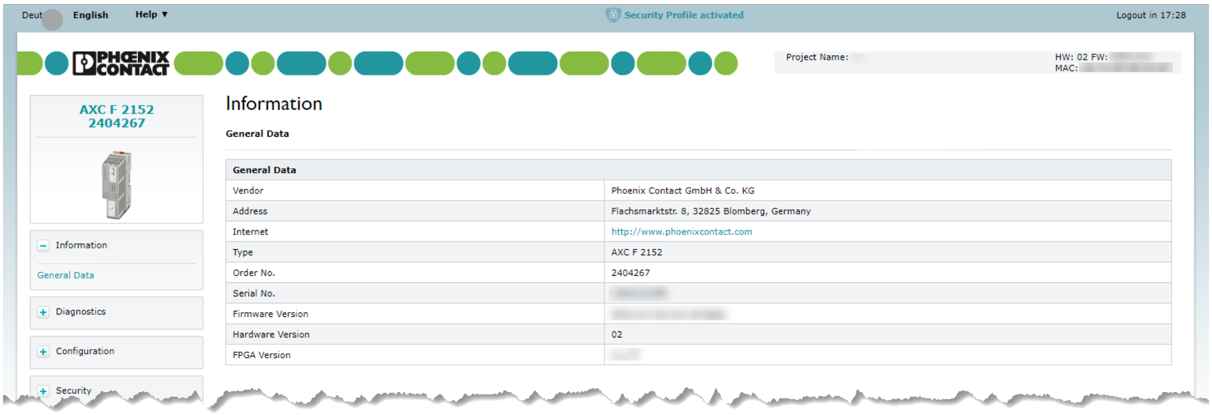
PLCnext starting up

The starting up of a PLCnext Control in a security context includes the following steps:

- Checking the device
- Deriving IP addresses
- Assigning IP addresses
- Configuring TLS
- Generating self-signed HTTPS certificates in the WBM
- Uploading the certificate in the browser
- Activating the Security Profile
- Checking the integrity state
- Checking SD card settings
- Creating users
- Configuring basic firewall settings
- Configuring Netload Limiter
- Security logging

Checking the device

- Log in to the WBM.
- Open the **General Data** page (**Information** → **General Data**).
- Check whether you are working on the correct device:
  - PLCnext Control AXC F 2152 , Order No. 2404267
  - Serial No. as printed on the device
  - Firmware Version min. 2022 LTS
  - Hardware Version min. 02



Project Name: [redacted]

HW: 02 FW: [redacted]
MAC: [redacted]

Information

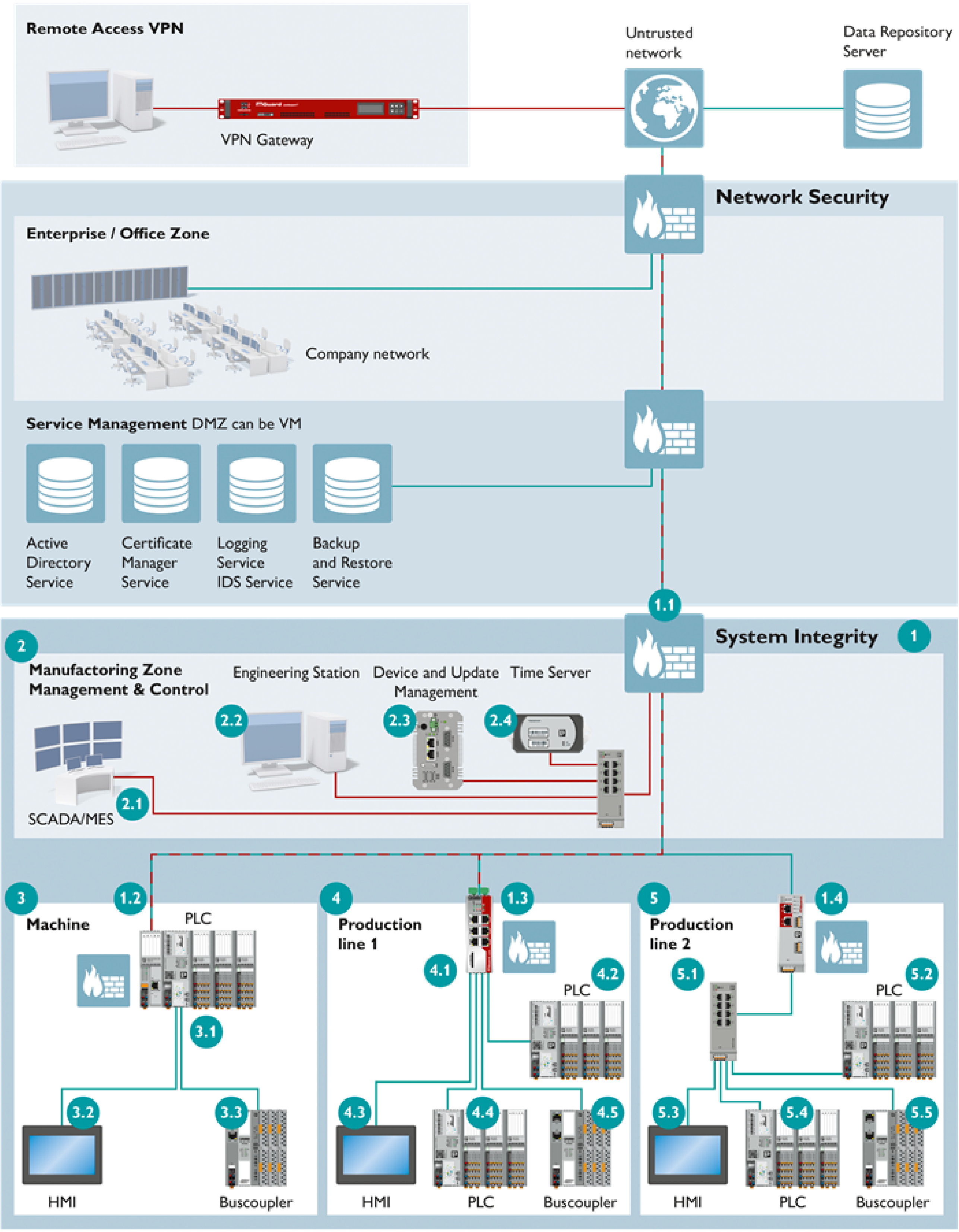
General Data

General Data	
Vendor	Phoenix Contact GmbH & Co. KG
Address	Flachsmarktstr. 8, 32825 Blomberg, Germany
Internet	http://www.phoenixcontact.com
Type	AXC F 2152
Order No.	2404267
Serial No.	[redacted]
Firmware Version	[redacted]
Hardware Version	02
FPGA Version	[redacted]

Deriving IP addresses

Your specific security context determines the network structure and also the IP addresses. To assign the IP addresses that are suitable for you, you must derive them from your security context.

The following is an example security context that you must adapt to your application.



Zone segmentation IP address spaces:

No.	Zone segments	IP address spaces	Subnetmask
1	System integrity	172.16.10.0/28	255.255.255.240
2	Manufacturing Zone Management & Control	172.16.20.0/24	255.255.255.0
3	Machine	172.16.30.0/26	255.255.255.192
4	Production line 1	172.16.40.0/24	255.255.255.0
5	Production line 2	172.16.50.0/24	255.255.255.0

1 System integrity: IP addess space 172.16.10.0/28, Subnetmask 255.255.255.240

No.	Zone segment	IP address
1.1	IT firewall network segmentation Manufacturing Zone Management & Control	172.16.10.10
1.2	AXC F 2152 network segmentation AXC F 2152 left pluggable Ethernet connection	172.16.10.30
1.3	mGuard RS 4000 network segmentation firewall and VPN	172.16.10.40
1.4	mGuard 1102 network segmentation firewall	172.16.10.50

2 Manufacturing Zone Management & Control: IP addess space 172.16.20.0/24, Subnetmask 255.255.255.0

No.	Zone segment	IP address
2.1	SCADA/MES	172.16.20.60
2.2	Engineering Station	172.16.20.100
2.3	Edge Device EPC 1522 Device and Patchmanagement	172.16.20.50
2.4	Time Server FL TIMESERVER NTP	172.16.20.40

3 Machine: IP address space 172.16.30.0/26, Subnetmask 255.255.255.192

No.	Zone segment	IP address
3.1	AXC F 2152 CPU Ethernet interface	172.16.30.10
3.2	HMI Touch-Panel - TP 6070-WVPS	172.16.30.20
3.3	Buscoupler AXL F BK PN TPS with Smart IOs	172.16.30.30

4 Production line 1: IP address space 172.16.40.0/24, Subnetmask 255.255.255.0

No.	Zone segment	IP address
4.1	mGuard RS 4000 Local IP Address	172.16.40.5
4.2	AXC F 2152 CPU ethernet interface	172.16.40.10
4.3	HMI Touch-Panel - TP 6070-WVPS	172.16.40.20
4.4	AXC F 2152 CPU ethernet interface	172.16.40.11
4.5	Buscoupler AXL F BK PN TPS with Smart IOs	172.16.40.30

5 Production line 2: IP address space 172.16.50.0/24, Subnetmask 255.255.255.0

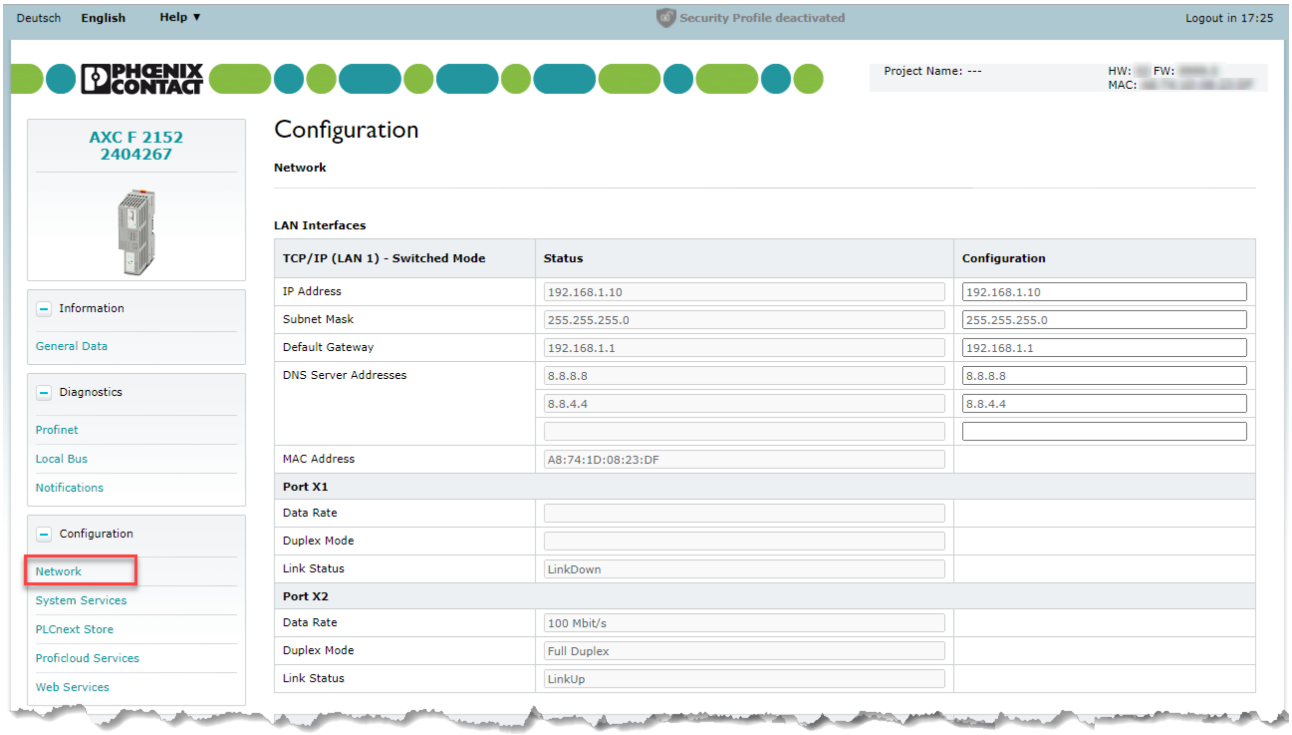
No.	Zone segment	IP address
5.1	mGuard 1102 Local IP Address	172.16.50.5
5.2	AXC F 2152 CPU ethernet interface	172.16.50.10
5.3	HMI Touch-Panel - TP 6070-WVPS	172.16.50.20
5.4	AXC F 2152 CPU ethernet interface	172.16.50.11
5.5	Buscoupler AXL F BK PN TPS with Smart IOs	172.16.50.30

- First, define a network definition. This is reflected in the first 24 bits of the IP addresses (in the example: **172.16.**xx.xxx). Bits 25 to 32 are reserved for the local devices.
- The Engineering Station (where the PLCnext Engineer is located) has the IP address 172.16.20.100 (255.255.255.0).
- The Machine Level is configured so that access from the Manufacturing Zone to the Machine Level is via the Ethernet interface of the extension module.
- The extension module is assigned the IP address 172.16.10.30. The IP address of the PLCnext Control is 172.16.30.10 (255.255.255.240).

For more information about the zones of the security context, refer to the topic Generic Security Concept .

Assigning IP addresses

- Log in to the WBM.
- Open the **Network** page (**Configuration** → **Network**).



Deutsch English Help ▼ Security Profile deactivated Logout in 17:25

Project Name: --- HW: [redacted] FW: [redacted] MAC: [redacted]

AXC F 2152
2404267

Configuration

Network

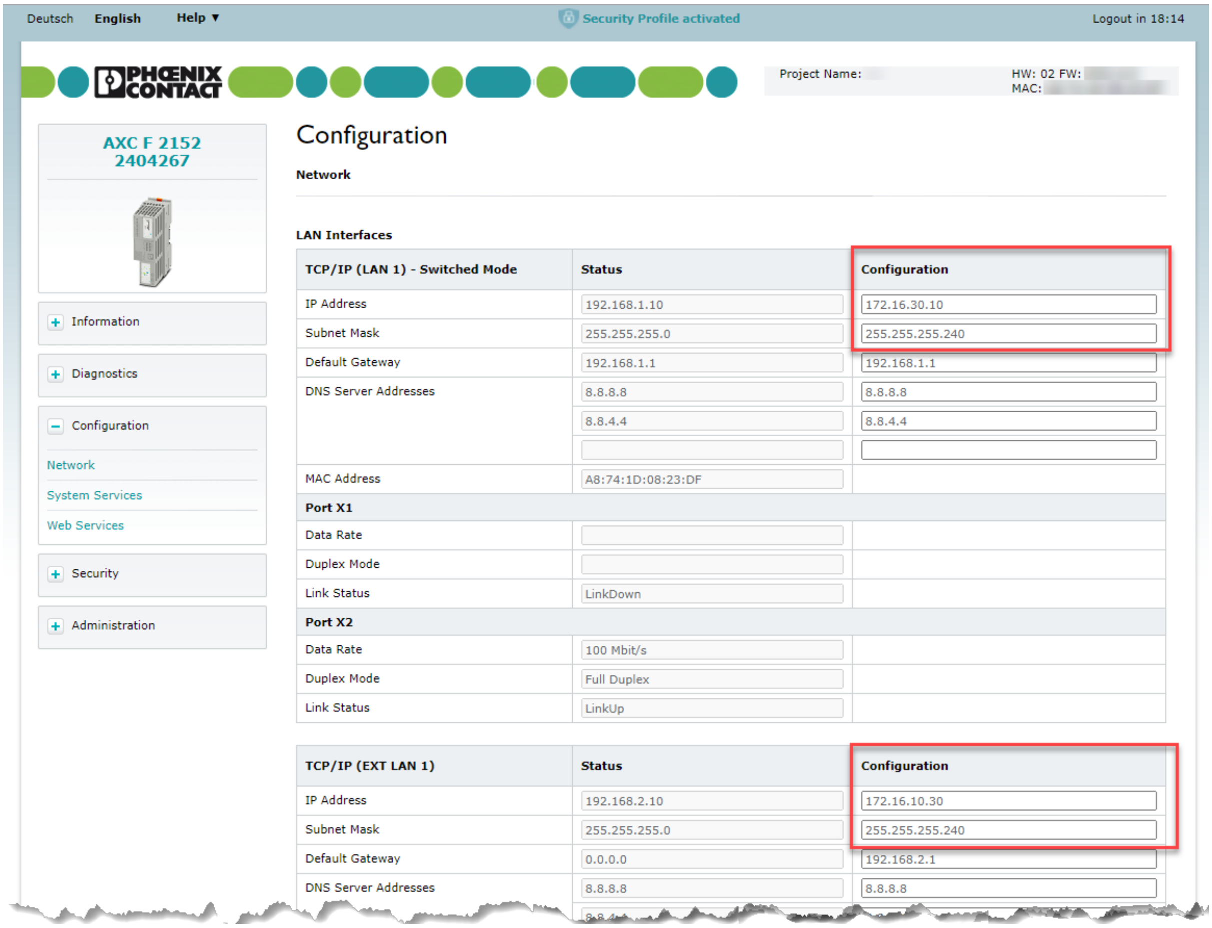
LAN Interfaces

TCP/IP (LAN 1) - Switched Mode	Status	Configuration
IP Address	192.168.1.10	192.168.1.10
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	192.168.1.1
DNS Server Addresses	8.8.8.8 8.8.4.4	8.8.8.8 8.8.4.4
MAC Address	A8:74:1D:08:23:DF	
Port X1		
Data Rate		
Duplex Mode		
Link Status	LinkDown	
Port X2		
Data Rate	100 Mbit/s	
Duplex Mode	Full Duplex	
Link Status	LinkUp	

The information under **TCP/IP (LAN1) - Switched Mode** refers to the subordinate network, i.e. the extension module. The information under **TCP/IP (EXT LAN 1)** refers to the higher-level network, i.e. the PLCnext Control.

...continuation see next page...

- Assign IP addresses and Subnet Masks for both networks appropriate for your security context (see topic Deriving IP addresses) by entering them in the Configuration area.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

Configuration

Network

LAN Interfaces

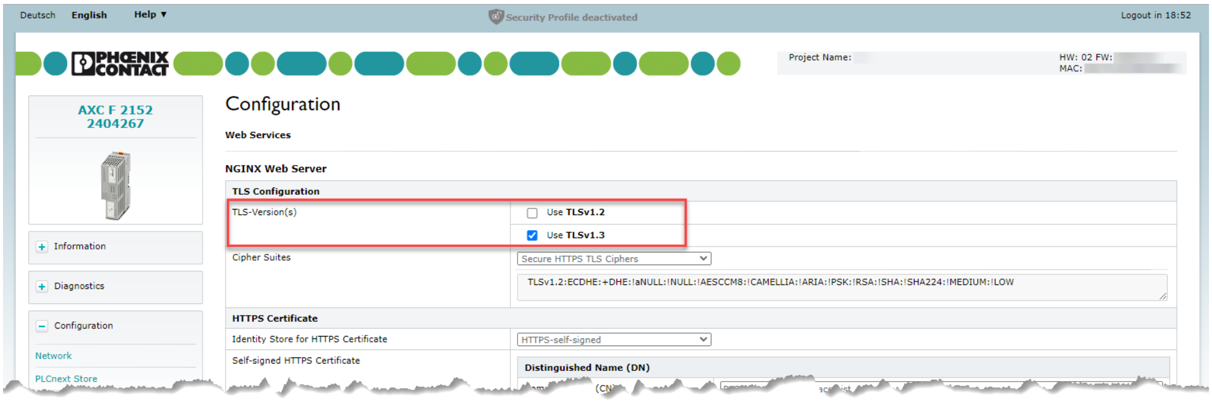
TCP/IP (LAN 1) - Switched Mode	Status	Configuration
IP Address	192.168.1.10	172.16.30.10
Subnet Mask	255.255.255.0	255.255.255.240
Default Gateway	192.168.1.1	192.168.1.1
DNS Server Addresses	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC Address	A8:74:1D:08:23:DF	
Port X1		
Data Rate		
Duplex Mode		
Link Status	LinkDown	
Port X2		
Data Rate	100 Mbit/s	
Duplex Mode	Full Duplex	
Link Status	LinkUp	

TCP/IP (EXT LAN 1)	Status	Configuration
IP Address	192.168.2.10	172.16.10.30
Subnet Mask	255.255.255.0	255.255.255.240
Default Gateway	0.0.0.0	192.168.2.1
DNS Server Addresses	8.8.8.8	8.8.8.8

- Click the Apply and reboot button.

Configuring TLS

- Log in to the WBM.
- Open the Web Services page (Configuration → Web Services).
- Select TLS version TLSv1.3 .



Configuration

Web Services

NGINX Web Server

TLS Configuration

TLS-Version(s)	☐ Use **TLSv1.2** ☑ Use **TLSv1.3**
Cipher Suites	Secure HTTPS TLS Ciphers TLSv1.2:ECDHE:+DHE:!aNULL:!NULL:!AESCCM8:!CAMELLIA:!ARIA:!PSK:!RSA:!SHA:!SHA224:!MEDIUM:!LOW

HTTPS Certificate

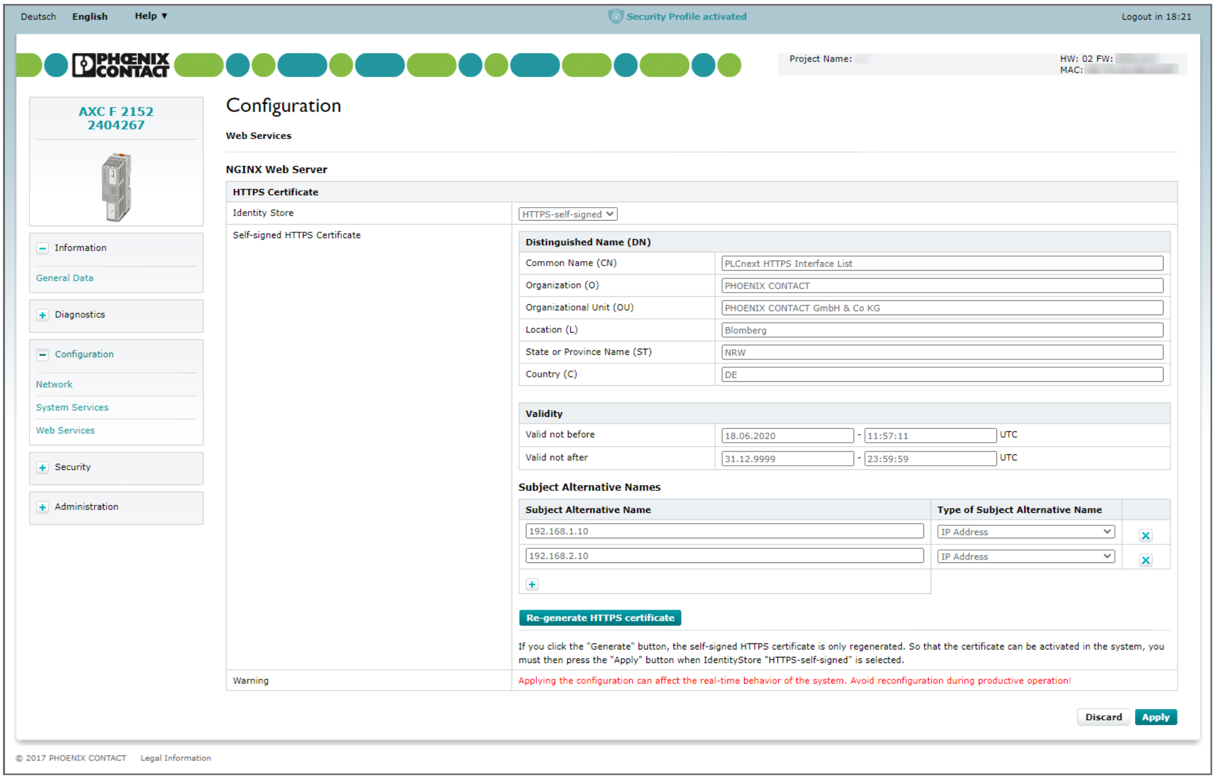
Identity Store for HTTPS Certificate	HTTPS-self-signed
Self-signed HTTPS Certificate	**Distinguished Name (DN)**

Note:

- If you cannot set TLS version TLSv1.3 , set TLS Version TLSv1.2 .
- If you set TLS Version TLSv1.2 , you must set Secure HTTPS TLS Ciphers cipher suite.
- If your browser does not support the secure cipher suite, you must set the Default HTTPS TLS Ciphers cipher suite. In this case, you must perform a risk analysis.

Generating self-signed HTTPS certificates in the WBM

- Log in to the WBM.
- Open the **Configuration** → **Web Services** page in the WBM.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

Configuration

Web Services

NGINX Web Server

HTTPS Certificate	
Identity Store	HTTPS-self-signed
Self-signed HTTPS Certificate	

Distinguished Name (DN)	
Common Name (CN)	PLCnext HTTPS Interface List
Organization (O)	PHOENIX CONTACT
Organizational Unit (OU)	PHOENIX CONTACT GmbH & Co KG
Location (L)	Blomberg
State or Province Name (ST)	NRW
Country (C)	DE

Validity			
Valid not before	18.06.2020	11:57:11	UTC
Valid not after	31.12.9999	23:59:59	UTC

Subject Alternative Names

Subject Alternative Name	Type of Subject Alternative Name
192.168.1.10	IP Address
192.168.2.10	IP Address

Re-generate HTTPS certificate

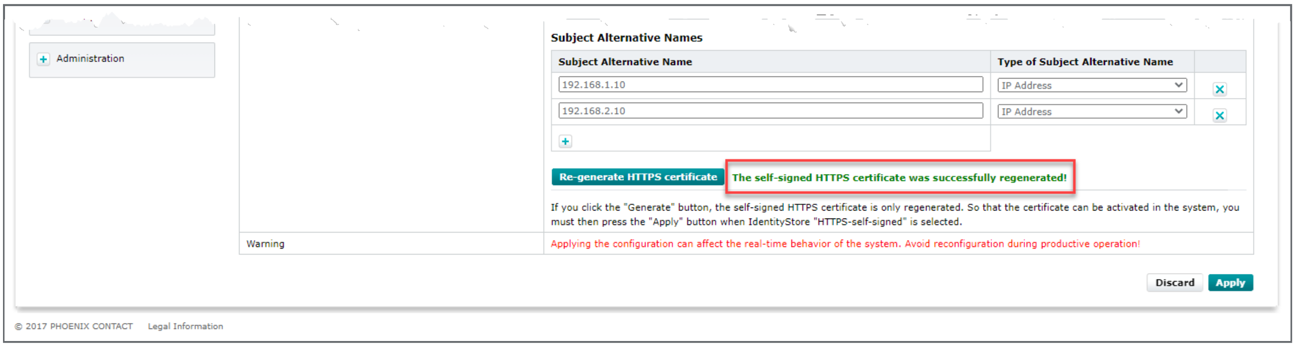
If you click the "Generate" button, the self-signed HTTPS certificate is only regenerated. So that the certificate can be activated in the system, you must then press the "Apply" button when IdentityStore "HTTPS-self-signed" is selected.

Warning: Applying the configuration can affect the real-time behavior of the system. Avoid reconfiguration during productive operation!

Discard Apply

- In the **Identity Store** drop-down menu, select **HTTPS-self-signed**.
- In the **Self-signed HTTPS Certificate** area, enter the required information.
- In the **Subject Alternative Names** area, enter the required IP addresses.
- Add more IP addresses if needed by clicking the **+**.
- Click the **Re-generate HTTPS certifcate** button.

If the certificate generation was successful, it will be displayed next to the **Re-generate HTTPS certifcate** button.



Subject Alternative Names

Subject Alternative Name	Type of Subject Alternative Name
192.168.1.10	IP Address
192.168.2.10	IP Address

Re-generate HTTPS certificate — The self-signed HTTPS certificate was successfully regenerated!

If you click the "Generate" button, the self-signed HTTPS certificate is only regenerated. So that the certificate can be activated in the system, you must then press the "Apply" button when IdentityStore "HTTPS-self-signed" is selected.

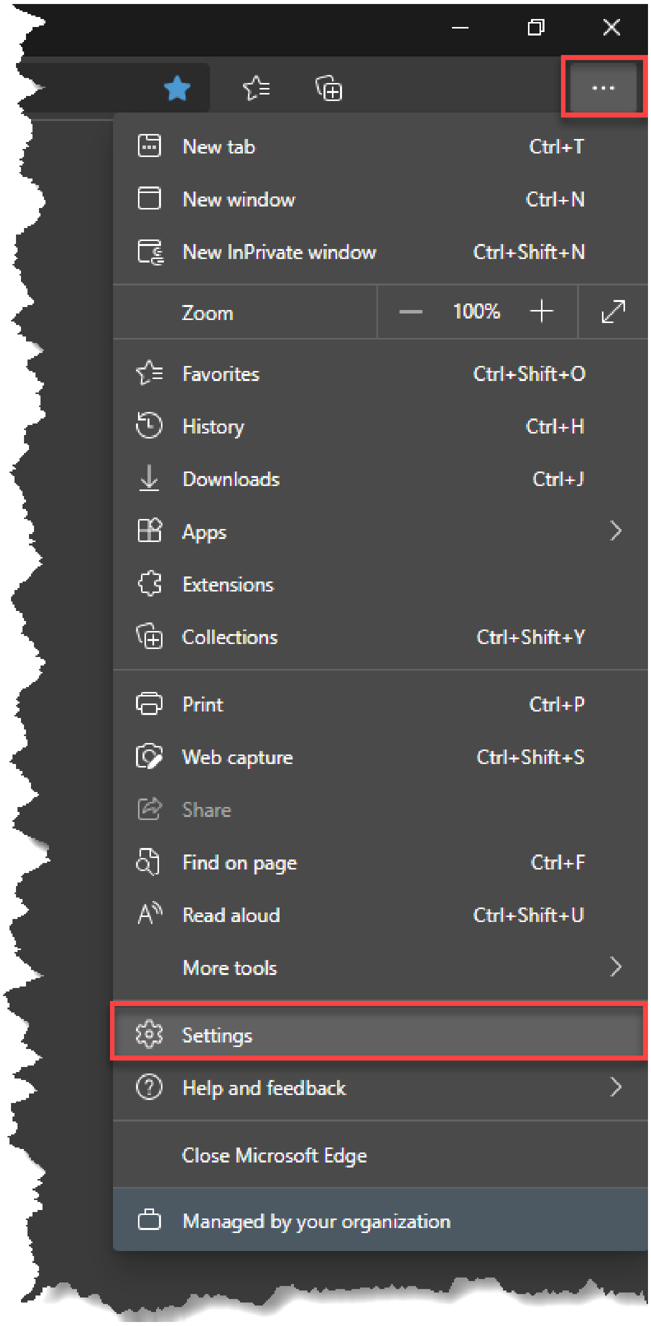
Warning: Applying the configuration can affect the real-time behavior of the system. Avoid reconfiguration during productive operation!

Discard Apply

- To activate the generated certificate in the system, click the **Apply** button.

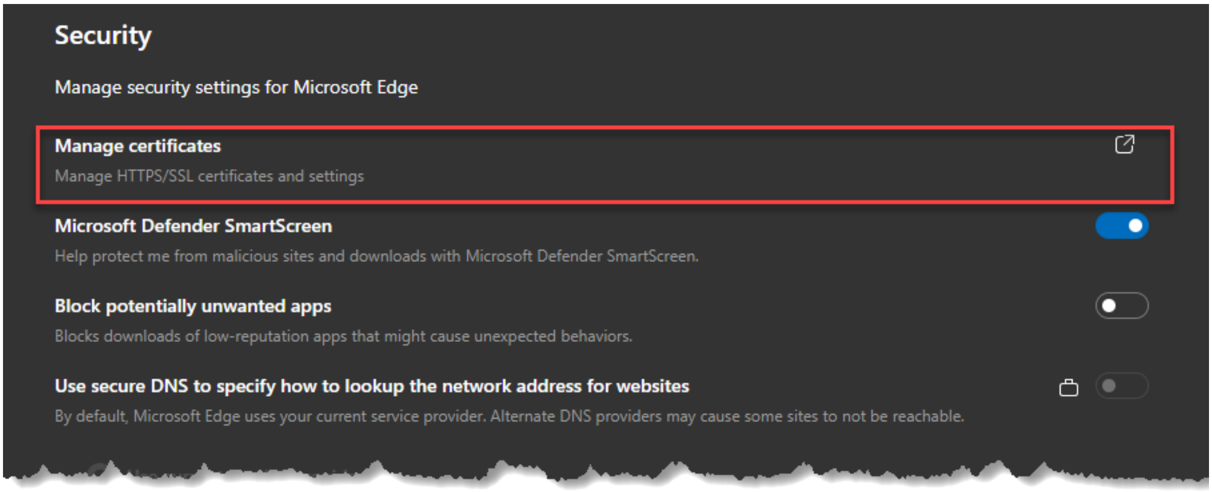
Uploading the certificate in the browser

- Log in to the WBM.
- Open the **Security** → **Certificate Authentication** page in the WBM.
- Open the **Identity Stores** tab.
- In the **HTTPS-self-signed** area, download the certificate you just generated by clicking the ⬇ button ("Download from controller to local pc") next to the certificate.
- Open your browser (Edge).
- Open the **Settings** menu.



- Open the **Privacy, search, and services** tab .

- In the **Security** section, click the **Manage certificates** button.



Security

Manage security settings for Microsoft Edge

Manage certificates
Manage HTTPS/SSL certificates and settings

Microsoft Defender SmartScreen
Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen.

Block potentially unwanted apps
Blocks downloads of low-reputation apps that might cause unexpected behaviors.

Use secure DNS to specify how to lookup the network address for websites
By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.

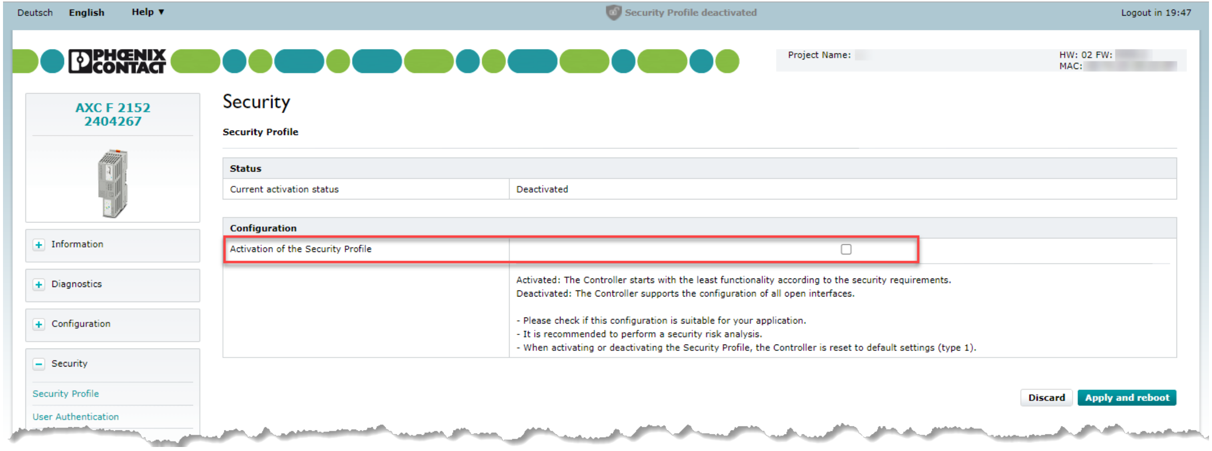
↪ A new window opens.

- Open the **Trusted root certificates** tab.
- Click the **Import...** button.
  ↪ The "Certificate Import Wizard" opens.
- Follow the instructions of the "Certificate Import Wizard".
- Select the certificate you want to import and click the **Open** button.
- Click the **Next** button.
- Select **Place all certificates in the following store** and click the **Browse...** button.
- Set the **certificate store** option to **Trusted root certificates** and click the **OK** button.
- Click the **Next** button.
- Click the **Finish** button.
- If a warning note opens, read the warning note and in case you want to confirm it, click the **Yes** button.
  ↪ The certificate was uploaded in the browser.
- Check the status of the certificate in your browser.

Handling the Security Profile

Activating the Security Profile

- Log in to the WBM.
- Open the **Security Profile** page (**Security** → **Security Profile**) in the WBM.
- Select the checkbox named "Activation of the Security Profile".



Security

Security Profile

Status	
Current activation status	Deactivated

Configuration	
Activation of the Security Profile	□
	Activated: The Controller starts with the least functionality according to the security requirements. Deactivated: The Controller supports the configuration of all open interfaces. - Please check if this configuration is suitable for your application. - It is recommended to perform a security risk analysis. - When activating or deactivating the Security Profile, the Controller is reset to default settings (type 1).

- Click the **Apply and reboot** button.

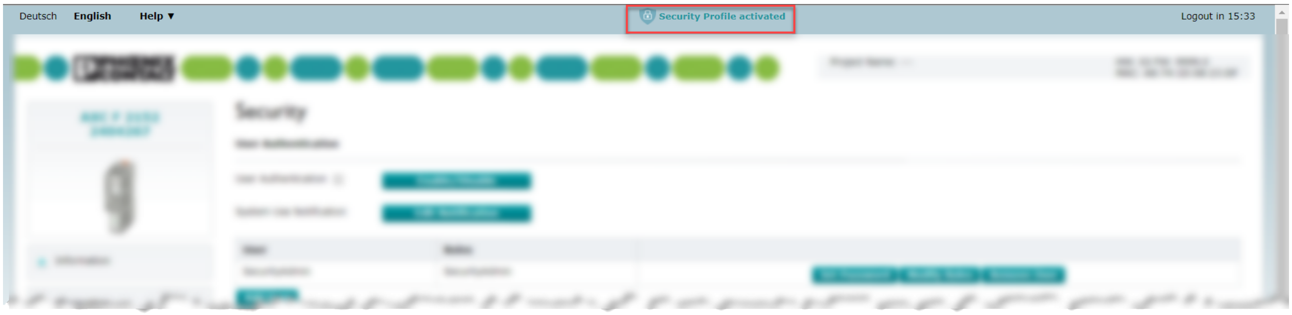
The PLCnext Control is now reset to default settings (type 1) and then rebooted. However, IP addresses and installed licenses are retained.

After rebooting you have to log in again.

> **Note:** There is no longer the role "Admin". You need to log in as "SecurityAdmin". The password is still the password printed on the housing of the PLCnext Control.

- Log in to the WBM as "SecurityAdmin".

In the top bar you can see that the Security Profile is activated.



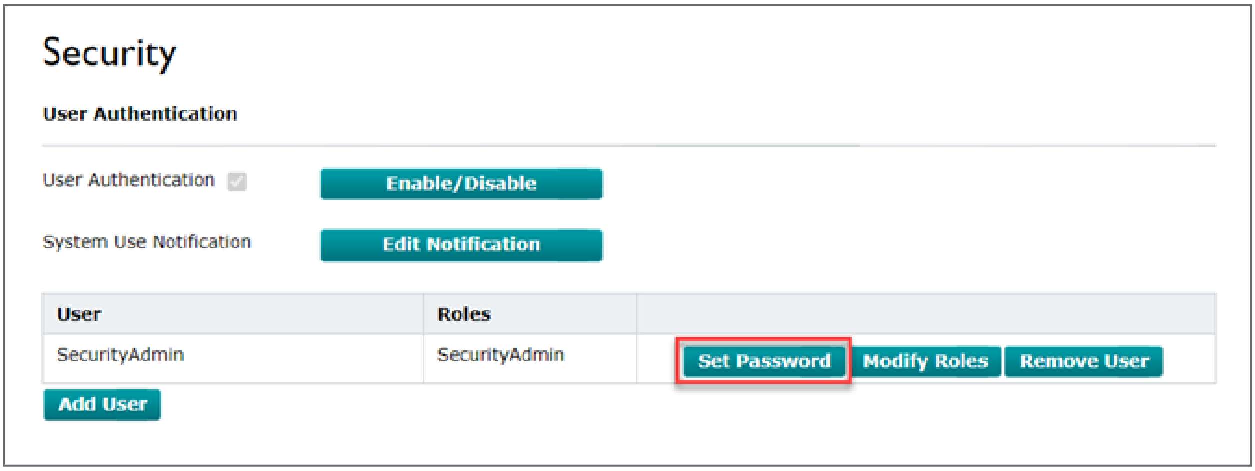
Note: Now follow the steps from the topic Checking the integrity state.

Note: With activating the Security Profile the https certificates are deleted. Therefore you must generate the https certificates again and upload them in your browser. Refer to the topics Generating self-signed https certificates in the WBM and Uploading the certificate in the browser.

Changing the password of the SecurityAdmin

You have to change the password of the SecurityAdmin. To do this, proceed as follows:

- Open the **User Authentication** page.
- Click the **Set Password** button.



Security

User Authentication

User Authentication ☑

System Use Notification

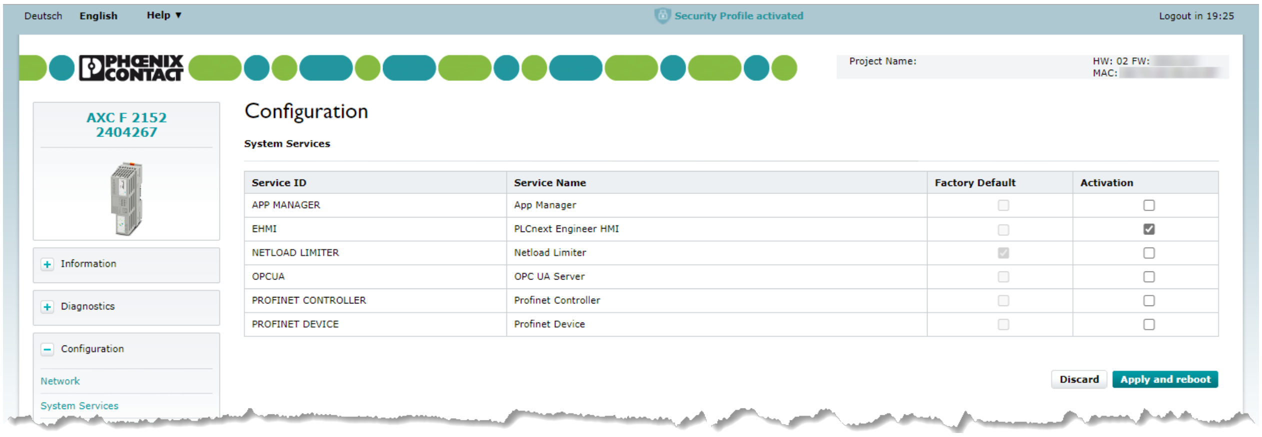
User	Roles	
SecurityAdmin	SecurityAdmin	

- Set a new password following the password complexity rules and save it by clicking the **Save** button.

Effects of the Security Profile

- With the Security Profile, some WBM pages are no longer accessible for security reasons and are disabled in the WBM navigation.
- The SecurityAdmin can only configure the system. All other activities must be performed by other roles. You need at least an Engineer to program in PLCnext Engineer and a Security Auditor to access the security notifications.
- You have no root access and no SSH access.
- The Security Profile follows the principle of least functionality: only components that have been considered in the threat analysis may run. This specifies exactly what is permissible.

– On the System Services page you may see effects of the principle of least functionality: The number of components is limited by the Security Profile. All services except Netload Limiter are disabled. Only activate the services that you actually need. For example, you must decide which visualization mechanism is used (eHMI or OPC UA) and then activate it accordingly. Consider your respective security context. If your network is sufficiently protected by additional organizational measures , you can activate the PROFINET Controller and possibly PROFINET Device if necessary.



Project Name:

HW: 02 FW: [redacted]
MAC: [redacted]

Configuration

System Services

Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	□	□
EHMI	PLCnext Engineer HMI	□	☑
NETLOAD LIMITER	Netload Limiter	☑	□
OPCUA	OPC UA Server	□	□
PROFINET CONTROLLER	Profinet Controller	□	□
PROFINET DEVICE	Profinet Device	□	□

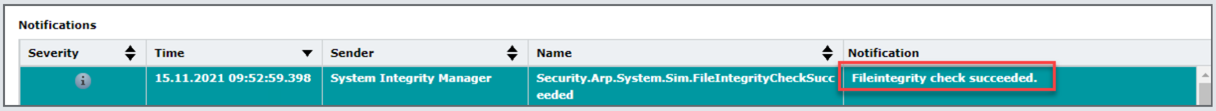
→ Go to the topic Creating users to set up additional users and login conditions.

ℹ For more information on the different roles and rights, refer to the User Authentication WBM topic in the PLCnext Technology - Info Center.

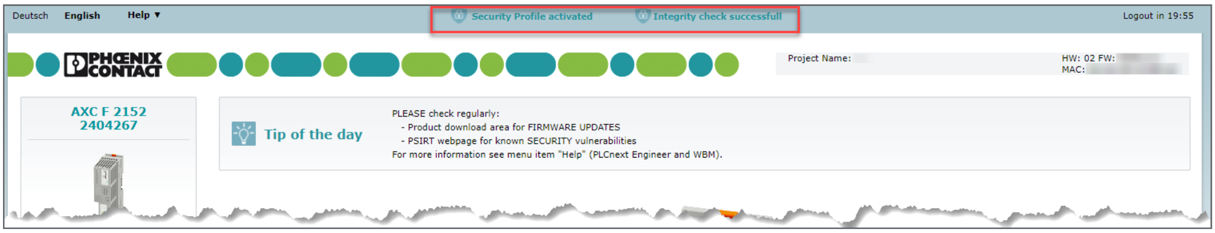
Checking the integrity state

If the Security Profile is activated, an integrity state check is performed after each boot and log-in to the WBM.

The integrity state is displayed in the WBM in the page header line right to the Security Profile state field.

> **Note:** Every event is logged. On the `Notifications` page in the WBM, you can see whether the file integrity check was successful.
>
> 
>
> Notifications
>
> | Severity | Time | Sender | Name | Notification |
> |---|---|---|---|---|
> | ⓘ | 15.11.2021 09:52:59.398 | System Integrity Manager | Security.Arp.System.Sim.FileIntegrityCheckSucceeded | Fileintegrity check succeeded. |
>
> ⓘ For more information on security logging, refer to the topic Security logging.

Security Profile is activated and the integrity state check is successful



Security Profile activated Integrity check successfull

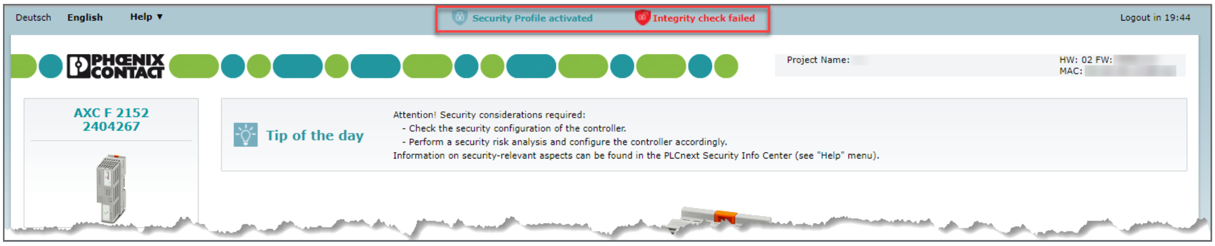
Project Name: [redacted] HW: 02 FW: [redacted] MAC: [redacted]

Tip of the day

PLEASE check regularly:
- Product download area for FIRMWARE UPDATES
- PSIRT webpage for known SECURITY vulnerabilities

For more information see menu item "Help" (PLCnext Engineer and WBM).

Security Profile is activated but the integrity state check failed



Security Profile activated Integrity check failed

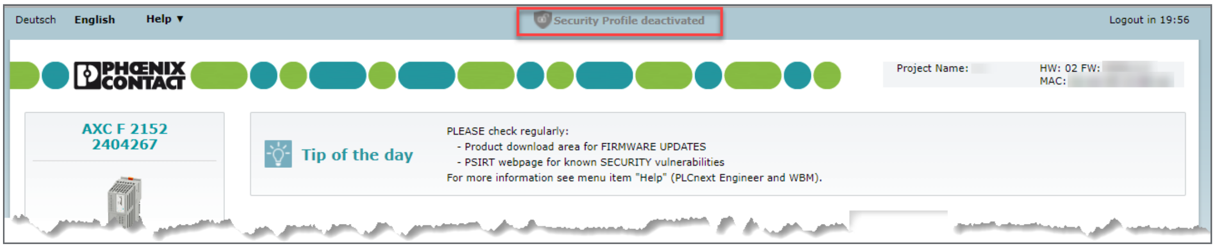
Project Name: [redacted] HW: 02 FW: [redacted] MAC: [redacted]

Tip of the day

Attention! Security considerations required:
- Check the security configuration of the controller.
- Perform a security risk analysis and configure the controller accordingly.

Information on security-relevant aspects can be found in the PLCnext Security Info Center (see "Help" menu).

Security Profile is deactivated, the integrity state field is hidden



Security Profile deactivated

Project Name: [redacted] HW: 02 FW: [redacted] MAC: [redacted]

Tip of the day

PLEASE check regularly:
- Product download area for FIRMWARE UPDATES
- PSIRT webpage for known SECURITY vulnerabilities

For more information see menu item "Help" (PLCnext Engineer and WBM).

Checking SD card settings

Note:

- Make sure that the Security Profile is activated before you start encrypting the SD card.

For BPC 9102S and RFC 4072S

When using a BPC 9102S or RFC 4072S, the use of an external SD card is mandatory. In a security context, you must use encrypted SD cards.

- Make sure that you only use an encrypted SD card.

For further information, refer to the topic SD card encryption.

For AXC F 1152, AXC F 2152, AXC F 3152, SPLC 1000 and SPLC 3000

You can use an AXC F 1152, AXC F 2152, AXC F 3152, SPLC 1000 and SPLC 3000 with or without an external SD card. Please note the following information for the respective use.

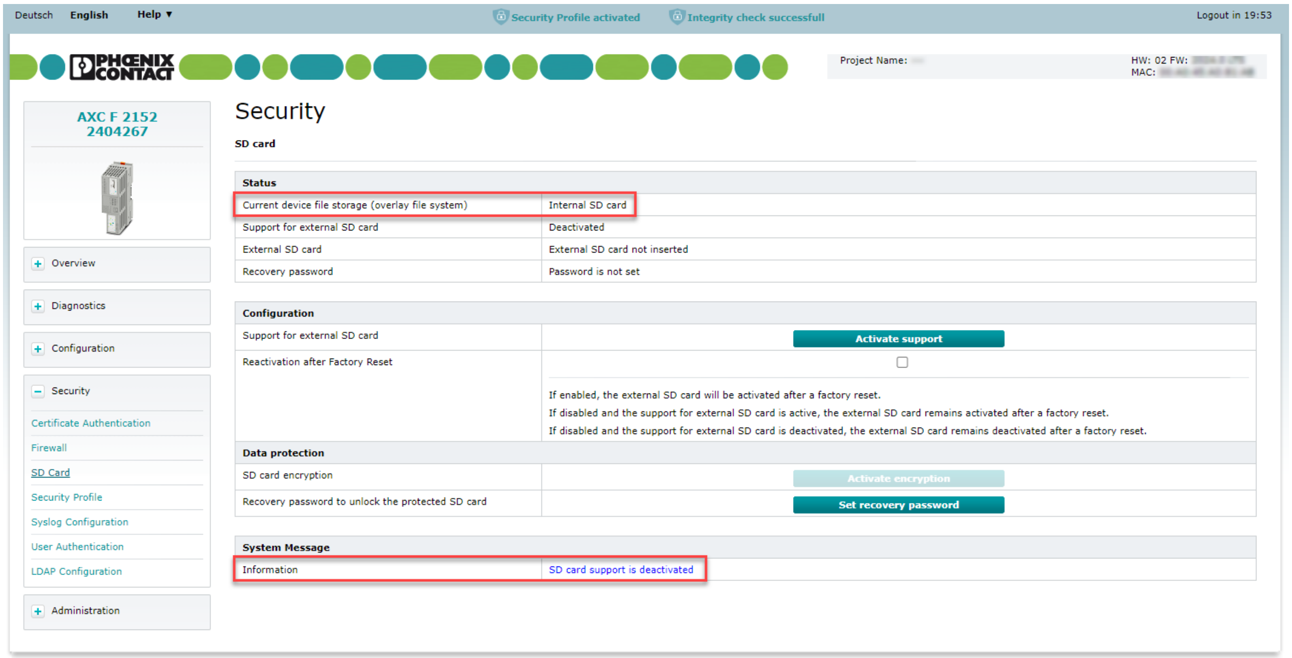
Use without external SD card

- Log in to the WBM.

To ensure that the default Security Profile settings are applied, proceed as follows:

- Open the **SD card** page (**Security** → **SD card**).
- Make sure that only the internal SD card is used to store device files.
- Make sure that the external SD card support is deactivated.

For information on how to deactivate SD card support, refer to the topic SD card encryption.



Project Name: [redacted]

HW: 02 FW: [redacted]
MAC: [redacted]

Security

SD card

Status	
Current device file storage (overlay file system)	Internal SD card
Support for external SD card	Deactivated
External SD card	External SD card not inserted
Recovery password	Password is not set

Configuration	
Support for external SD card	Activate support
Reactivation after Factory Reset	□ If enabled, the external SD card will be activated after a factory reset. If disabled and the support for external SD card is active, the external SD card remains activated after a factory reset. If disabled and the support for external SD card is deactivated, the external SD card remains deactivated after a factory reset.

Data protection	
SD card encryption	Activate encryption
Recovery password to unlock the protected SD card	Set recovery password

System Message	
Information	SD card support is deactivated

Use with external encrypted SD card

Due to the default Security Profile settings, SD card support is also deactivated by default for these controllers. However, you can use an encrypted SD card when using these controllers.

You can only use the following SD cards for encryption:

- SD FLASH 8GB PLCNEXT MEMORY **LIC** (item no. 1151112)
- SD FLASH 32GB PLCNEXT MEMORY **LIC** (item no. 1151111)
- SD FLASH PLCNEXT MEMORY **LIC CFG** (item no. 1308064)

These cards have two partitions: The first partition ("system") is reserved for license handling and a second partition for the controller data. This second partition ("overlay") is encrypted using the WBM.

For the encryption of the SD card, *dm-crypt* with the encryption mode *aes-xts-plain* is used. For secure key derivation, *argon2id* is used.
dm-crypt is a cryptography module of the device mapper in the Linux kernel. *dm-crypt* can encrypt and decrypt data using various algorithms. The encryption can be applied to any device files, in most cases to partitions (as in this case to the "overlay" partition of the SD card).

- Make sure that you only use an encrypted SD card.

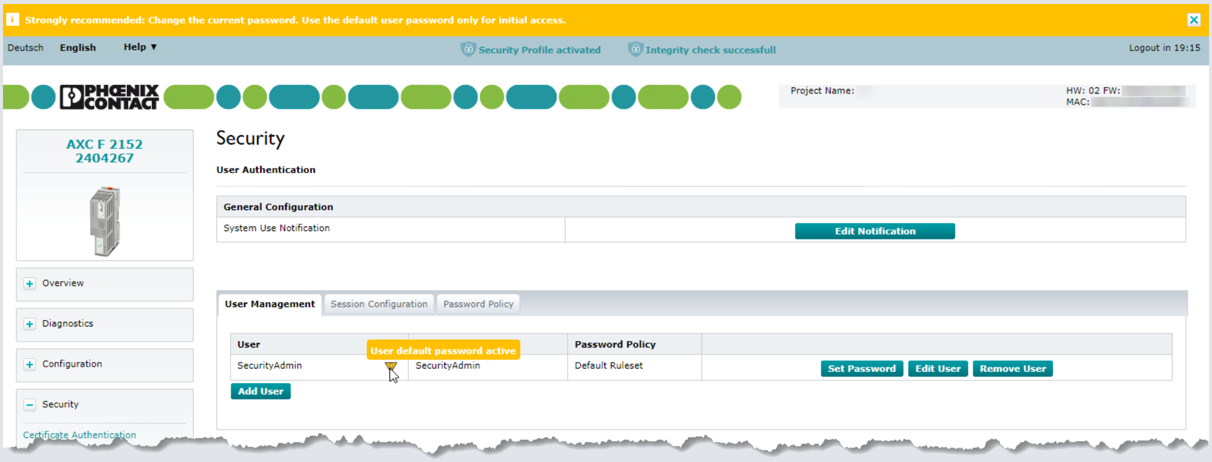
For information on how to activate SD card support and how to encrypt a SD card, refer to the topic SD card encryption.

Creating users

The SecurityAdmin can only configure the system. All other activities must be performed by other users with other roles. You need at least a Security Auditor to access the security notifications, an Engineer to program in PLCnext Engineer and an Operator to operate an HMI. Below you will see how to add these users with their specific roles.

Note: It is strongly recommended that you only use the default user password for the first access. Change the default password immediately after the first access. Observe the password complexity rules .

If you have created a user, you will see a corresponding message in the WBM to change the default password (from firmware 2024.0 LTS).



Strongly recommended: Change the current password. Use the default user password only for initial access.

Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

AXC F 2152
2404267

Security

User Authentication

General Configuration	
System Use Notification	Edit Notification

User		Password Policy	
SecurityAdmin	SecurityAdmin	Default Ruleset	Set Password Edit User Remove User

User default password active

For more information on the different users, roles and rights, refer to the User Authentication topic in the main PLCnext Technology - Info Center.

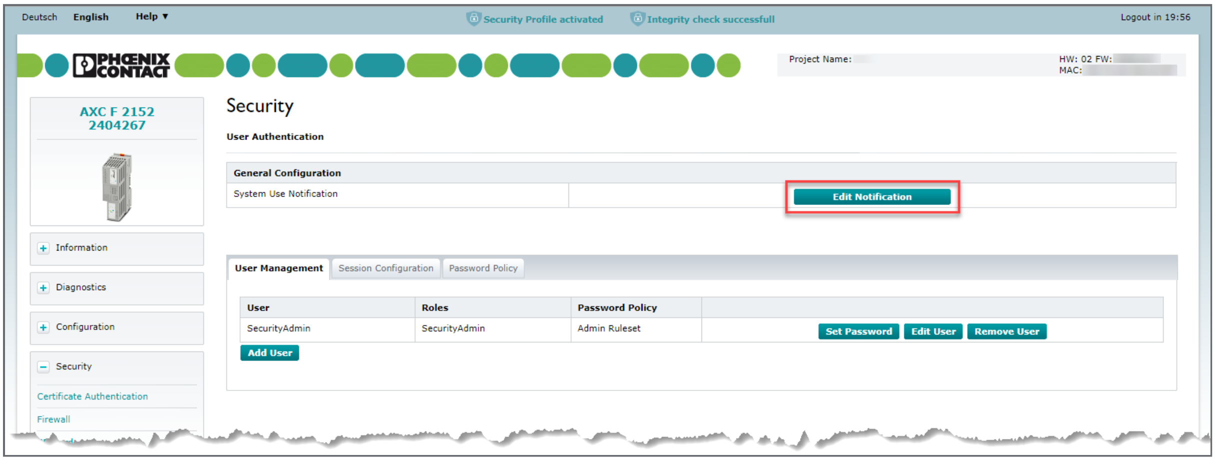
For the following procedures you need **access to the Web-based Management** on the PLCnext Control.

System Use Notification

The system use notification is displayed each time a user wants to log on to the controller. The system use notification is independent of the language of the user interface in WBM and PLCnext Engineer. You should therefore take all required languages into account when editing.

To edit the system use notification, proceed as follows:

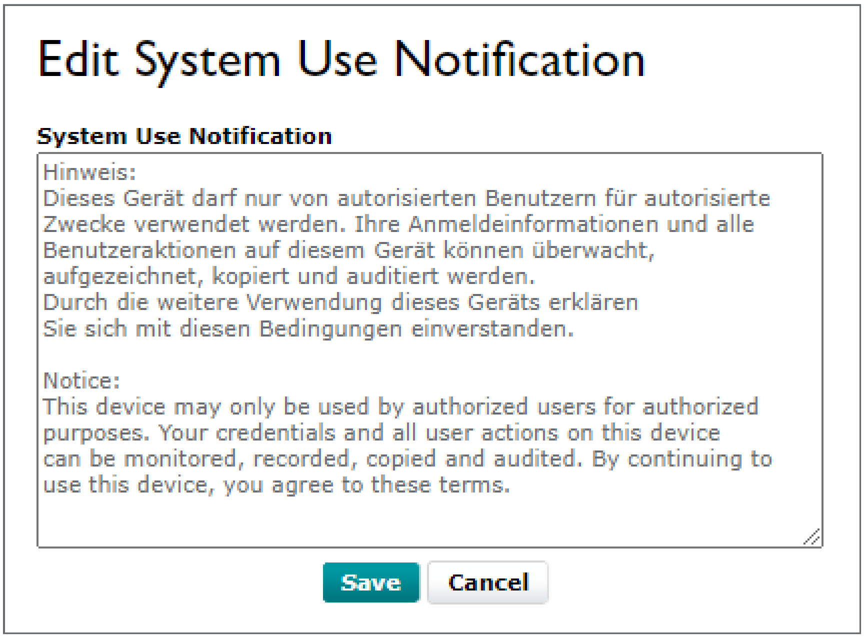
- Click the **Edit Notification** button.



User	Roles	Password Policy
SecurityAdmin	SecurityAdmin	Admin Ruleset

↪ An input window opens.

- Edit the System Use Notification.



Edit System Use Notification

System Use Notification

Hinweis:
Dieses Gerät darf nur von autorisierten Benutzern für autorisierte Zwecke verwendet werden. Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Gerät können überwacht, aufgezeichnet, kopiert und auditiert werden.
Durch die weitere Verwendung dieses Geräts erklären Sie sich mit diesen Bedingungen einverstanden.

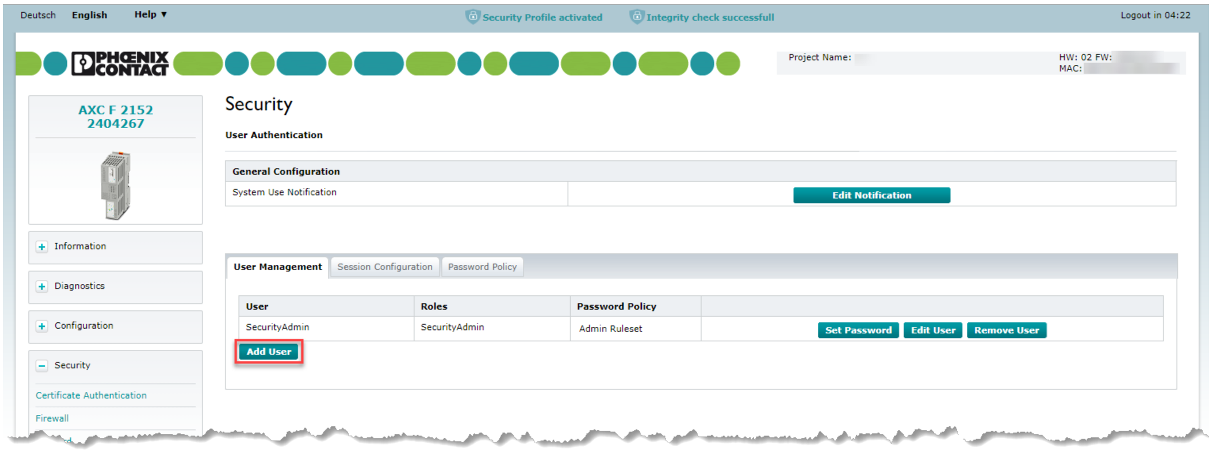
Notice:
This device may only be used by authorized users for authorized purposes. Your credentials and all user actions on this device can be monitored, recorded, copied and audited. By continuing to use this device, you agree to these terms.

- Confirm the entry by clicking the **Save** button.
↪ The text is then transferred to the controller and stored.

Adding a Security Auditor

To add a Security Auditor, proceed as follows:

- Log in to the WBM.
- Open the Security → User Authentication page in the WBM.
- Click the Add User button.



Security

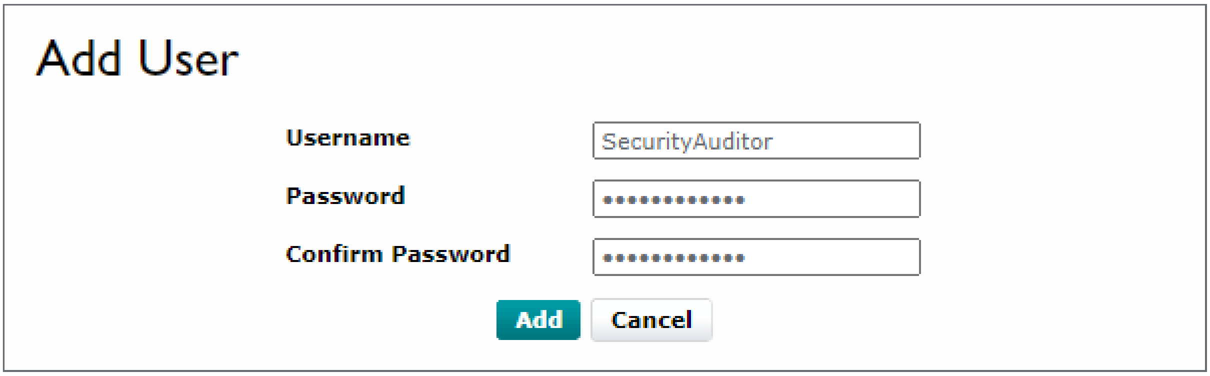
User Authentication

General Configuration	
System Use Notification	

User	Roles	Password Policy
SecurityAdmin	SecurityAdmin	Admin Ruleset

↪ The dialog Add User opens.

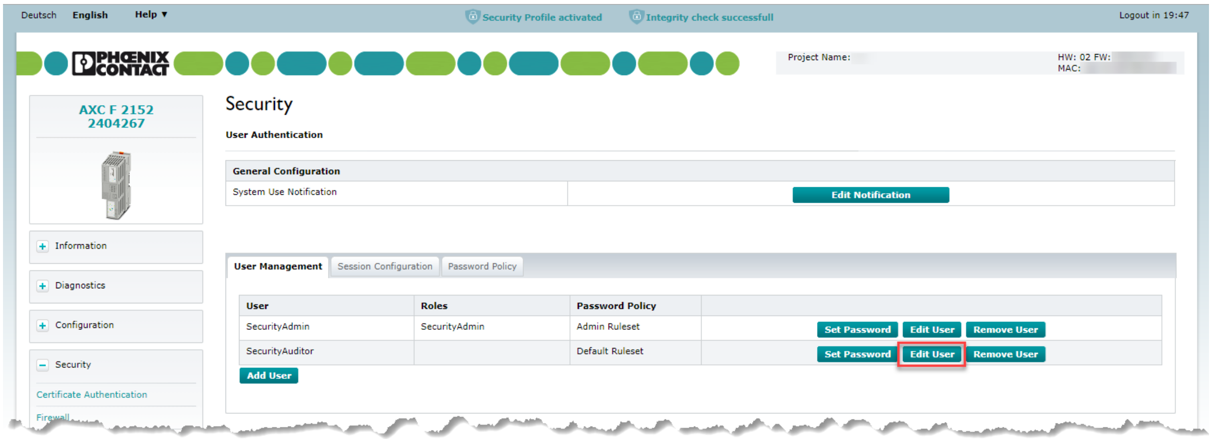
- Enter a username and a password following the password complexity rules.



Add User

Username	SecurityAuditor
Password	●●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●●

- Click the Add button.
- In the added row SecurityAuditor, click the Edit User button.



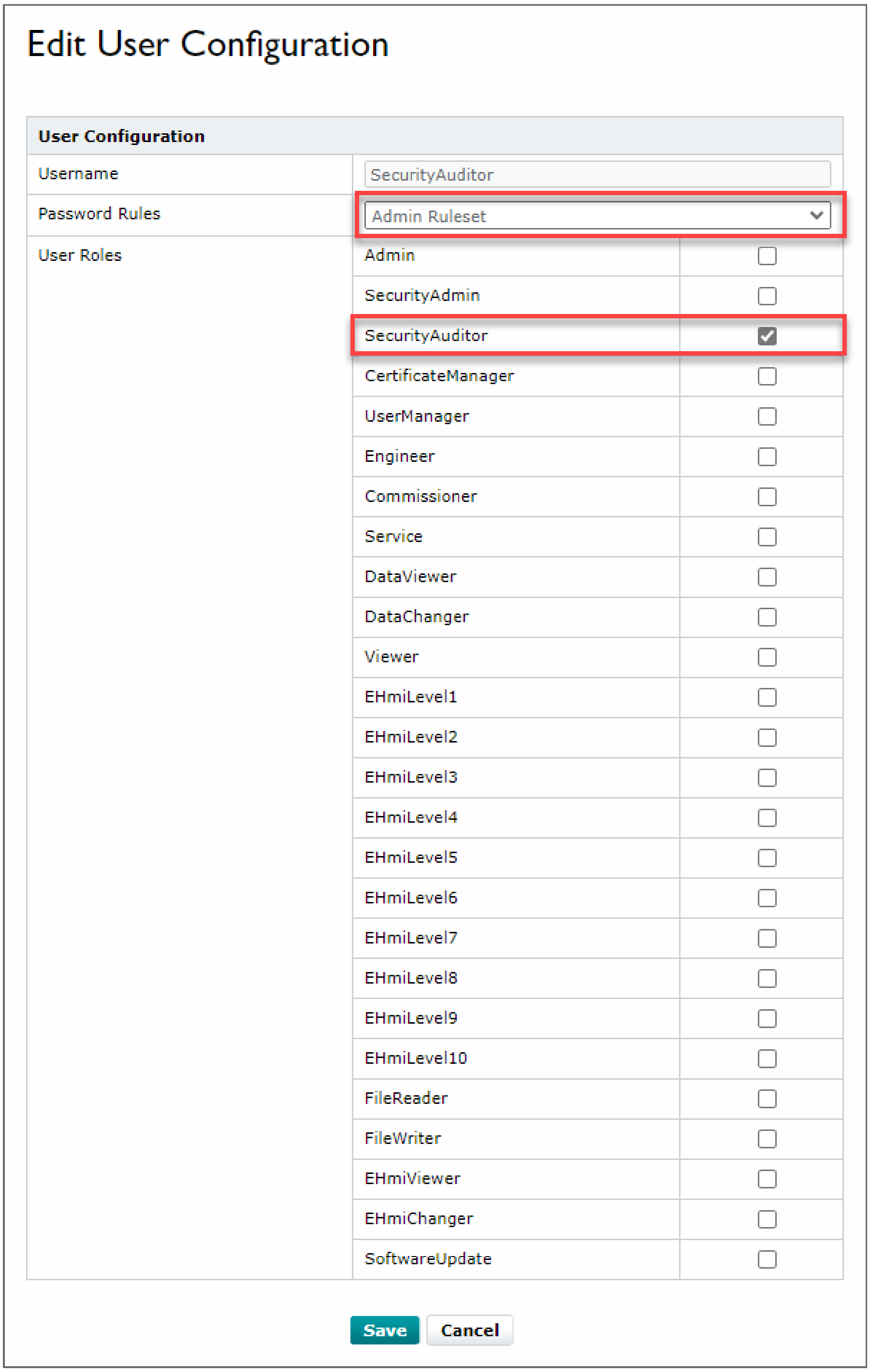
Security

User Authentication

General Configuration	
System Use Notification	

User	Roles	Password Policy
SecurityAdmin	SecurityAdmin	Admin Ruleset
SecurityAuditor		Default Ruleset

- In the dialog that opens, select a ruleset (`Password rules`; we advise the "Admin Ruleset") and the appropriate role (`User Roles`) by activating the checkbox at **SecurityAuditor**.



Edit User Configuration

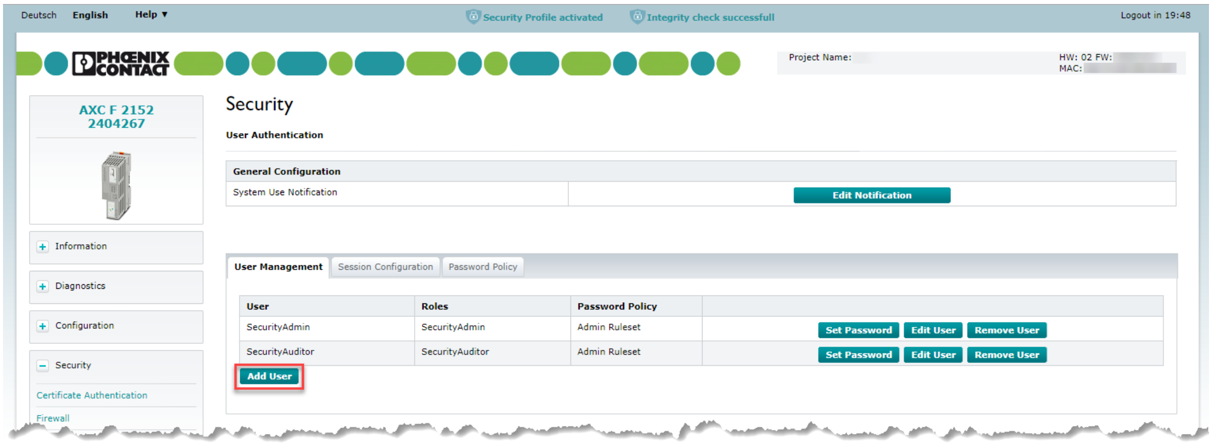
User Configuration		
Username	SecurityAuditor	
Password Rules	Admin Ruleset	
User Roles	Admin	□
	SecurityAdmin	□
	SecurityAuditor	☑
	CertificateManager	□
	UserManager	□
	Engineer	□
	Commissioner	□
	Service	□
	DataViewer	□
	DataChanger	□
	Viewer	□
	EHmiLevel1	□
	EHmiLevel2	□
	EHmiLevel3	□
	EHmiLevel4	□
	EHmiLevel5	□
	EHmiLevel6	□
	EHmiLevel7	□
	EHmiLevel8	□
	EHmiLevel9	□
	EHmiLevel10	□
	FileReader	□
	FileWriter	□
	EHmiViewer	□
	EHmiChanger	□
	SoftwareUpdate	□

- Click the `Save` button.
↪ You've added a Security Auditor.

Adding an Engineer

To add an Engineer, proceed as follows:

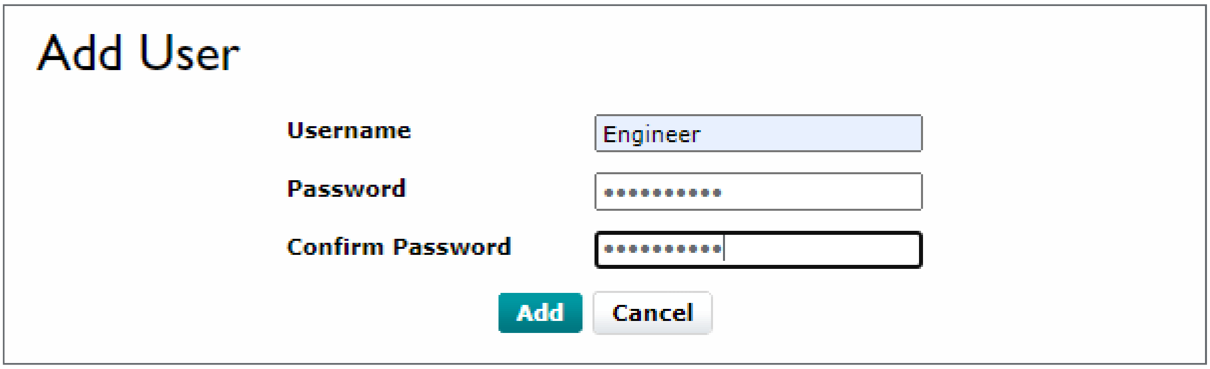
- Log in to the WBM.
- Open the **Security** → **User Authentication** page in the WBM.
- Click the **Add User** button.



User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
SecurityAuditor	SecurityAuditor	Admin Ruleset	Set Password Edit User Remove User

↪ The dialog **Add User** opens.

- Enter a username and a password following the password complexity rules.



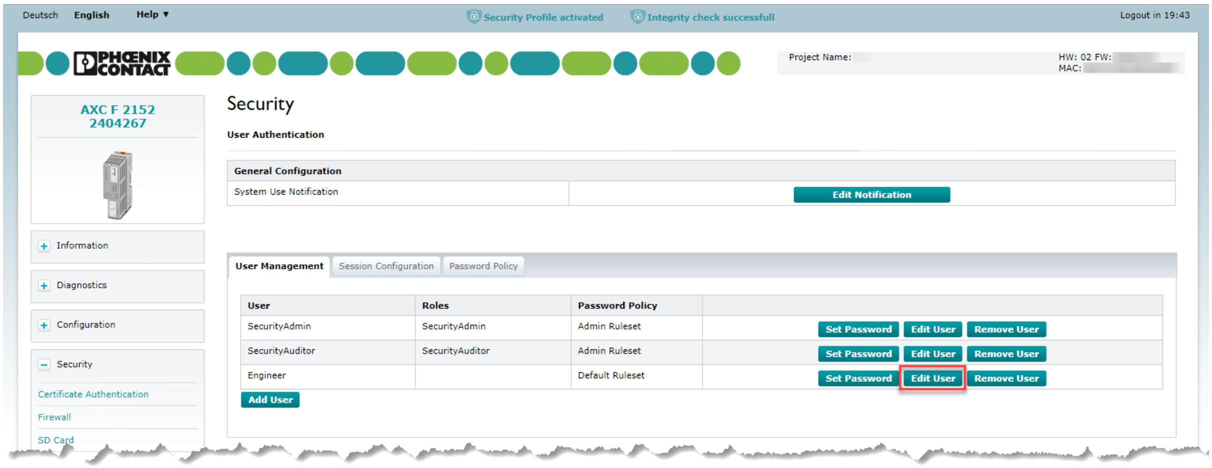
Add User

Username: Engineer

Password: ●●●●●●●●●●

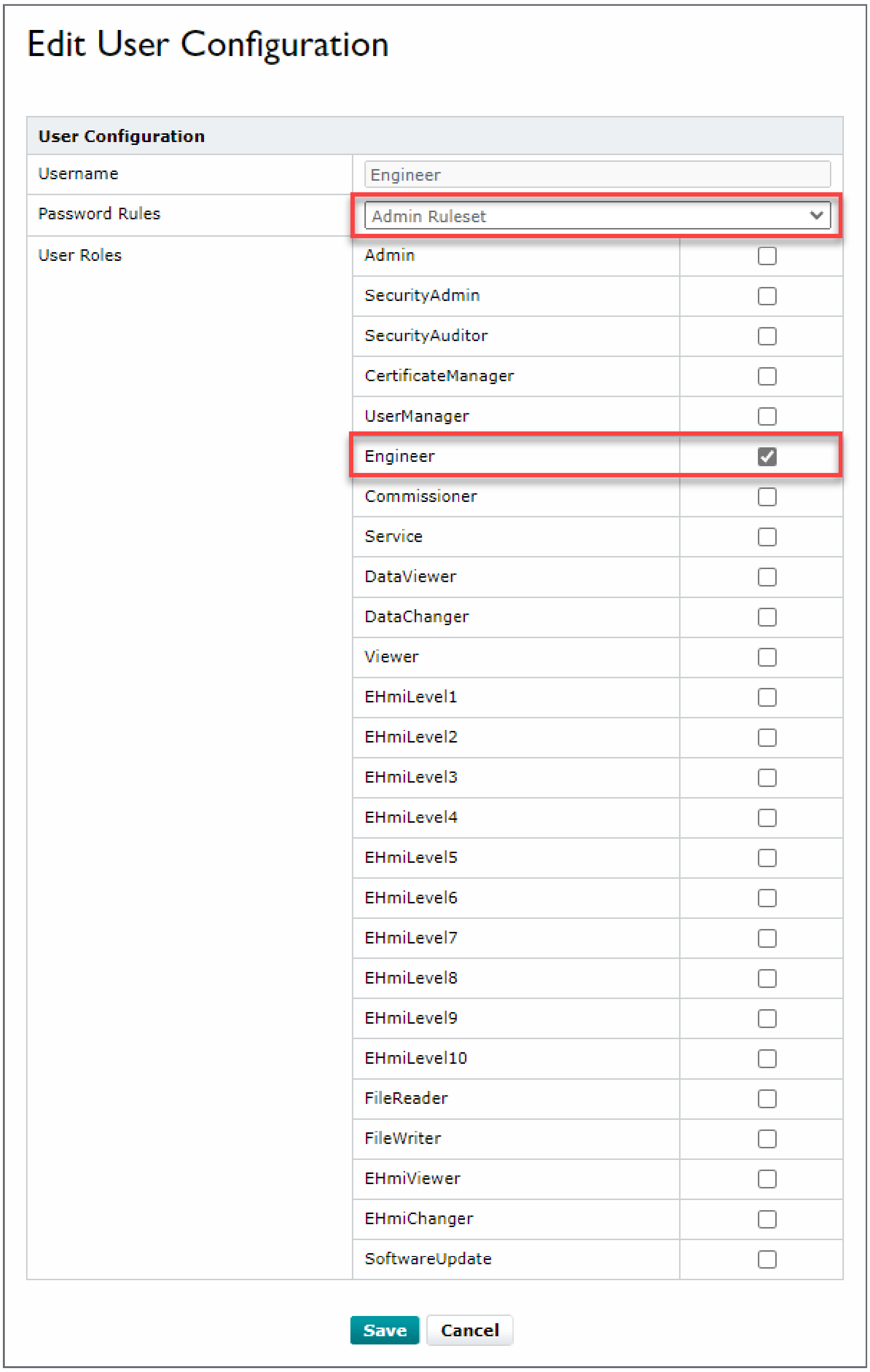
Confirm Password: ●●●●●●●●●●

- Click the **Add** button.
- In the added row **Engineer**, click the **Edit User** button.



User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
SecurityAuditor	SecurityAuditor	Admin Ruleset	Set Password Edit User Remove User
Engineer		Default Ruleset	Set Password Edit User Remove User

- In the dialog that opens, select a ruleset (**Password rules** ; we advise the "Admin Ruleset") and the appropriate role (**User Roles**) by activating the checkbox at **Engineer** .



Edit User Configuration

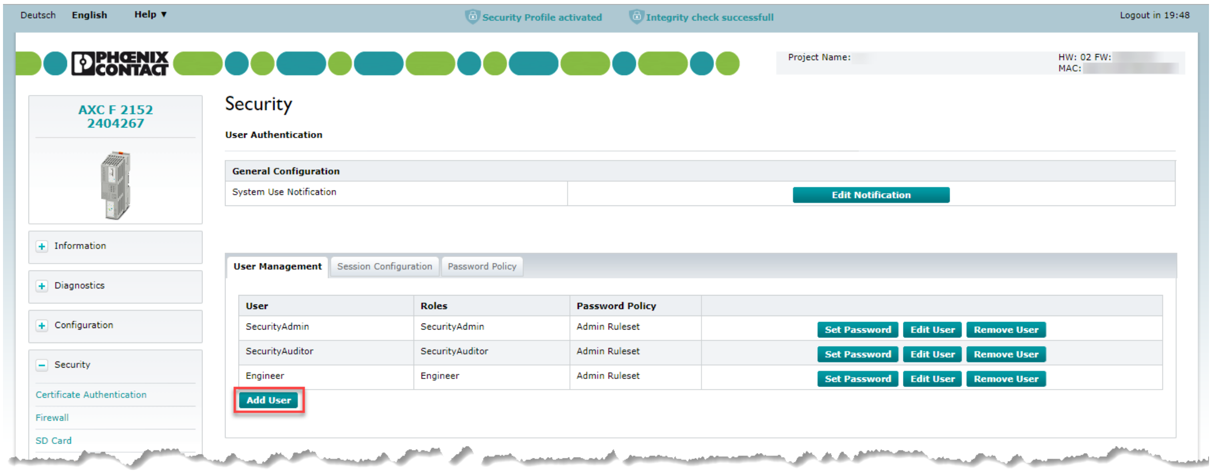
User Configuration		
Username	Engineer	
Password Rules	Admin Ruleset	
User Roles	Admin	☐
	SecurityAdmin	☐
	SecurityAuditor	☐
	CertificateManager	☐
	UserManager	☐
	Engineer	☑
	Commissioner	☐
	Service	☐
	DataViewer	☐
	DataChanger	☐
	Viewer	☐
	EHmiLevel1	☐
	EHmiLevel2	☐
	EHmiLevel3	☐
	EHmiLevel4	☐
	EHmiLevel5	☐
	EHmiLevel6	☐
	EHmiLevel7	☐
	EHmiLevel8	☐
	EHmiLevel9	☐
	EHmiLevel10	☐
	FileReader	☐
	FileWriter	☐
	EHmiViewer	☐
	EHmiChanger	☐
	SoftwareUpdate	☐

- Click the **Save** button.
↪ You've added an Engineer.

Adding an Operator

To add an Engineer, proceed as follows:

- Log in to the WBM.
- Open the Security → User Authentication page in the WBM.
- Click the Add User button.



Security

User Authentication

General Configuration	
System Use Notification	Edit Notification

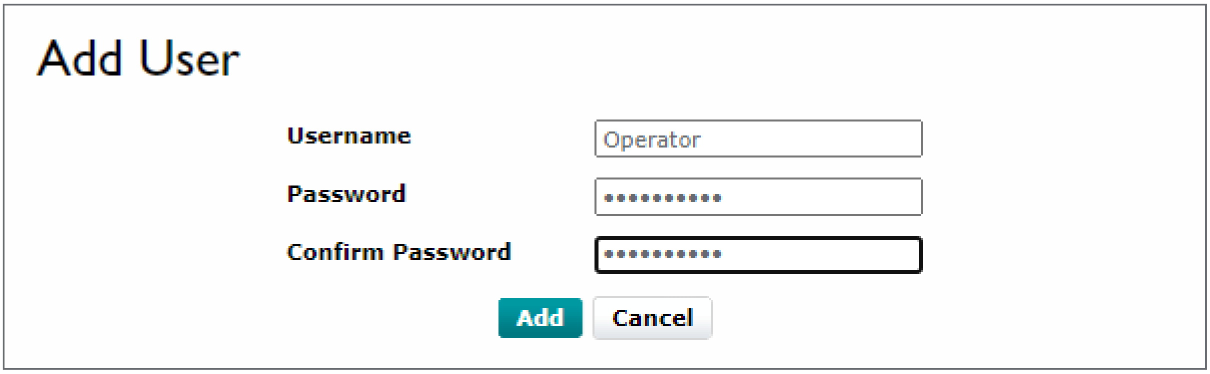
User Management | Session Configuration | Password Policy

User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
SecurityAuditor	SecurityAuditor	Admin Ruleset	Set Password Edit User Remove User
Engineer	Engineer	Admin Ruleset	Set Password Edit User Remove User

Add User

↪ The dialog Add User opens.

- Enter a username and a password following the password complexity rules.



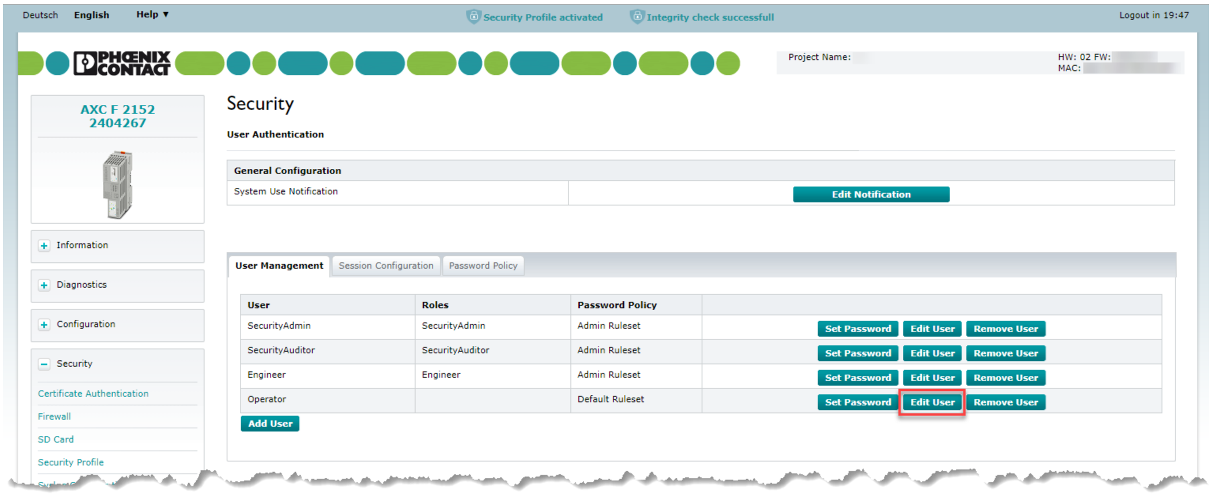
Add User

Username: Operator

Password: ••••••••••

Confirm Password: ••••••••••

- Click the Add button.
- In the added row Operator, click the Edit User button.



Security

User Authentication

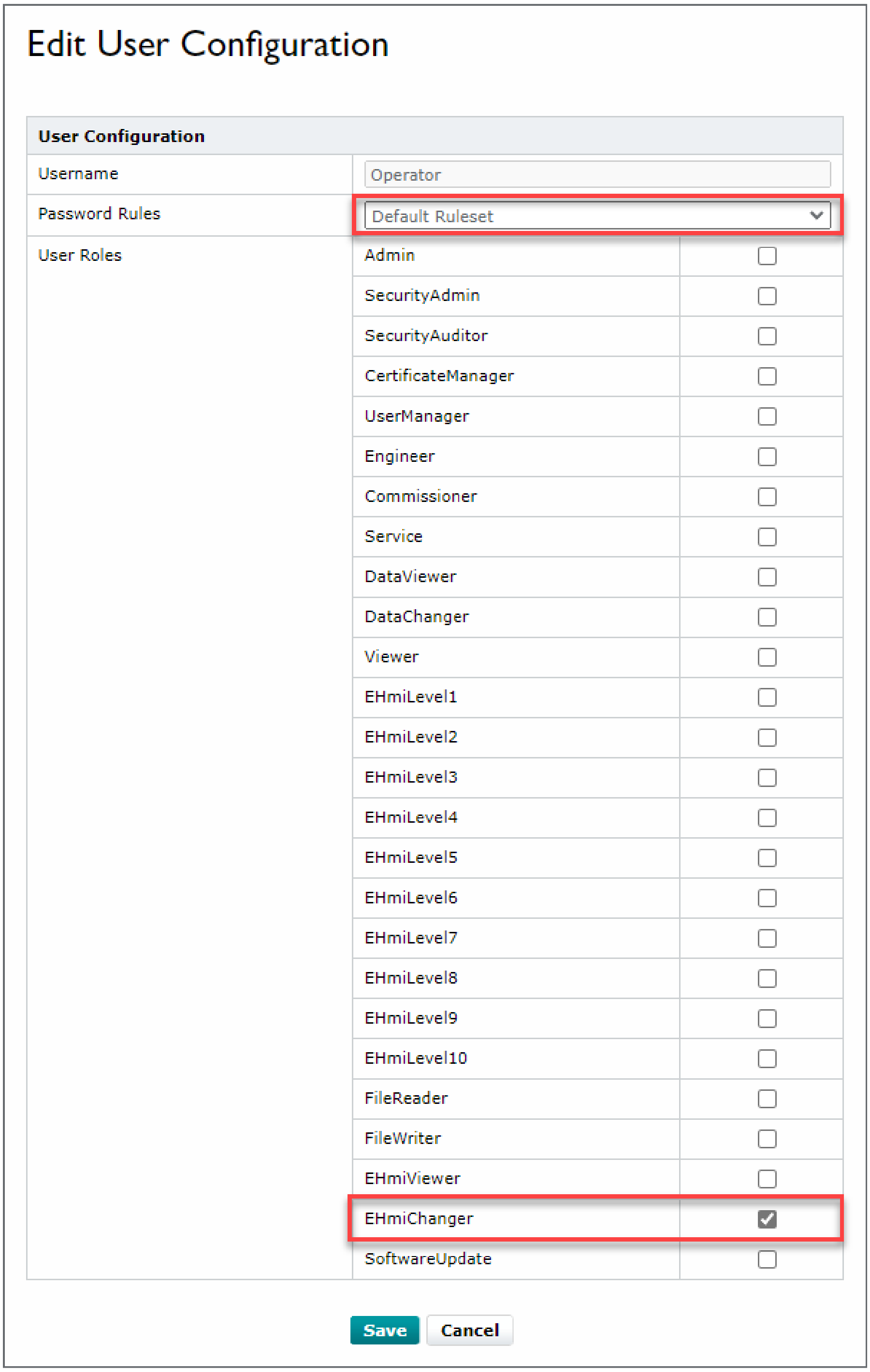
General Configuration	
System Use Notification	Edit Notification

User Management | Session Configuration | Password Policy

User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
SecurityAuditor	SecurityAuditor	Admin Ruleset	Set Password Edit User Remove User
Engineer	Engineer	Admin Ruleset	Set Password Edit User Remove User
Operator		Default Ruleset	Set Password Edit User Remove User

Add User

- In the dialog that opens, select the appropriate role by activating the checkbox at **EHmiChanger**.



Edit User Configuration

User Configuration		
Username	Operator	
Password Rules	Default Ruleset	
User Roles	Admin	□
	SecurityAdmin	□
	SecurityAuditor	□
	CertificateManager	□
	UserManager	□
	Engineer	□
	Commissioner	□
	Service	□
	DataViewer	□
	DataChanger	□
	Viewer	□
	EHmiLevel1	□
	EHmiLevel2	□
	EHmiLevel3	□
	EHmiLevel4	□
	EHmiLevel5	□
	EHmiLevel6	□
	EHmiLevel7	□
	EHmiLevel8	□
	EHmiLevel9	□
	EHmiLevel10	□
	FileReader	□
	FileWriter	□
	EHmiViewer	□
	EHmiChanger	☑
	SoftwareUpdate	□

- Click the **Save** button.
  ↪ You've added an Operator.

Changing the password

Note: Users must change their passwords following the password complexity rules when they log in with their role for the first time.

Adding more users

If necessary, set up additional users. The number and the roles of the respective users depend on your system and the respective application.

Local user management

You can set up the users locally.

However, a global user management via LDAP is possible. When working with multiple devices (more than 3), Phoenix Contact suggests a global, network-based user management via active directory server (LDAP).

ℹ For more information on LDAP, refer to the LDAP connection - file-based configuration topic in the PLCnext Technology - Info Center.

Information about the Admin

Even if the Security Profile is enabled, the Admin is allowed to make changes via SSH, e.g. the Netload Limiter configuration or the VPN configuration. For the commissioning phase it is possible to configure the Admin to make changes to PLCnext Technology configuration files. Afterwards the Admin must be deleted again in the User Manager!

⚠ **CAUTION**

Unauthenticated access

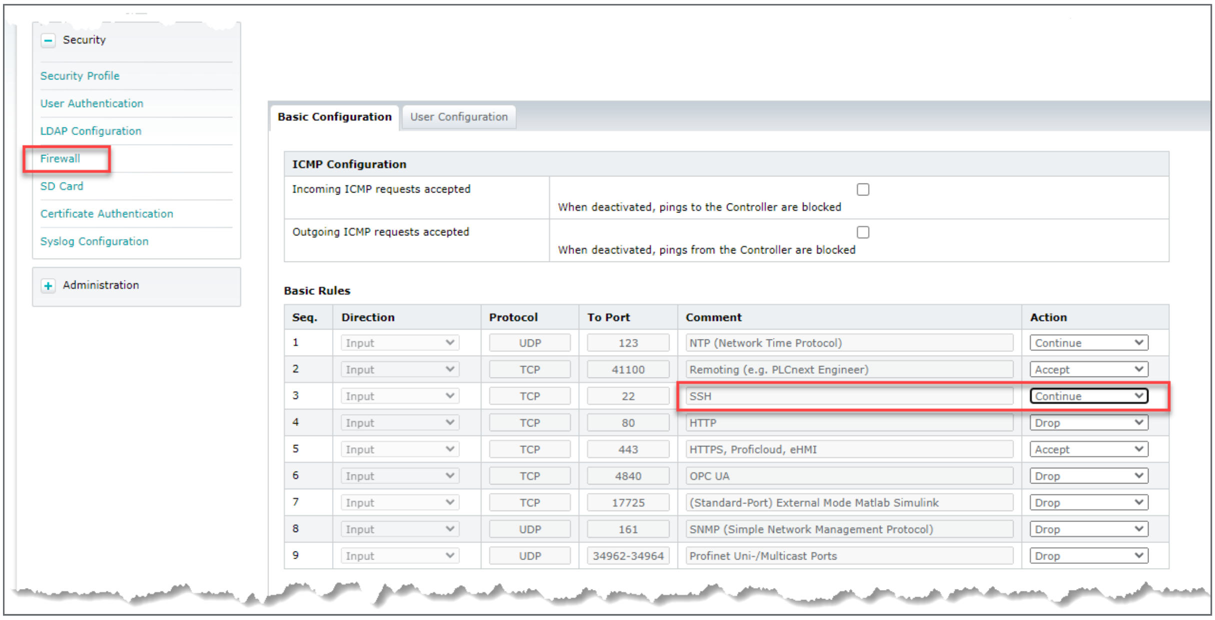
More accesses are possible via the Admin. This can disrupt production and reduce security.

- Do not start any plant with activated Admin!

With the Admin user, you can also use SSH to check the NTP connection. To do this, you must enable SSH in the firewall basic configurations (for more information, refer to the firewall basic configurations) and set an input rule:

...continuation see next page...

Basic Configuration:



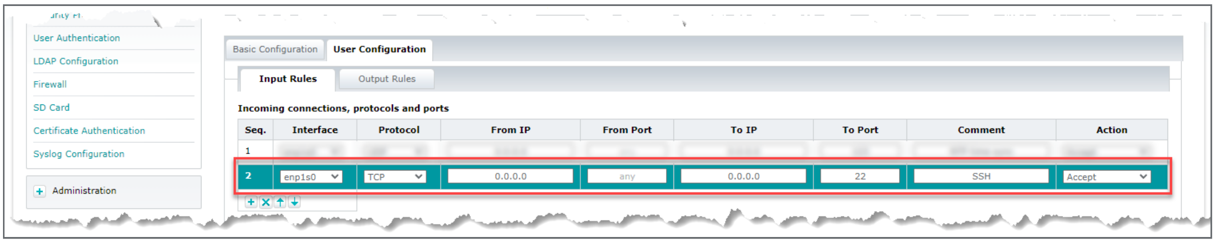
ICMP Configuration

Incoming ICMP requests accepted	□ When deactivated, pings to the Controller are blocked
Outgoing ICMP requests accepted	□ When deactivated, pings from the Controller are blocked

Basic Rules

Seq.	Direction	Protocol	To Port	Comment	Action
1	Input	UDP	123	NTP (Network Time Protocol)	Continue
2	Input	TCP	41100	Remoting (e.g. PLCnext Engineer)	Accept
3	Input	TCP	22	SSH	Continue
4	Input	TCP	80	HTTP	Drop
5	Input	TCP	443	HTTPS, Proficloud, eHMI	Accept
6	Input	TCP	4840	OPC UA	Drop
7	Input	TCP	17725	(Standard-Port) External Mode Matlab Simulink	Drop
8	Input	UDP	161	SNMP (Simple Network Management Protocol)	Drop
9	Input	UDP	34962-34964	Profinet Uni-/Multicast Ports	Drop

Input Rule:

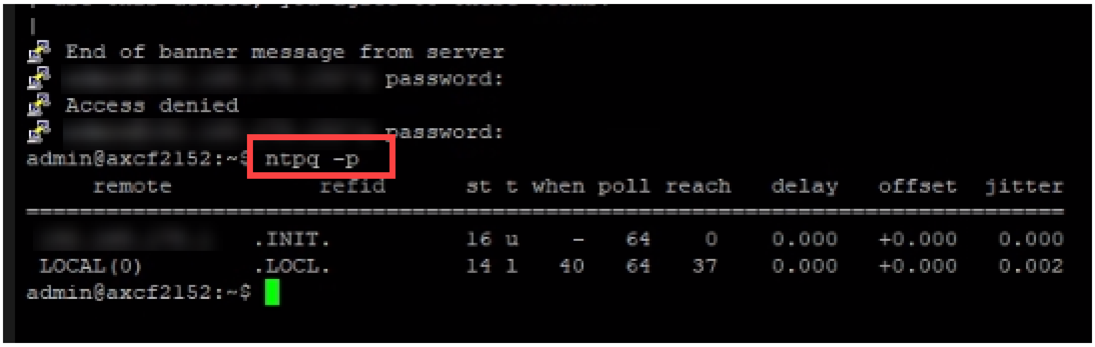


Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
2	enp1s0	TCP	0.0.0.0	any	0.0.0.0	22	SSH	Accept

Note: Configure the IP addresses in the firewall so that SSH access can only take place from the defined device.

Using the console, you can now check whether the connection has been established by using the `ntpq -p` command.



```
End of banner message from server
[redacted] password:
Access denied
[redacted] password:
admin@axcf2152:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 [redacted]         .INIT.          16 u    -   64    0    0.000   +0.000   0.000
 LOCAL(0)        .LOCL.          14 l   40   64   37    0.000   +0.000   0.002
admin@axcf2152:~$
```

Checking password validity in the WBM

- Log in to the WBM.
- Open the **Cockpit** page (**Diagnostics** → **Cockpit**) in the WBM.

Based on the messages, you can check whether the passwords are still valid and whether a user has already changed his default password.

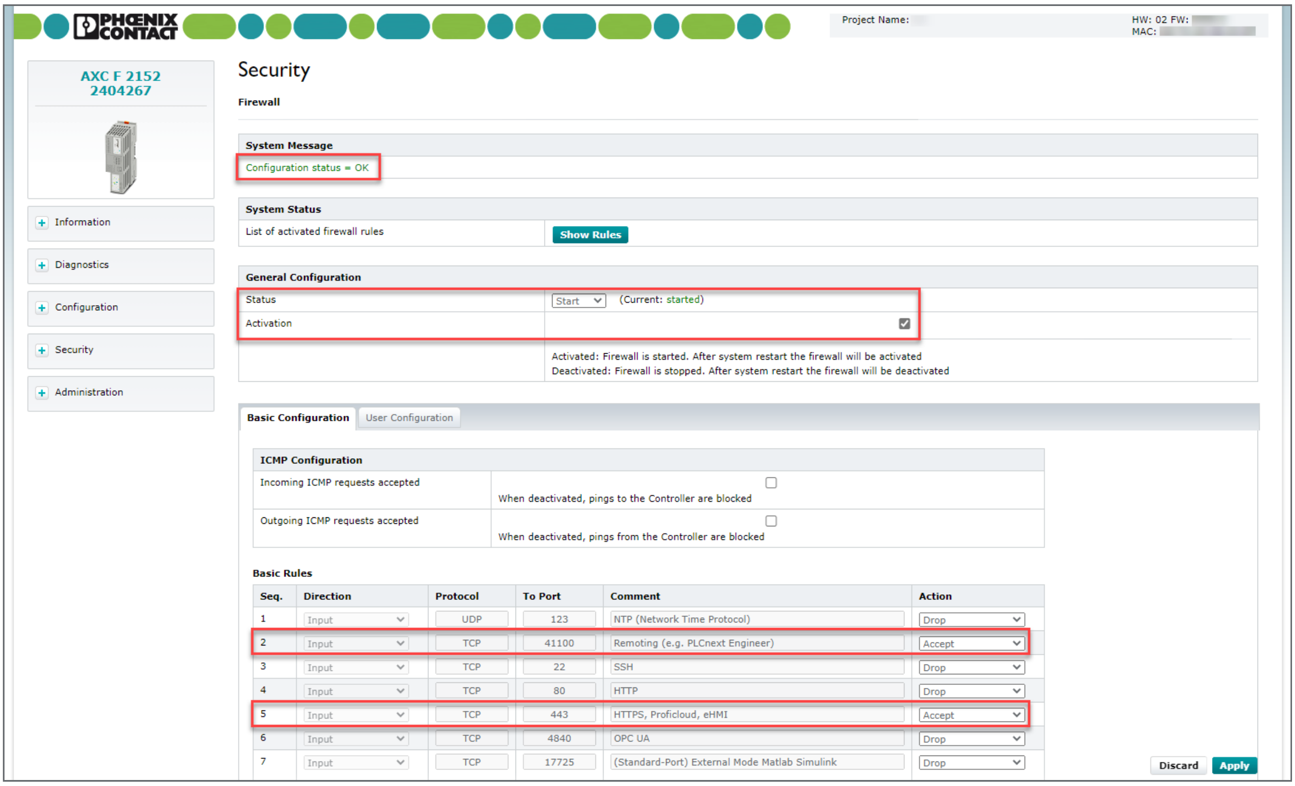
Configuring basic firewall settings

ℹ For basic firewall configuration information, refer to the Firewall WBM topic in the main PLCnext Technology - Info Center.

- Log in to the WBM.
- Open the **Firewall** page (**Security** → **Firewall**) in the WBM.
- Check in the **System Messages** section whether the Configuration status is OK.
- Check in the **General Configuration** section whether the Status is "Start (Current: started)" and the Checkbox "Activation" is activated.
- Check in the **Basic Rules** section whether only the following incoming connections are enabled:

Description	Protocol	Port
Common remoting, e.g., using PLCnext Engineer	TCP	Port 41100
HTTPS, web server for eHMI and WBM	TCP	Port 443

- Optional: Export the list of activated firewall rules. This may be helpful if you want to save the firewall rules in your plant documentation. For information on how to proceed with that, refer to the Firewall WBM topic in the main PLCnext Technology - Info Center.



Security

Firewall

System Message

Configuration status = OK

System Status

List of activated firewall rules — Show Rules

General Configuration

Status	Start (Current: started)
Activation	☑
	Activated: Firewall is started. After system restart the firewall will be activated Deactivated: Firewall is stopped. After system restart the firewall will be deactivated

ICMP Configuration

Incoming ICMP requests accepted	☐ When deactivated, pings to the Controller are blocked
Outgoing ICMP requests accepted	☐ When deactivated, pings from the Controller are blocked

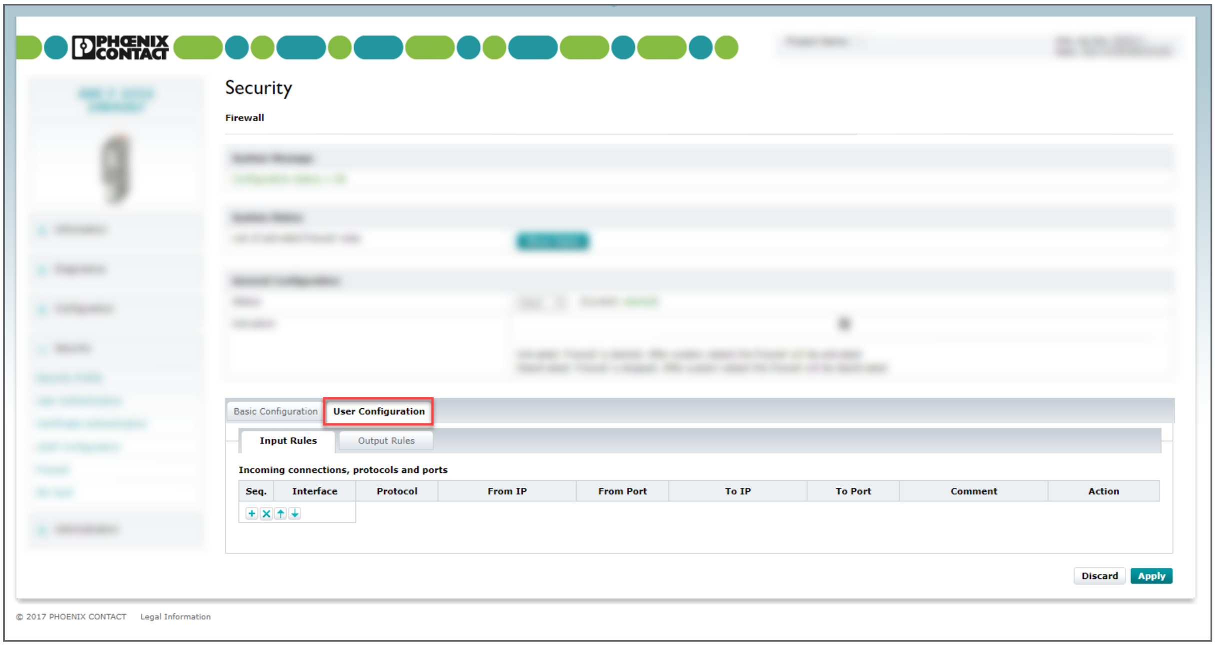
Basic Rules

Seq.	Direction	Protocol	To Port	Comment	Action
1	Input	UDP	123	NTP (Network Time Protocol)	Drop
2	Input	TCP	41100	Remoting (e.g. PLCnext Engineer)	Accept
3	Input	TCP	22	SSH	Drop
4	Input	TCP	80	HTTP	Drop
5	Input	TCP	443	HTTPS, Proficloud, eHMI	Accept
6	Input	TCP	4840	OPC UA	Drop
7	Input	TCP	17725	(Standard-Port) External Mode Matlab Simulink	Drop

...continuation see next page...

- Check whether further user-defined settings are necessary for your application.
- If you need to allow further ports, open the **User Configuration** tab.

  ℹ For further information see Configuring extended firewall settings topic in this PLCnext Technology - Security Info Center.



Security

Firewall

Incoming connections, protocols and ports

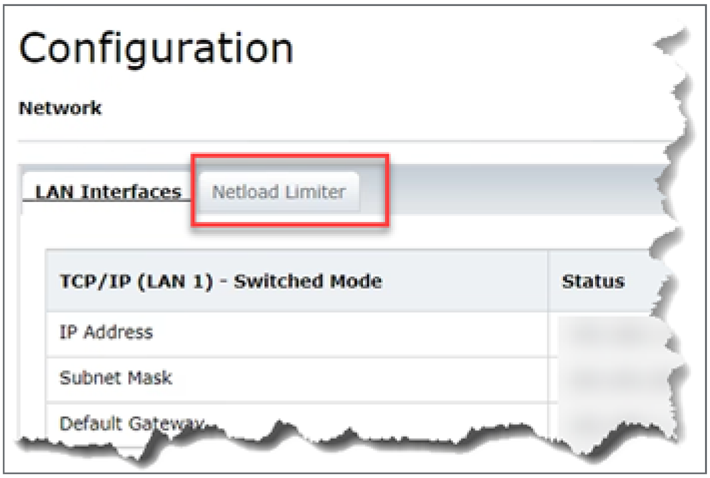
Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action

© 2017 PHOENIX CONTACT Legal Information

Configuring Netload Limiter

You configure the Netload Limiter on the **Network** page (**Configuration** → **Network**) in the WBM.

- Log in to the WBM.
- Open the **Netload Limiter** tab.



Configuration

Network

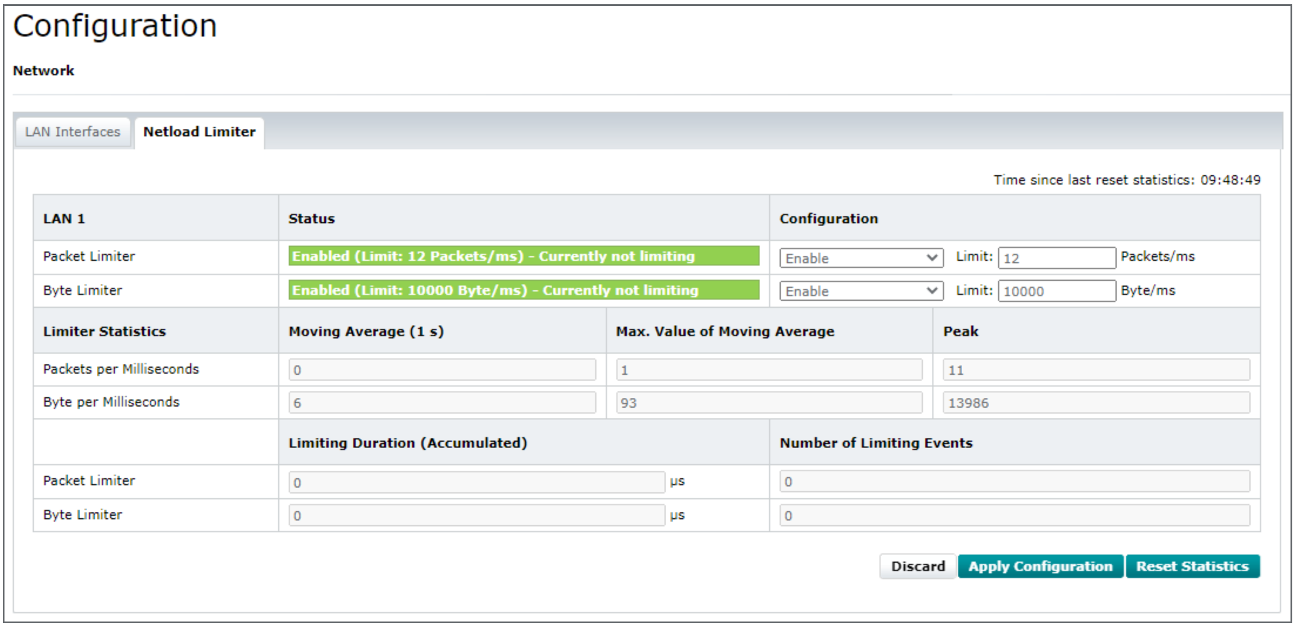
TCP/IP (LAN 1) - Switched Mode	Status
IP Address	
Subnet Mask	
Default Gateway	

Note:

- The **Time since last reset statistics** counter in the upper-right corner of this WBM page shows the time that has elapsed since the last reset of the statistics.
- Statistics are always collected, even if no limiter is enabled.
- Statistics are not reset by applying a configuration change.
- The **Reset Statistics** button resets the enabled packet and byte counters in this WBM page as well as the **Time since last reset statistics** time counter. It does not reset the controller. However, when resetting the controller, the enabled counters in this WBM page are restarting, too.

...continuation see next page...

When the Packet Limiter or Byte Limiter is enabled but currently not limiting, the status is highlighted **green**:



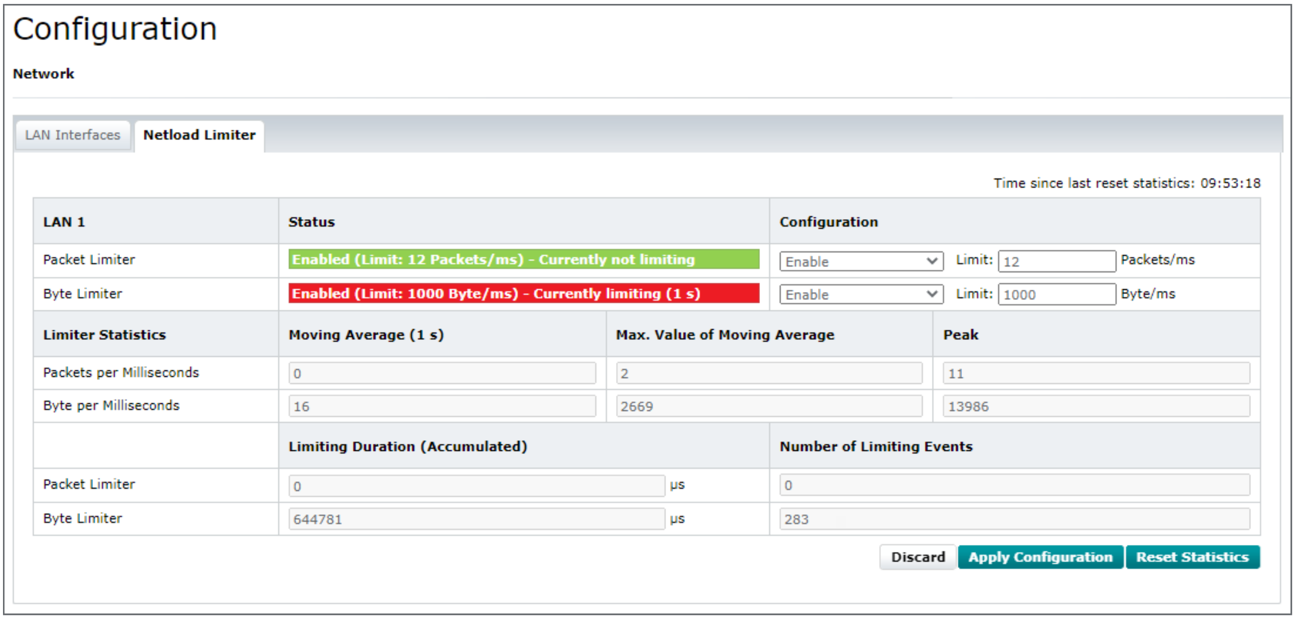
Configuration

Network

Time since last reset statistics: 09:48:49

LAN 1	**Status**	**Configuration**	
Packet Limiter	Enabled (Limit: 12 Packets/ms) - Currently not limiting	Enable Limit: 12 Packets/ms	
Byte Limiter	Enabled (Limit: 10000 Byte/ms) - Currently not limiting	Enable Limit: 10000 Byte/ms	
Limiter Statistics	**Moving Average (1 s)**	**Max. Value of Moving Average**	**Peak**
Packets per Milliseconds	0	1	11
Byte per Milliseconds	6	93	13986
	Limiting Duration (Accumulated)	**Number of Limiting Events**	
Packet Limiter	0 µs	0	
Byte Limiter	0 µs	0	

When a limiter is enabled and currently limiting, the status shows a **red** marker for the limiter in question:



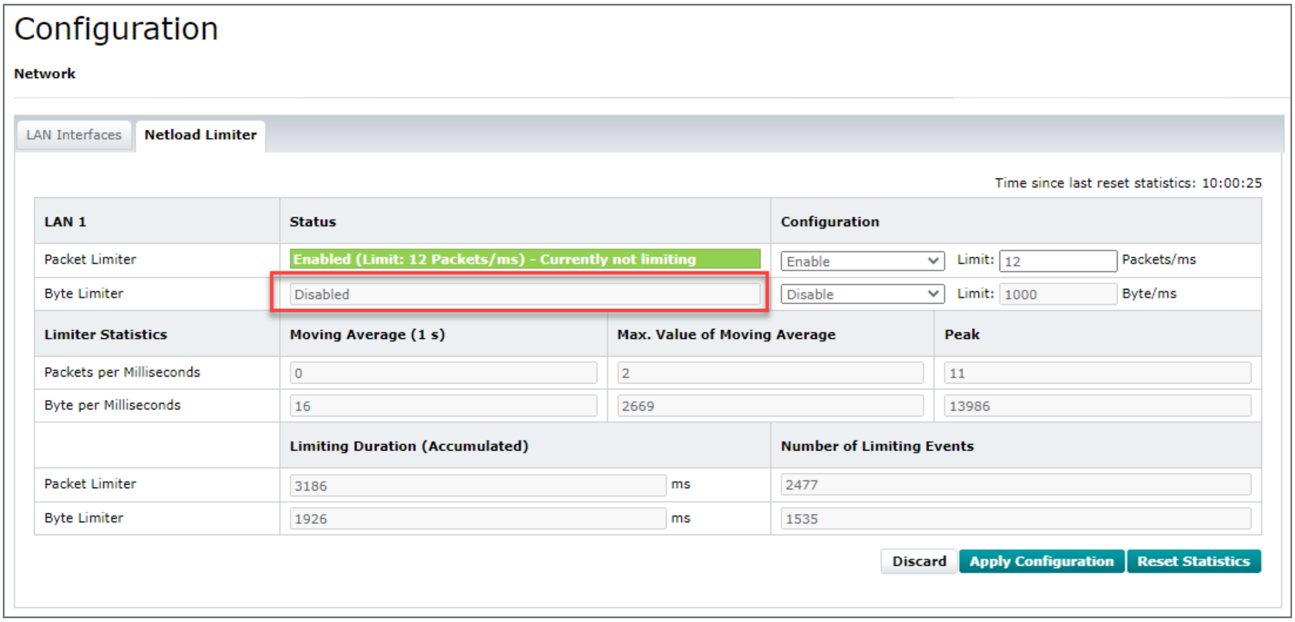
Configuration

Network

Time since last reset statistics: 09:53:18

LAN 1	**Status**	**Configuration**	
Packet Limiter	Enabled (Limit: 12 Packets/ms) - Currently not limiting	Enable Limit: 12 Packets/ms	
Byte Limiter	Enabled (Limit: 1000 Byte/ms) - Currently limiting (1 s)	Enable Limit: 1000 Byte/ms	
Limiter Statistics	**Moving Average (1 s)**	**Max. Value of Moving Average**	**Peak**
Packets per Milliseconds	0	2	11
Byte per Milliseconds	16	2669	13986
	Limiting Duration (Accumulated)	**Number of Limiting Events**	
Packet Limiter	0 µs	0	
Byte Limiter	644781 µs	283	

You can disable one limiter while leaving the other limiter enabled:



Configuration

Network

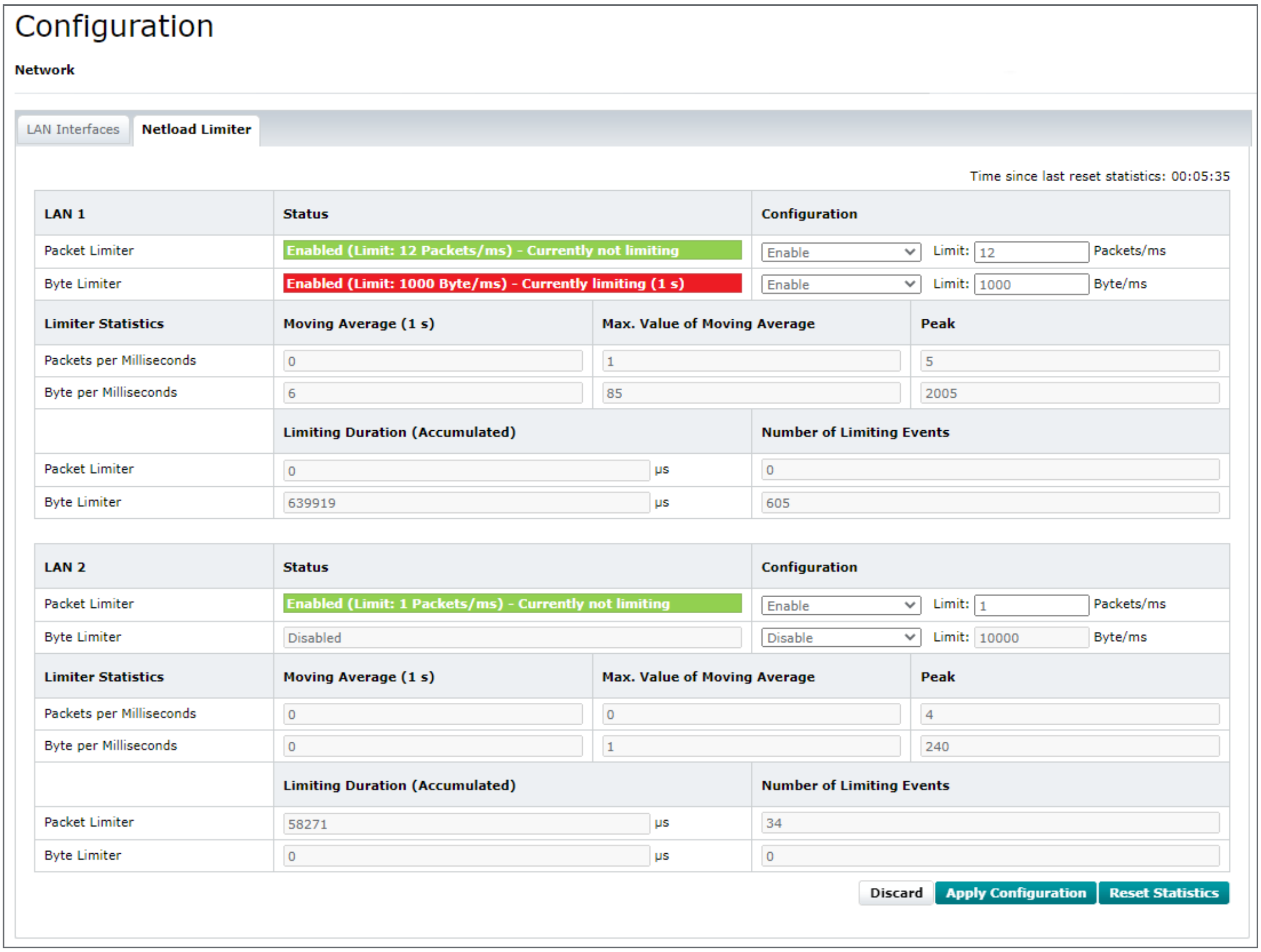
Time since last reset statistics: 10:00:25

LAN 1	Status	Configuration
Packet Limiter	Enabled (Limit: 12 Packets/ms) - Currently not limiting	Enable Limit: 12 Packets/ms
Byte Limiter	Disabled	Disable Limit: 1000 Byte/ms

Limiter Statistics	Moving Average (1 s)	Max. Value of Moving Average	Peak
Packets per Milliseconds	0	2	11
Byte per Milliseconds	16	2669	13986

	Limiting Duration (Accumulated)	Number of Limiting Events
Packet Limiter	3186 ms	2477
Byte Limiter	1926 ms	1535

If you're using the AXC F 2152 with the left-aligned AXC F XT ETH 1TX Ethernet module (mandatory in the security context for network segmentation), it may look like this:



Configuration

Network

Time since last reset statistics: 00:05:35

LAN 1	Status	Configuration
Packet Limiter	Enabled (Limit: 12 Packets/ms) - Currently not limiting	Enable Limit: 12 Packets/ms
Byte Limiter	Enabled (Limit: 1000 Byte/ms) - Currently limiting (1 s)	Enable Limit: 1000 Byte/ms

Limiter Statistics	Moving Average (1 s)	Max. Value of Moving Average	Peak
Packets per Milliseconds	0	1	5
Byte per Milliseconds	6	85	2005

	Limiting Duration (Accumulated)	Number of Limiting Events
Packet Limiter	0 µs	0
Byte Limiter	639919 µs	605

LAN 2	Status	Configuration
Packet Limiter	Enabled (Limit: 1 Packets/ms) - Currently not limiting	Enable Limit: 1 Packets/ms
Byte Limiter	Disabled	Disable Limit: 10000 Byte/ms

Limiter Statistics	Moving Average (1 s)	Max. Value of Moving Average	Peak
Packets per Milliseconds	0	0	4
Byte per Milliseconds	0	1	240

	Limiting Duration (Accumulated)	Number of Limiting Events
Packet Limiter	58271 µs	34
Byte Limiter	0 µs	0

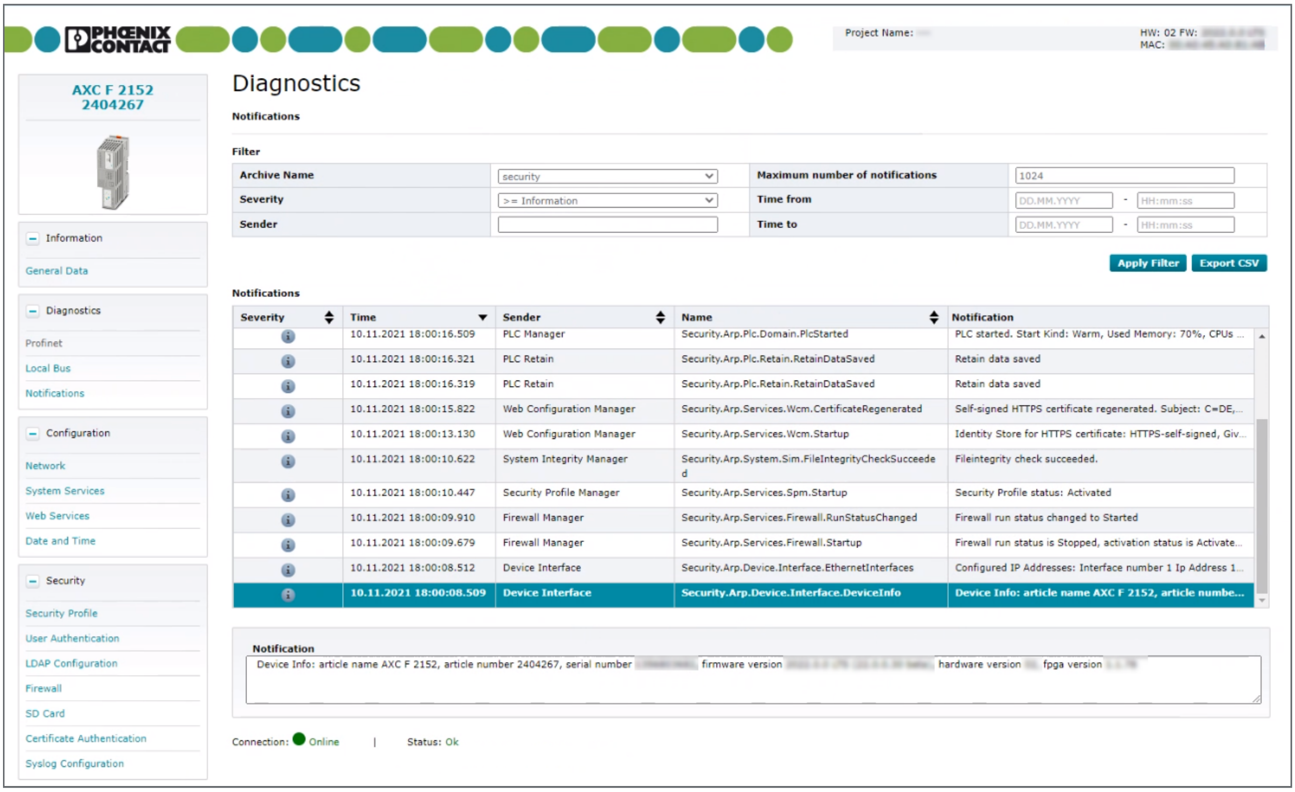
Security logging

- Log in to the WBM.
- Open the **Notifications** page (**Diagnostics** → **Notifications**).

Note: Only the SecurityAdmin and the SecurityAuditor have access to the notifications.

The UserManager assigns a session ID to each user who logs in. The session ID is displayed at the corresponding notifications for all activities. The SecurityAdmin and the SecurityAuditor have access to the security logging. On the basis of the notifications it is possible to see how the PLCnext Control is booted (whether the integrity is given) and general information about all activities of the logged-in users (who changed what when and how) in the sense of non-repudiation according to IEC 62443.

i For more information on security logging, refer to the topic Configuring central logging.



Diagnostics

Notifications

Filter

Archive Name	security	Maximum number of notifications	1024
Severity	>= Information	Time from	DD.MM.YYYY - HH:mm:ss
Sender		Time to	DD.MM.YYYY - HH:mm:ss

Apply Filter · Export CSV

Notifications

Severity	Time	Sender	Name	Notification
i	10.11.2021 18:00:16.509	PLC Manager	Security.Arp.Plc.Domain.PlcStarted	PLC started. Start Kind: Warm, Used Memory: 70%, CPUs ...
i	10.11.2021 18:00:16.321	PLC Retain	Security.Arp.Plc.Retain.RetainDataSaved	Retain data saved
i	10.11.2021 18:00:16.319	PLC Retain	Security.Arp.Plc.Retain.RetainDataSaved	Retain data saved
i	10.11.2021 18:00:15.822	Web Configuration Manager	Security.Arp.Services.Wcm.CertificateRegenerated	Self-signed HTTPS certificate regenerated. Subject: C=DE,...
i	10.11.2021 18:00:13.130	Web Configuration Manager	Security.Arp.Services.Wcm.Startup	Identity Store for HTTPS certificate: HTTPS-self-signed, Giv...
i	10.11.2021 18:00:10.622	System Integrity Manager	Security.Arp.System.Sim.FileIntegrityCheckSucceeded	Fileintegrity check succeeded.
i	10.11.2021 18:00:10.447	Security Profile Manager	Security.Arp.Services.Spm.Startup	Security Profile status: Activated
i	10.11.2021 18:00:09.910	Firewall Manager	Security.Arp.Services.Firewall.RunStatusChanged	Firewall run status changed to Started
i	10.11.2021 18:00:09.679	Firewall Manager	Security.Arp.Services.Firewall.Startup	Firewall run status is Stopped, activation status is Activate...
i	10.11.2021 18:00:08.512	Device Interface	Security.Arp.Device.Interface.EthernetInterfaces	Configured IP Addresses: Interface number 1 Ip Address 1...
i	**10.11.2021 18:00:08.509**	**Device Interface**	**Security.Arp.Device.Interface.DeviceInfo**	**Device Info: article name AXC F 2152, article numbe...**

Notification

Device Info: article name AXC F 2152, article number 2404267, serial number [redacted] firmware version [redacted] hardware version [redacted] fpga version [redacted]

Connection: ● Online | Status: Ok

Note: To see all messages and remove the filter, clear the box at "Sender" and then click **Apply Filter**.

Ensuring audit storage capacity

Notification Manager: Configurable file size (default 10 MB) when limit reached configurable number of messages are deleted (default 16). Security messages are hand over to syslog. Logrotate is executed every hour. Syslog-ng interface for external logging can be configured.

PLCnext environmental requirements

PLCnext environmental requirements

Operating a PLCnext Control in a security context includes the following steps regarding environmental requirements:

- Configuring PLCnext Engineer
- Checking project data integrity
- Configuring extended firewall settings
- Configuring the system time
- Configuring central logging
- Activating OPC UA Server
- Activating OPC UA Client
- Activating HMI
- Activating PROFINET®
- Activating the App Manager
- Activating software updates
- Performing backup and restore

Configuring PLCnext Engineer

ℹ For information on how to use PLCnext Engineer or how to create a project, refer to the Getting started with PLCnext Engineer topic in the main PLCnext Technology - Info Center.

- Open PLCnext Engineer.
- Open the project that you want to transfer to the PLCnext Control.

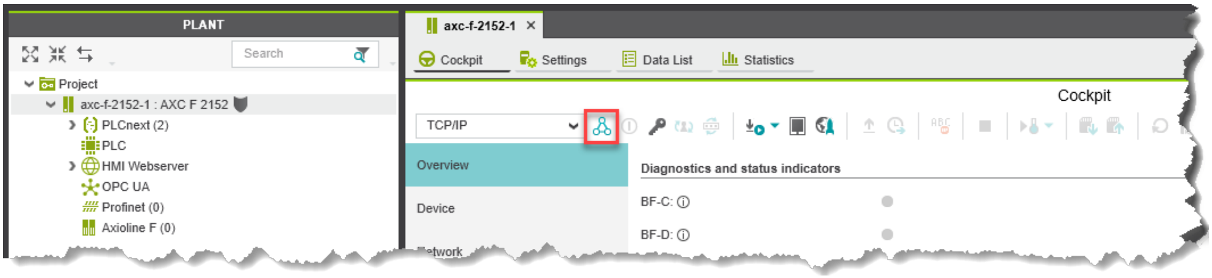
Note: You may need to assign the correct IP addresses before connecting to the controller. Please note the following points:

- First set the IP address range, then the IP address for the expansion module.
- Only release the subnet range that you actually need.

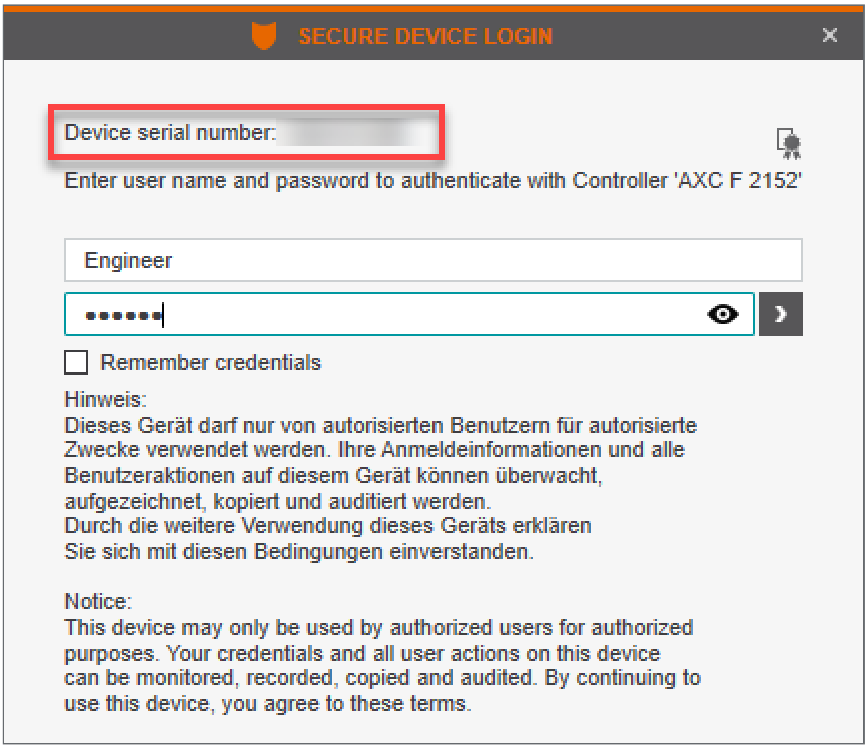
ℹ For information on configuring the IP settings, please refer to the Configuring the IP settings topic in the main PLCnext Technology - Info Center.

...continuation see next page...

- Connect PLCnext Engineer to the PLCnext Control by clicking the button (**Connect to the controller to establish communication with online services**).



↪ The **SECURE DEVICE LOGIN** opens.
Note: To ensure that you are connecting to the correct device, you must compare the serial number displayed in the login dialog with the serial number printed on the device.



SECURE DEVICE LOGIN

Device serial number: [redacted]

Enter user name and password to authenticate with Controller 'AXC F 2152'

Engineer

••••••

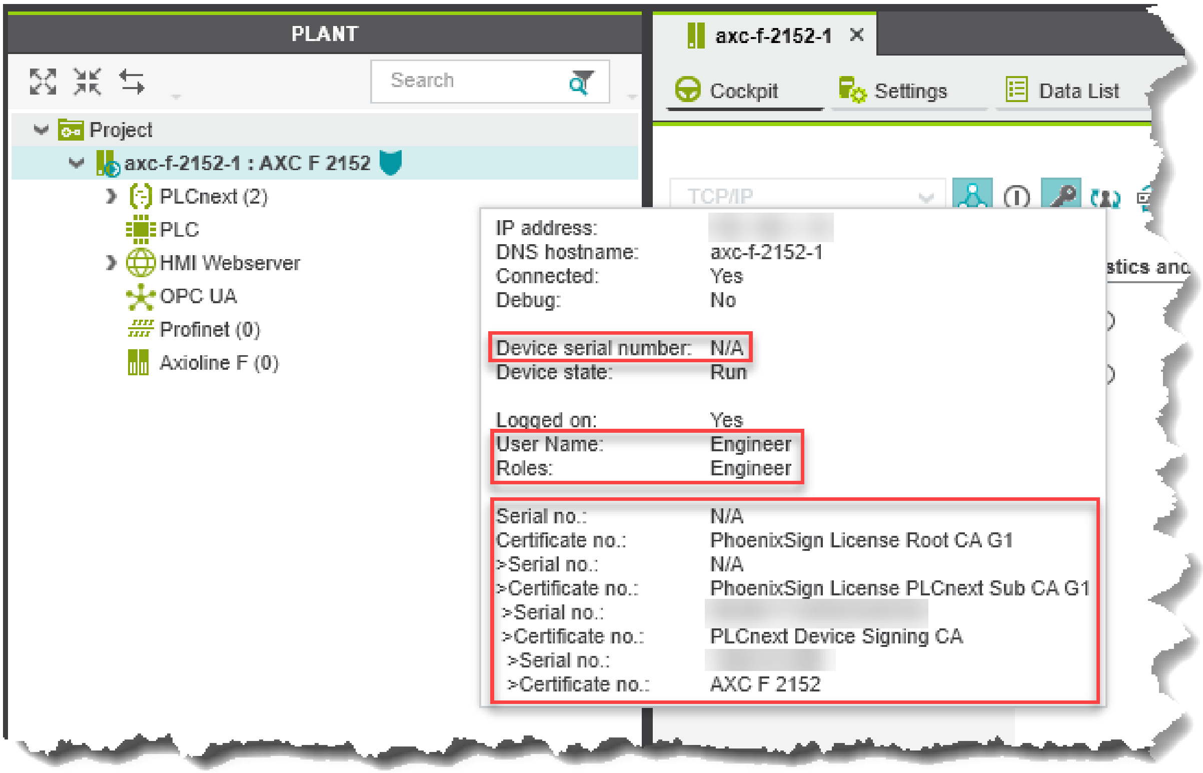
□ Remember credentials

Hinweis:
Dieses Gerät darf nur von autorisierten Benutzern für autorisierte Zwecke verwendet werden. Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Gerät können überwacht, aufgezeichnet, kopiert und auditiert werden.
Durch die weitere Verwendung dieses Geräts erklären Sie sich mit diesen Bedingungen einverstanden.

Notice:
This device may only be used by authorized users for authorized purposes. Your credentials and all user actions on this device can be monitored, recorded, copied and audited. By continuing to use this device, you agree to these terms.

- Make sure that you are connecting to the correct device by checking the displayed serial number.
- Enter your user name and your password.
  Note: You have to log in with the user who has the role "Engineer".

- Display the context menu of the controller node in the **PLANT** area via mouseover.



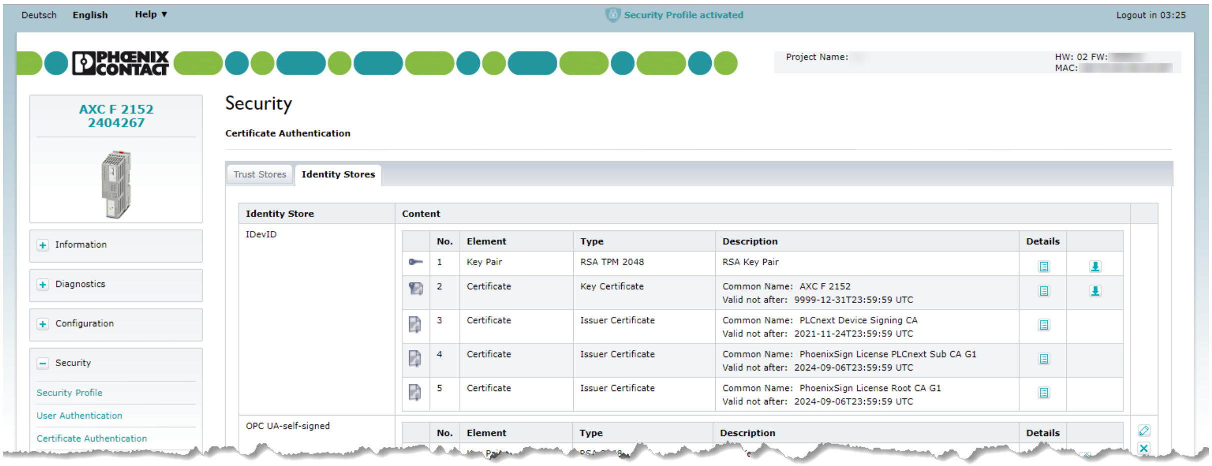
IP address: [redacted]
DNS hostname: axc-f-2152-1
Connected: Yes
Debug: No

Device serial number: N/A
Device state: Run

Logged on: Yes
User Name: Engineer
Roles: Engineer

Serial no.: N/A
Certificate no.: PhoenixSign License Root CA G1
>Serial no.: N/A
>Certificate no.: PhoenixSign License PLCnext Sub CA G1
>Serial no.: [redacted]
>Certificate no.: PLCnext Device Signing CA
>Serial no.: [redacted]
>Certificate no.: AXC F 2152

- Make sure you are connected to the correct device (**Device serial number**).
- Check how you are logged in (**User Name**) and what role you have (**Roles**).
- The lower section of the context menu lists the certificates and issuers that were applied to the device. You can also see this information in the WBM on the **Certificate Authentication** page on the **Identity Stores** tab.



Security

Certificate Authentication

Trust Stores | Identity Stores

Identity Store	Content
IDevID	

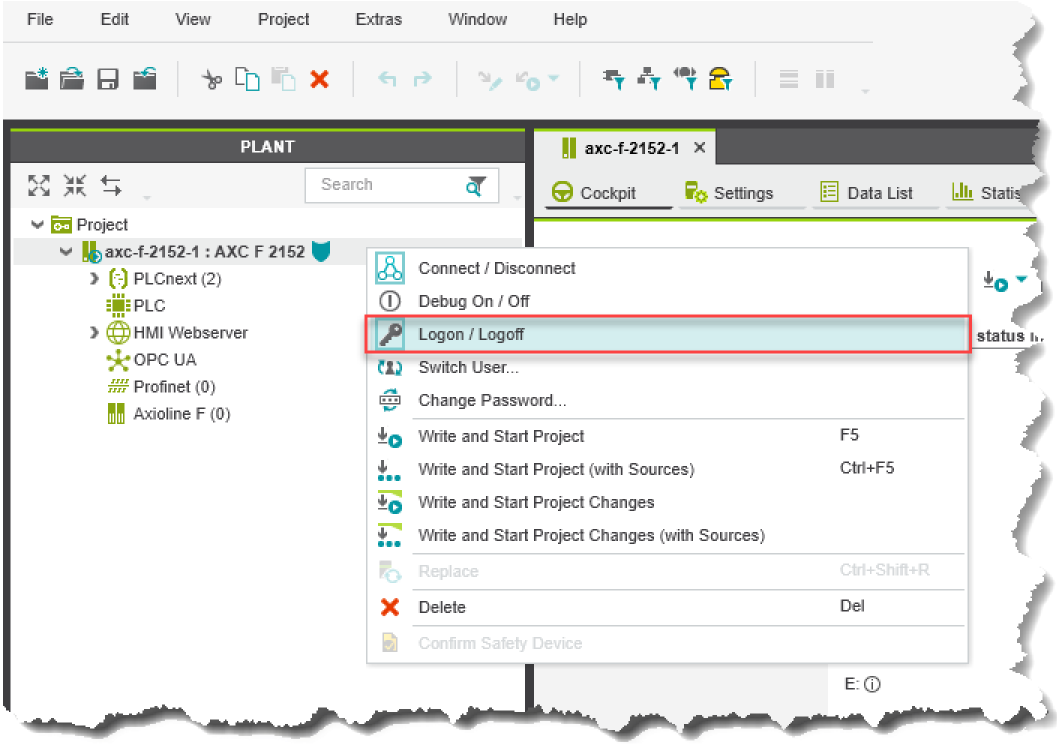
	No.	Element	Type	Description	Details	
	1	Key Pair	RSA TPM 2048	RSA Key Pair		
	2	Certificate	Key Certificate	Common Name: AXC F 2152 Valid not after: 9999-12-31T23:59:59 UTC		
	3	Certificate	Issuer Certificate	Common Name: PLCnext Device Signing CA Valid not after: 2021-11-24T23:59:59 UTC		
	4	Certificate	Issuer Certificate	Common Name: PhoenixSign License PLCnext Sub CA G1 Valid not after: 2024-09-06T23:59:59 UTC		
	5	Certificate	Issuer Certificate	Common Name: PhoenixSign License Root CA G1 Valid not after: 2024-09-06T23:59:59 UTC		

OPC UA-self-signed

	No.	Element	Type	Description	Details

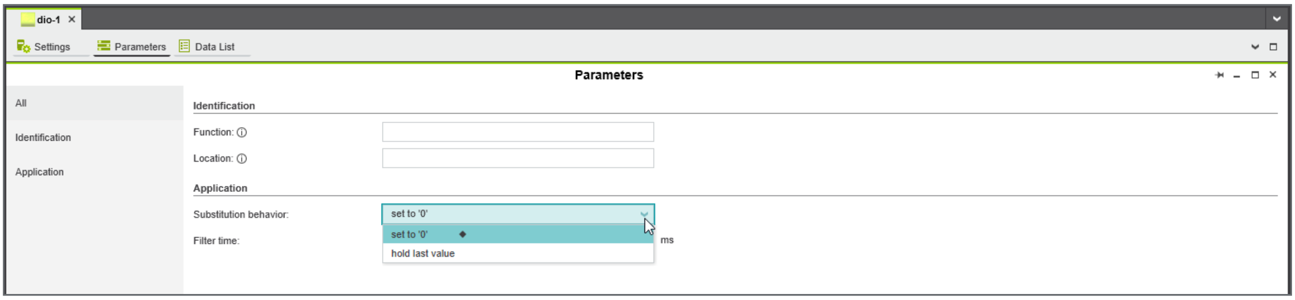
- Transfer the system time to the PLCnext Control by clicking the button.
- Transfer the project to the PLCnext Control.

- After transferring the project to the PLCnext Control, log out of PLCnext Engineer via the context menu, which you reach by right-clicking on the controller node in the PLANT area.



Substitution behavior for output modules

For each output module you can define a substitution behavior in PLCnext Engineer. The default setting is set to '0'. Depending on your application you have to adjust the setting.



Function: ⓘ

Location: ⓘ

Substitution behavior: set to '0'

Filter time: ms

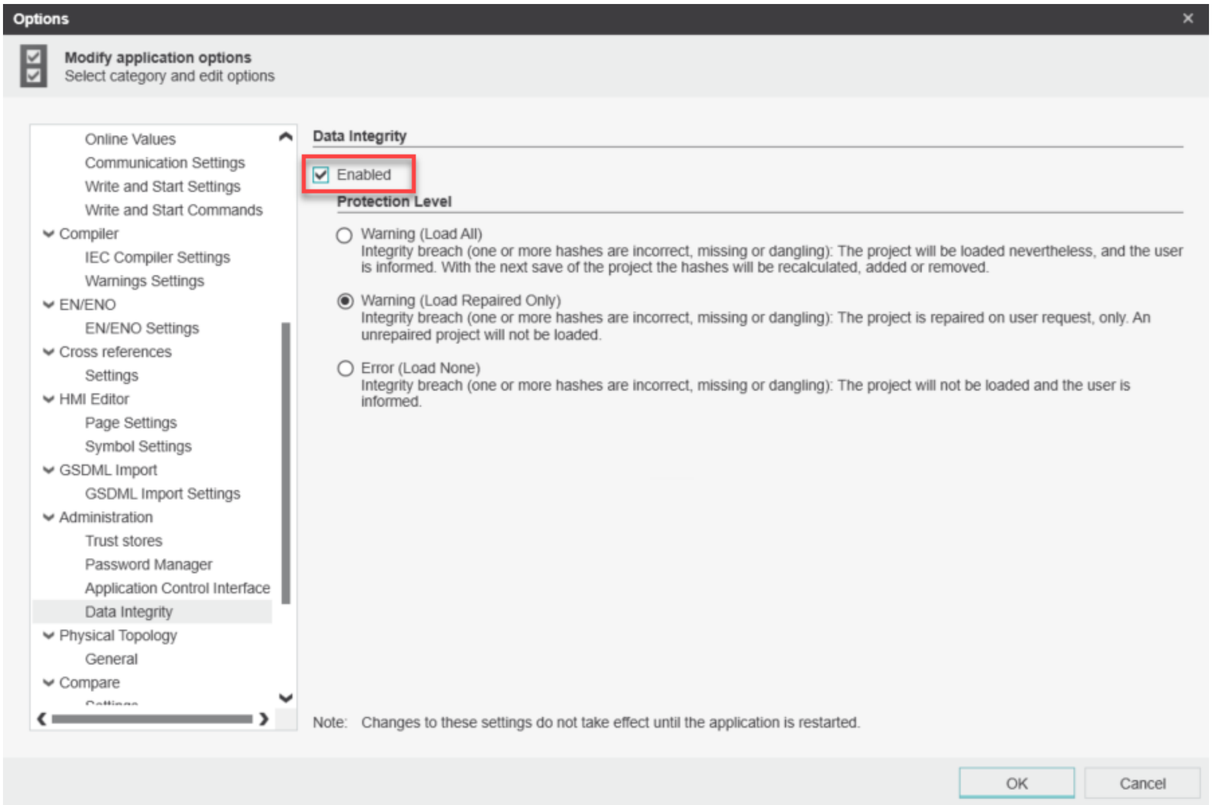
Activating PLCnext Engineer project data integrity check

In PLCnext Engineer from version 2023.0, you can enable the project integrity check (hash protection of projects and libraries locally stored on your computer). With activated Enabled checkbox (hash protection is activated), PLCnext Engineer calculates hash codes (numeric value of fixed length that uniquely identifies data) about the project. The project's hash codes are checked for mismatching or missing hashes when opening the project. Depending on the protection level selected here, you will be informed with a warning/error message and the appropriate action will be performed.
With deactivated hash protection (Enabled checkbox deactivated; default setting), PLCnext Engineer does not use hash codes for comparison of project contents. No hash codes are calculated and checked. You will not be informed whether a project has or does not have hash codes.

Phoenix Contact recommends to enable the hash protection (data integrity check). Proceed as follows:

- In PLCnext Engineer, open the options menu: Extras → Options...

- Open the **Administration** drop-down menu.
- Click on **Data integrity**.
- Activate the checkbox **Enabled**.



Data Integrity

☑ Enabled

Protection Level

○ Warning (Load All)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will be loaded nevertheless, and the user is informed. With the next save of the project the hashes will be recalculated, added or removed.

● Warning (Load Repaired Only)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project is repaired on user request, only. An unrepaired project will not be loaded.

○ Error (Load None)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will not be loaded and the user is informed.

Note: Changes to these settings do not take effect until the application is restarted.

- Click the **OK** button.
- Restart PLCnext Engineer.

For further information, refer to the topic Configuring PLCnext Engineer (combined safety).

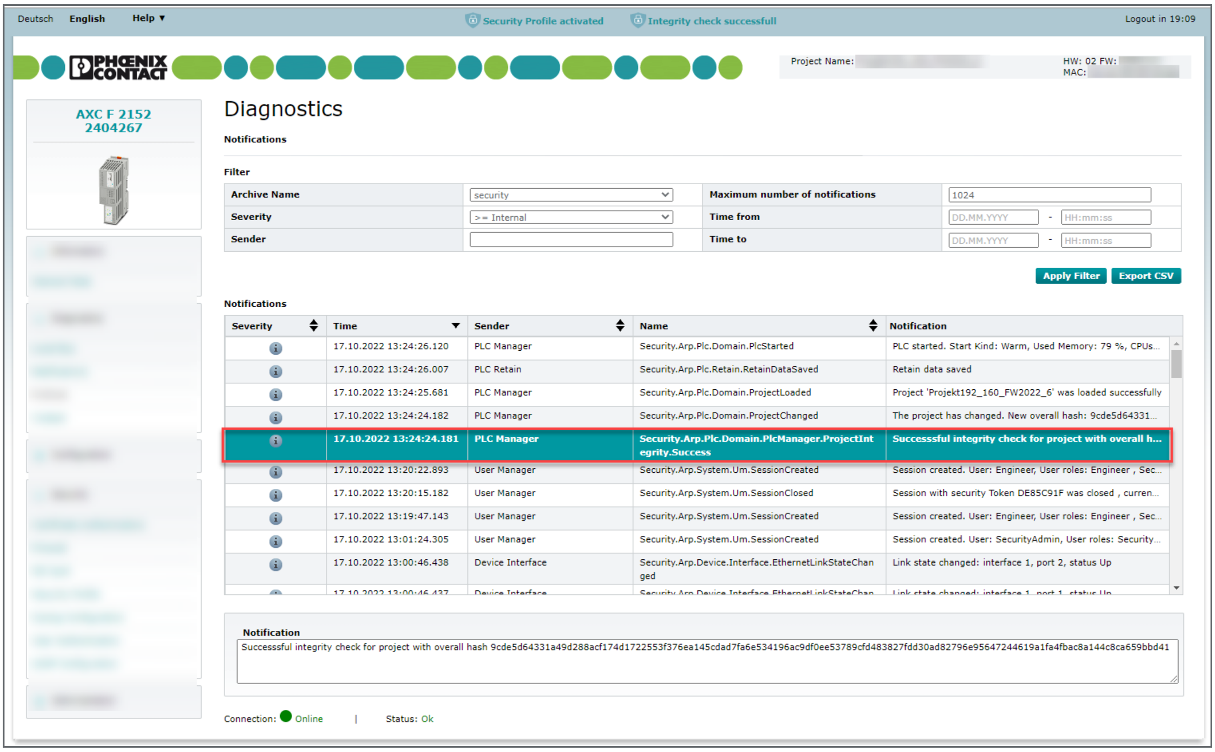
Checking project data integrity

Libraries and projects in PLCnext Engineer are hashed. The hashes assigned with PLCnext Engineer are checked by PLCnext Control. This way you can verify that data is not modified, tampered with, or corrupted.

When creating the project in PLCnext Engineer, a manifest file with hashes is generated. Before the project is loaded on the PLCnext Control, it is checked whether this project has integrity. This integrity check writes a notification.

After downloading a project to the PLCnext Control you have to make sure that the integrity check of the project data was successful. To do this, you need to check the notifications. Proceed as follows:

- Log in to the WBM.
- Open the **Notifications** page (**Diagnostics** → **Notifications**).
- Check if you can see a notification stating that the integrity check was successful for your project. See the example screenshot below.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

Diagnostics

Notifications

Filter

Archive Name	security	Maximum number of notifications	1024
Severity	>= Internal	Time from	DD.MM.YYYY - HH:mm:ss
Sender		Time to	DD.MM.YYYY - HH:mm:ss

Notifications

Severity	Time	Sender	Name	Notification
i	17.10.2022 13:24:26.120	PLC Manager	Security.Arp.Plc.Domain.PlcStarted	PLC started. Start Kind: Warm, Used Memory: 79 %, CPUs...
i	17.10.2022 13:24:26.007	PLC Retain	Security.Arp.Plc.Retain.RetainDataSaved	Retain data saved
i	17.10.2022 13:24:25.681	PLC Manager	Security.Arp.Plc.Domain.ProjectLoaded	Project 'Projekt192_160_FW2022_6' was loaded successfully
i	17.10.2022 13:24:24.182	PLC Manager	Security.Arp.Plc.Domain.ProjectChanged	The project has changed. New overall hash: 9cde5d64331...
i	**17.10.2022 13:24:24.181**	**PLC Manager**	**Security.Arp.Plc.Domain.PlcManager.ProjectIntegrity.Success**	**Successsful integrity check for project with overall h...**
i	17.10.2022 13:20:22.893	User Manager	Security.Arp.System.Um.SessionCreated	Session created. User: Engineer, User roles: Engineer , Sec...
i	17.10.2022 13:20:15.182	User Manager	Security.Arp.System.Um.SessionClosed	Session with security Token DE85C91F was closed , curren...
i	17.10.2022 13:19:47.143	User Manager	Security.Arp.System.Um.SessionCreated	Session created. User: Engineer, User roles: Engineer , Sec...
i	17.10.2022 13:01:24.305	User Manager	Security.Arp.System.Um.SessionCreated	Session created. User: SecurityAdmin, User roles: Security...
i	17.10.2022 13:00:46.438	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 1, port 2, status Up
i	17.10.2022 13:00:46.437	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChan	Link state changed: interface 1, port 1, status Up

Notification

Successsful integrity check for project with overall hash 9cde5d64331a49d288acf174d1722553f376ea145cdad7fa6e534196ac9df0ee53789cfd483827fdd30ad82796e95647244619a1fa4fbac8a144c8ca659bbd41

Connection: ● Online | Status: Ok

Further steps of the check follow, which you must check for completeness:

- The project is loaded onto the controller.
- The project name of the project is displayed. Check if the project name matches the project you wanted to load on the controller.
- PLCnext Control started.

The project data integrity check detects various errors and displays them in the notifications. The following entries are possible:

- "Manifest file does not exist"
- "Hash algorithm not supported"
- "Hash value of the file is not correct"
- "File does not belong to the project"
- "File does not exist"

All devices have the same default configuration, which depends on the Security Profile:

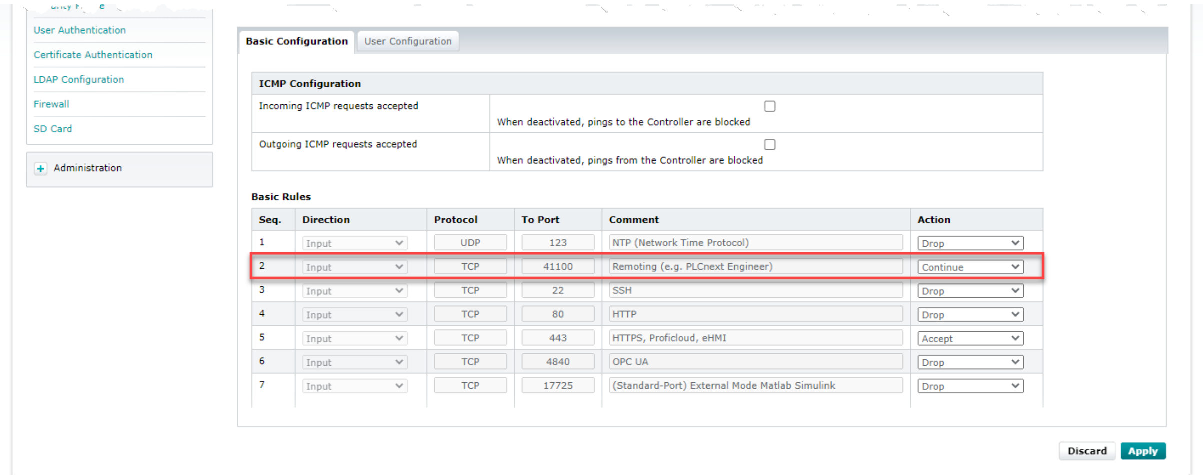
- With activated Security Profile: Error
  PLCnext Control does not go to the RUN status, but to the FAIL status (Ready (error)).
  ℹ For more information about the status, see the corresponding documentation, e. g. User manual AXC F 2152.
- Without activated Security Profile: Warning
  A warning is displayed, but PLCnext Control starts and the program runs.

Configuring extended firewall settings

See also the Configuring basic firewall settings topic. For basic firewall configuration information, refer to the Firewall WBM topic in the main PLCnext Technology - Info Center .

In the exemplary security context, access from the Engineering Station is only allowed via the extension module from the superordinate network.
To configure accesses according to the security context, proceed as follows:

- Log in to the WBM.
- Open the **Firewall** page (**Security** → **Firewall**) in the WBM.
- Open the **Basic Configuration** tab.
- In the **Basic Rules** section, select **Continue** from the drop-down list for the Remoting in the **Action** column.



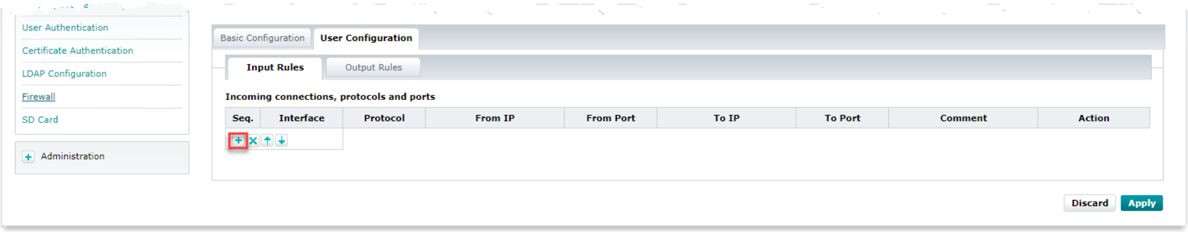
ICMP Configuration

Incoming ICMP requests accepted	□ When deactivated, pings to the Controller are blocked
Outgoing ICMP requests accepted	□ When deactivated, pings from the Controller are blocked

Basic Rules

Seq.	Direction	Protocol	To Port	Comment	Action
1	Input	UDP	123	NTP (Network Time Protocol)	Drop
2	Input	TCP	41100	Remoting (e.g. PLCnext Engineer)	Continue
3	Input	TCP	22	SSH	Drop
4	Input	TCP	80	HTTP	Drop
5	Input	TCP	443	HTTPS, Proficloud, eHMI	Accept
6	Input	TCP	4840	OPC UA	Drop
7	Input	TCP	17725	(Standard-Port) External Mode Matlab Simulink	Drop

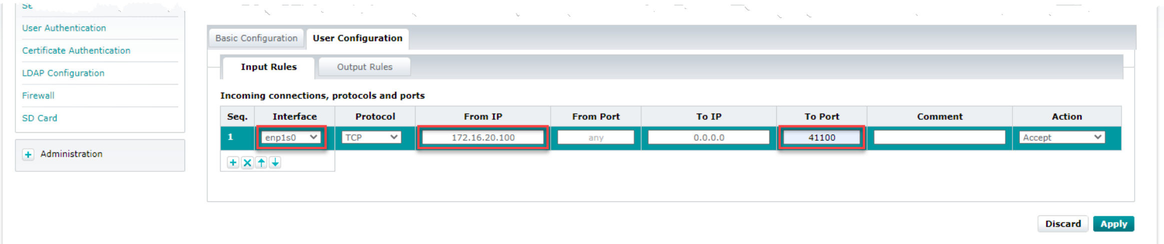
- Click the **Apply** button.
- Open the **User Configuration** tab.
- On the **Input Rules** tab, click the + (**New rule**)



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action

- Provide the following information:
  - Select the interface (refer to the topic AXC F 2152).
  - Enter the corresponding IP address (the IP address of the Engineering Station in the superordinate network).
  - Enter the target port.



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	enp1s0	TCP	172.16.20.100	any	0.0.0.0	41100		Accept

- Click the **Apply** button.
  ↪ Now you have access from the superordinate network (e.g. PLCnext Engineer) only via the extension module.

Plant documentation

If you want to use the list of activated firewall rules in your plant documentation, you can export the list from the WBM. Proceed as follows:

System Status section

If the firewall is active, you can generate an overview of all enabled firewall rules in a **.txt* file.

- Click on **Show Rules** in the **System Status** section.
  ↪ The **.txt* file with the activated firewall rules is being generated and opens in a dialog box.
- To save the active rules to a **.txt* file, click **Save to file** in the dialog box.
  ↪ The **.txt* file is saved to the directory selected in the next step.

ℹ For further information, refer to the Firewall WBM topic in the main PLCnext Technology - Info Center.

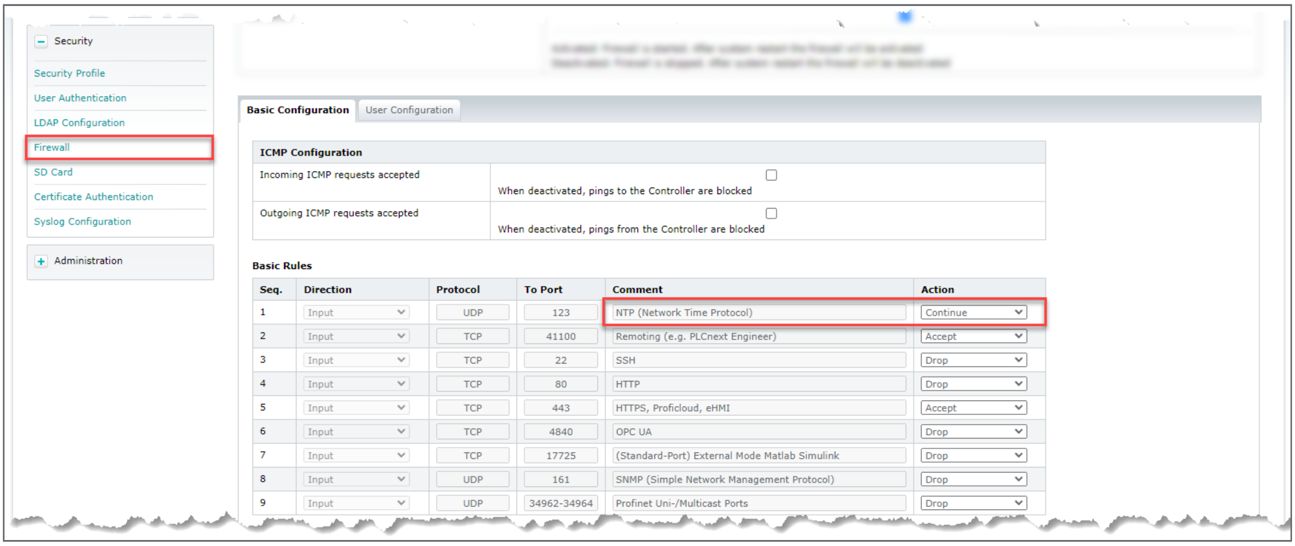
Configuring the system time

Centralized security logging only makes sense if all devices have a synchronized time. NTP is already supported today. TimeServer provides all devices with the same time base. For each device you have to configure which time server it should use.

Use the corresponding WBM page for this as described in the Date and Time topic in the main PLCnext Technology - Info Center.

> **Note:** Make sure that the firewall basic configurations and the input rules on the `Firewall` page (`Security` → `Firewall`) in the WBM are correct:

Basic Configuration:



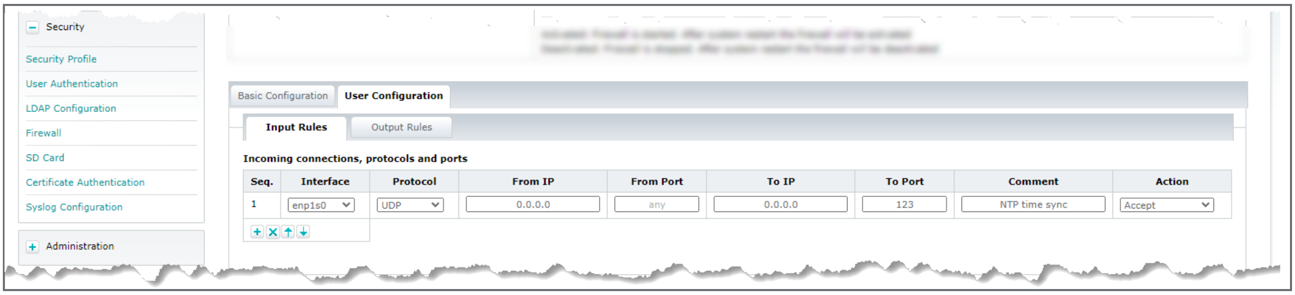
ICMP Configuration

Incoming ICMP requests accepted	□ When deactivated, pings to the Controller are blocked
Outgoing ICMP requests accepted	□ When deactivated, pings from the Controller are blocked

Basic Rules

Seq.	Direction	Protocol	To Port	Comment	Action
1	Input	UDP	123	NTP (Network Time Protocol)	Continue
2	Input	TCP	41100	Remoting (e.g. PLCnext Engineer)	Accept
3	Input	TCP	22	SSH	Drop
4	Input	TCP	80	HTTP	Drop
5	Input	TCP	443	HTTPS, Proficloud, eHMI	Accept
6	Input	TCP	4840	OPC UA	Drop
7	Input	TCP	17725	(Standard-Port) External Mode Matlab Simulink	Drop
8	Input	UDP	161	SNMP (Simple Network Management Protocol)	Drop
9	Input	UDP	34962-34964	Profinet Uni-/Multicast Ports	Drop

Input Rules:



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	enp1s0	UDP	0.0.0.0	any	0.0.0.0	123	NTP time sync	Accept

ℹ For information on how to set the system time, refer to the System time topic in the main PLCnext Technology - Info Center.

There are some parameters to be set, e.g. what deviation from the time is acceptable, the maximum unavailability, etc.

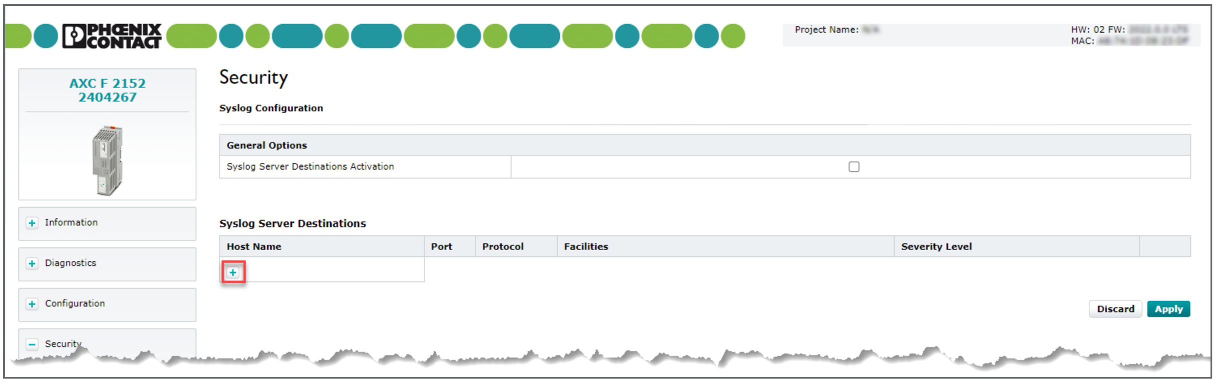
Configuring central logging

Logging in the security context only makes sense in a network. When configuring the SysLog, you set to which higher-level server the data is sent and which data it is.

ℹ For information on basic security logging, refer to the topic Security logging.

ℹ For further information on SysLog configuration, refer to the topic Security - Syslog configuration in the main PLCnext Technology - Info Center.

- Log in to the WBM.
- Open the **Syslog Configuration** page (**Security** → **Syslog Configuration**).
- To add a new Syslog server destination configuration, select the **+** button.



Project Name: [redacted]

HW: 02 FW: [redacted]
MAC: [redacted]

Security

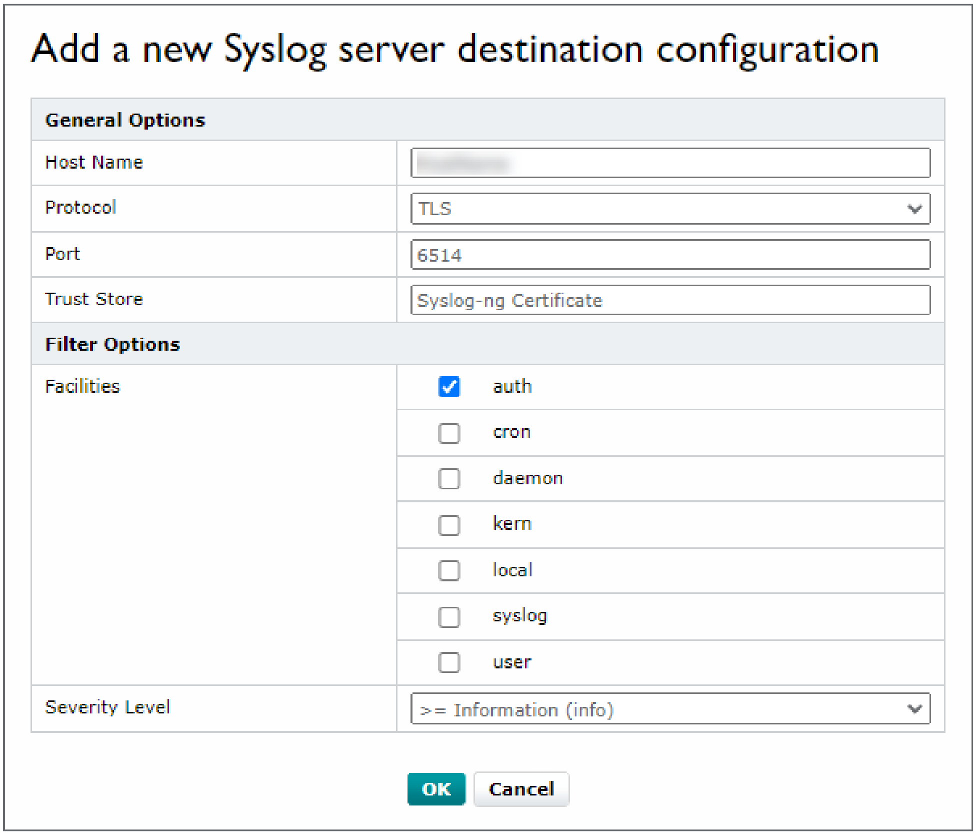
Syslog Configuration

General Options	
Syslog Server Destinations Activation	☐

Syslog Server Destinations

Host Name	Port	Protocol	Facilities	Severity Level

- Provide the following information:



Add a new Syslog server destination configuration

General Options	
Host Name	[redacted]
Protocol	TLS
Port	6514
Trust Store	Syslog-ng Certificate
Filter Options	
Facilities	☑ auth ☐ cron ☐ daemon ☐ kern ☐ local ☐ syslog ☐ user
Severity Level	>= Information (info)

- **Host Name** : IP address of the device (host) to send the logging messages to.
- **Protocol** : It is recommended to configure TLS.

- **Port**: Select the port on which the devices exchange data. Make sure that the port is enabled in the firewall settings.
- **Trust Store**: Select the Trust Store.
- **Facilities**: Choose what kind of data should be exchanged. Choose **auth** in any case.
- **Severity Level**: Select **>=Information (info)**.

In addition to the settings in the WBM, you must also make settings on the higher-level server.

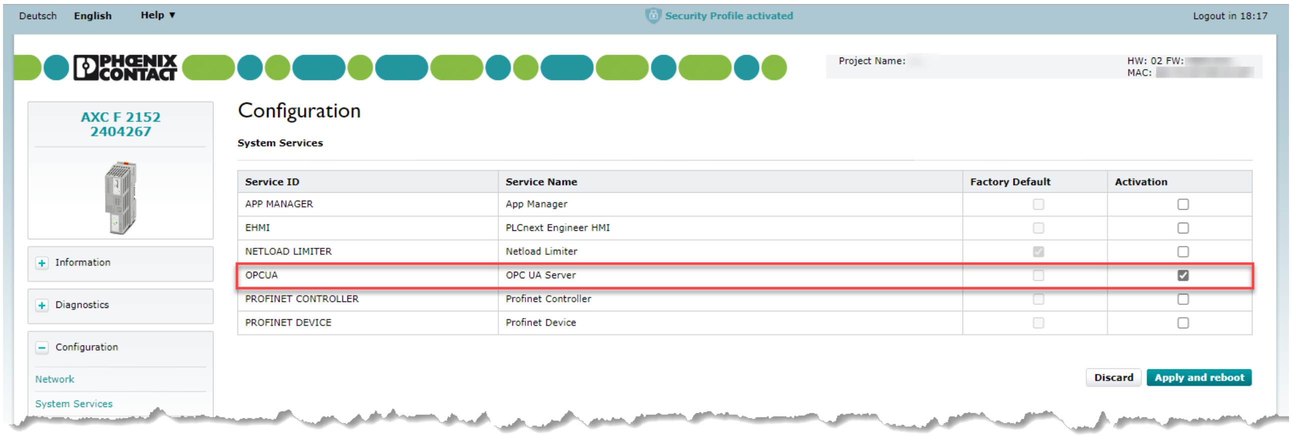
- Make the necessary changes in the syslog-ng.conf file.

Note: The specified IP address and the selected port must be enabled in the firewall. For further information, refer to the topic Configuring extended firewall settings.

Activating OPC UA Server

To activate OPC UA Server, proceed as follows:

- Log in to the WBM.
- Open the **Configuration** → **System Services** page in the WBM.
- Activate the OPC UA Server by its checkbox.
- Click the **Apply and reboot** button.



Project Name:

HW: 02 FW: [redacted]
MAC: [redacted]

Configuration

System Services

Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	□	□
EHMI	PLCnext Engineer HMI	□	□
NETLOAD LIMITER	Netload Limiter	☑	□
OPCUA	OPC UA Server	□	☑
PROFINET CONTROLLER	Profinet Controller	□	□
PROFINET DEVICE	Profinet Device	□	□

Note:

- You have to make some settings in the OPC UA Client.
- Your OPC UA client requires a system use notification that complies with your legal requirements. You can see an example in the User Authentication WBM topic in the main PLCnext Technology - Info Center.

Secured OPC UA Communication

On the 'Security' page of the 'OPC UA' PLANT tree node, you can specify settings regarding certificates and authentication which must be performed successfully in order to establish a secure connection between OPC UA clients and the OPC UA server. Furthermore, you can define which encryption algorithms the OPC UA server will provide to its clients to secure transmitted data.

After modifying these settings and writing them to the controller (as part of the PLCnext Engineer project), the controller (i.e., OPC UA server) generates the self-signed certificate (if needed) when switching its state from `Stop` to `Run` and applies it.

Certificate

Configures the certificate management on the OPC UA server.

- **'File on controller':** a certificate file (including a private key) is stored in the IdentityStore on the controller device. This can be a CA-signed or a self-signed certificate (see term definitions at the end of this topic). The location on the controller is fixed and cannot be modified.

  The transfer of the certificate into the controller's IdentityStore can be done via the Web Based Management (WBM) interface of the controller or using the tool SCP Secure Copy (the transfer is not possible using PLCnext Engineer).

  Refer to the controller manual of your PLCnext Technology device for details. Refer to the table row 'TrustStores' below for an explanation of the term "IdentityStore".

- **'Self-signed by controller':** the server generates and uses the self-signed certificate, generated by the server and signed with its own private key. Using the self-signed certificate causes greater efforts when establishing a network with many application instances because the certificate must be distributed manually to the involved instances.

  After selecting 'Self-signed by controller', the 'Subject' options become visible with which you specify subject(s) of the certificate. Modifying these subject settings result in a newly generated self-signed certificate after the next project download. Refer to the table row "Type of subject" below for details.

- **'Provided by OPC UA GDS':** The OPC UA server embedded in the PLCnext Technology device is ready to be automatically provided with certificates according to the Certificate Push Management defined by the OPC UA standard (V 1.04, Part 12). This includes the initial certificates as well as all follow-up certificates (updates).

  The certificates are expected to be automatically provided by a Global Discovery Server (GDS) which implements the push mechanism. The Global Discovery Server is expected to connect to the OPC UA server in the PLCnext Technology device as a "special" OPC UA client.

  The Global Discovery Server is not part of PLCnext Engineer. Any suitable tool customary on the market can be used. It must be configured accordingly, in order to supply the OPC UA server on the PLCnext Technology device as well as all OPC UA clients (i.e., all relevant devices within your network/security domain) with certificates. Note that the Global Discovery Server can also be located in a different security domain (subnetwork).

  After having selected 'Provided by OPC UA GDS', you have to define the names for the TrustStore and the IdentityStore of the OPC UA server. The names are freely definable. You can see and inspect the content of these stores at the Web Based Management (WBM) of the controller. The OPC UA server uses them to store data there which it received from the Global Discovery Server (GDS). Into the named IdentityStore it stores the certificate and key which it is instructed by the GDS to authenticate itself against clients. Into the TrustStore it stores trusted and issuer certificates as it receives them from the GDS to verify client certificates with.

  After selecting 'Provided by OPC UA GDS', the 'Subject' options become also visible with which you specify subject(s) of the certificate. Depending on the Global Discovery Server involved, these subject settings can be integrated in the certificates that will be delivered to the OPC UA server. Refer to the table row "Type of subject" below for details.

Trust Stores

These fields are only visible if 'Server certificate' is set to 'Provided by OPC UA GDS' (see row above).
You have to define the names of the TrustStore and the Identity Store which the OPC UA server shall use to store data it receives from the Global Discovery Server (GDS). Enter the freely definable names into the text fields. You can inspect the current content of these stores via the Web Based Management (WBM) interface of the PLCnext Technology device.

- **'IdentityStore name':** Defines the name of the IdentityStore of the OPC UA server on the PLCnext Technology device where the OPC UA server shall store its own application instance certificate and key as it is instructed to use by the Global Discovery Server. With the information stored in the IdentityStore, the OPC UA server authenticates itself against clients.

- **'TrustStore name':** Defines the name of the TrustStore of the OPC UA server on the PLCnext Technology device into which the OPC UA server stores the data it receives from a Global Discovery Server (GDS) to authenticate clients with. Using the information in the TrustStore, the OPC UA server can verify the identity of connecting OPC UA clients by validating the authenticity of the certificates they present.

  A PLCnext Technology device may contain several TrustStores. The OPC UA server embedded in the PLCnext Technology device currently supports one TrustStore. The counterpart of a TrustStore in the PLCnext Technology device is the IdentityStore (see above).

For both the TrustStore and the IdentityStore, the following applies:

- The contained data are stored in the PLCnext Technology file system and can optionally be protected by hardware measures. By default, manufacturer-defined TrustStores and IdentityStores can be implemented.
  Examples: A default TrustStore which contains data for validating the authenticity of the Proficloud server when establishing a connection to the Proficloud, or an IdentityStore for the authentication at the HTTPS server or the Remoting server of the device.
- TrustStores and IdentityStores on the PLCnext Technology device can be explored via the Web Based Management (WBM) interface.
- In the current implementation, three TrustStores and three IdentityStores are ready for use by the OPC UA server. The OPC UA server currently supports one TrustStore and one IdentityStore at a time. Which one is used depends on the OPC UA server configuration.

  IdentityStores:

  1. One IdentityStore with fixed name for the self-signed certificate. This store is used when selecting the configuration option 'Self-signed by controller'.
  2. One IdentityStore with fixed name for the certificate file. This store is used when selecting the configuration option 'File on controller'.
  3. One IdentityStore with a name defined via PLCnext Engineer for the certificate pushed by the GDS. This store is used when selecting the configuration option 'Provided by OPC UA GDS'.

  TrustStores:

  1. One TrustStore with fixed name for use with the certificate file. This store is used when selecting the configuration option 'File on controller' or 'Self-signed by controller'.
  2. One TrustStore with a name defined via PLCnext Engineer for information pushed by the GDS. This store is used when selecting the configuration option 'Provided by OPC UA GDS'.

     In this case, the following applies: if not yet defined (e.g., by WBM), you can simply create a **new** TrustStore or IdentityStore by typing any name into the inputs fields. This way, a corresponding store with this name will be created on the device when the OPC UA server executes the project. Once created, the store will still be empty but listed in the WBM.

  Note: As long as the TrustStore is empty, the OPC UA server trusts all clients.

- The content of both the TrustStore and the IdentityStore can be modified via the WBM interface. This way, you can manually "prefill" the TrustStore in order to enable the OPC UA server to trust the Global Discovery Server which will provide the OPC UA server with further certificates. You can furthermore prefill the IdentityStore with a server certificate in order to enable the server to authenticate itself as trusted member of your security domain, for example, at the Global Discovery Server.
- Configure the Global Discovery Server involved accordingly to trust the OPC UA server (in order to establish a connection between OPC UA server and GDS). Then set up the GDS in a way that it cyclically writes the required security data into the TrustStore and the IdentityStore of the OPC UA server.

Note: The OPC UA standard uses different terms. The standard mentions a TrustList the content of which is very similar to the content of a TrustStore of the PLCnext Technology device. The standard specifies a CertificateGroup which is very similar to the information within an IdentityStore of the PLCnext Technology device.

Type of subject

These fields are only visible if 'Server certificate' is set to 'Self-signed by controller' or 'Provided by OPC UA GDS'.

Note: In case of 'Provided by OPC UA GDS' it depends on the implementation of the Global Discovery Server involved whether the subject settings made here are considered or not.

A subject specifies the owner of a certificate. A subject can be accompanied by alternative names. Within certificates according to the X.509 standard these alternative names are recorded within a so-called "subjAltName"-Extension within the certificate.

Using these input fields, you can specify alternative names the OPC UA server shall include in the self-signed certificate it generates or in the certificate signing request it generates for a Global Discovery Server.
You can specify up to five alternative names for the subject. Each alternative name shall describe a DNS name or IP address the OPC UA server is reachable at. The OPC UA server automatically also includes the DNS name specified in the basic settings as an alternative name regardless of the settings here.
This way, you can enable up to four communication paths (provided that this is supported by your network architecture, for example, using a router, existing port forwarding (firewall in router to OPC UA server) and implemented local DynDNS).
When establishing the connection, OPC UA clients verify whether the address (DNS name or IP address) from the URL they wanted to connect to is contained in the server certificate.
If several possibilities exist for connecting the OPC UA server from outside or inside the domain, each possible address part of a URL must be contained in the certificate. Otherwise, the authentication fails.
Any specified DNS name or IP address (depending on the selection in 'Type of subject') is written into the self-signed certificate. If 'not set' is selected in a subject field, it is ignored by the server when generating the certificate. When specifying 'not set' for all subjects, no alternative name will be included in the self-signed certificate except for the DNS name from the Basic Settings which is always included.

Note: If clients use short URLs (because they are located in the same domain as the OPC UA server), list these short names here as alternative names.

Security Policies

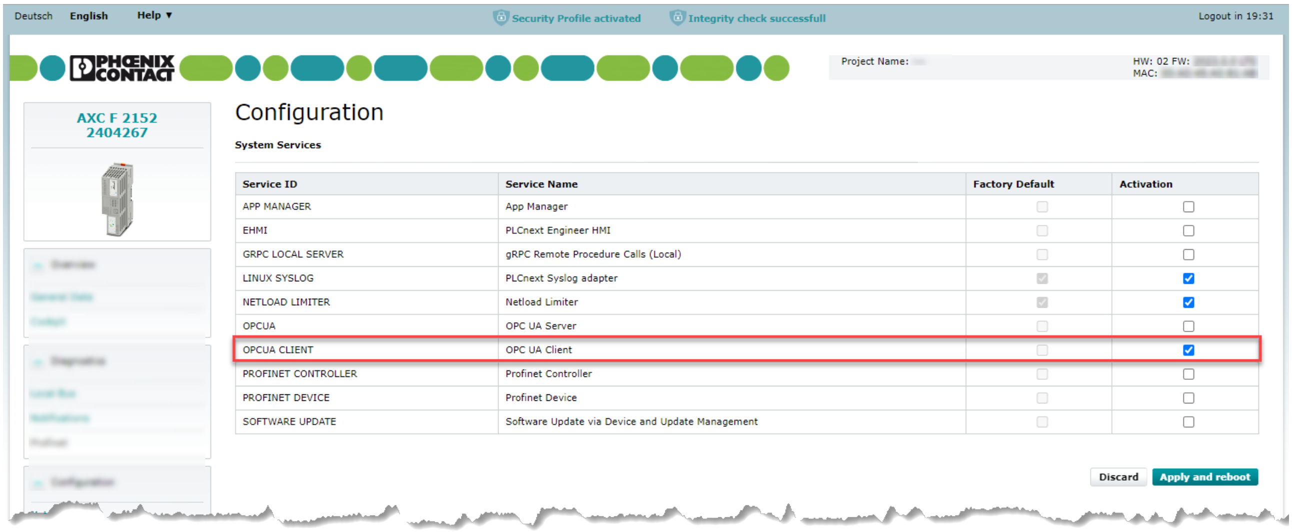
Defines the encryption algorithm(s) (Cipher Suite), the OPC UA server offers to its clients. The encryption algorithm is applied to and secures the data transfer between OPC UA server and client.
Select 'Yes' in the relating drop-down list to make the respective algorithm available for clients. If set to 'No', the encryption algorithm cannot be selected in the OPC UA client settings.
From top to bottom, the encryption and signature strength increases:

- 'Enable AES 128 SHA256 RSA OAEP algorithm'
- 'Enable Basic 256 algorithm'
  This Basic 256 algorithm is deprecated and is therefore set to 'No' by default. Only use this setting if the OPC UA client does not support a higher encryption.
- 'Enable Basic 256 SHA256 algorithm'
- 'Enable AES 256 SHA256 RSA PSS algorithm'

Activating OPC UA® Client

To activate OPC UA® Client, proceed as follows:

- Log in to the WBM.
- Open the **System Services** page (**Configuration** → **System Services**) in the WBM.
- Activate the OPC UA Client by its checkbox.
- Click the **Apply and reboot** button.



Project Name: [redacted]

HW: 02 FW: [redacted]
MAC: [redacted]

Configuration

System Services

Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	□	□
EHMI	PLCnext Engineer HMI	□	□
GRPC LOCAL SERVER	gRPC Remote Procedure Calls (Local)	□	□
LINUX SYSLOG	PLCnext Syslog adapter	☑	☑
NETLOAD LIMITER	Netload Limiter	☑	☑
OPCUA	OPC UA Server	□	□
OPCUA CLIENT	OPC UA Client	□	☑
PROFINET CONTROLLER	Profinet Controller	□	□
PROFINET DEVICE	Profinet Device	□	□
SOFTWARE UPDATE	Software Update via Device and Update Management	□	□

Note:

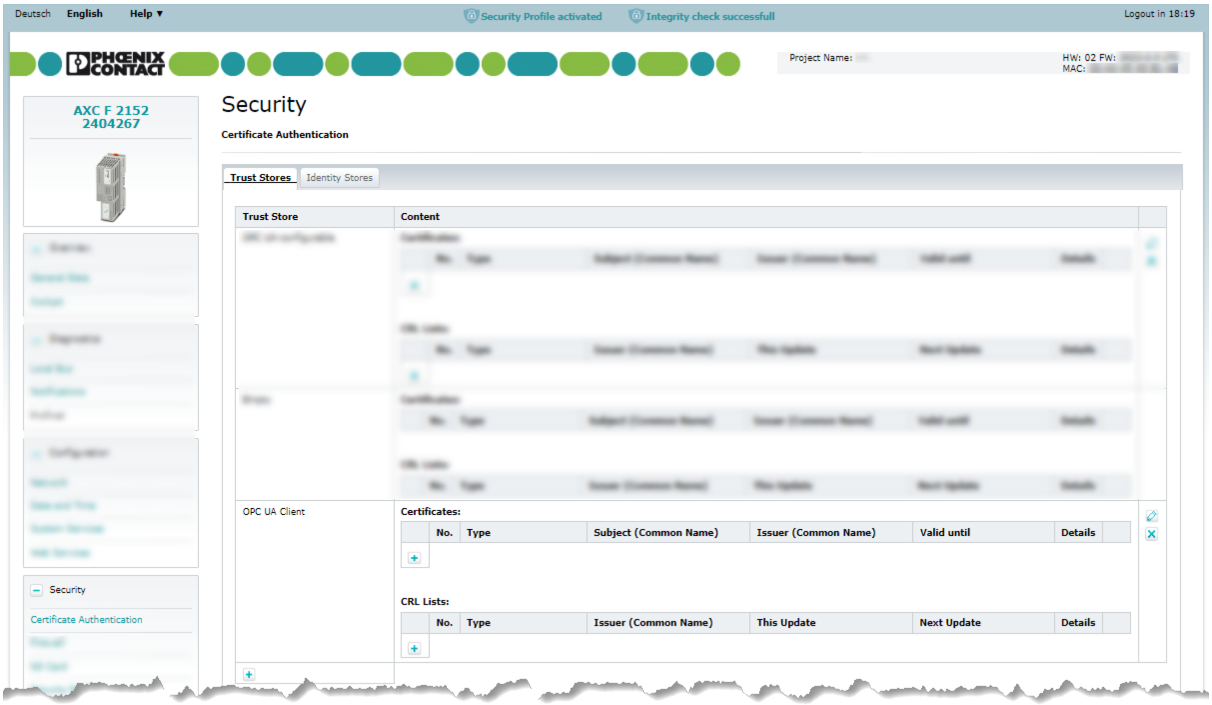
– You have to make some settings in the OPC UA Server.
– Your OPC UA client requires a system use notification that complies with your legal requirements. You can see an example in the User Authentication WBM topic in the main PLCnext Technology - Info Center.

The OPC UA® Client supports the "Minimum UA Client Profile". Currently only manual configuration is supported (configuration via PLCnext Engineer is in progress).

- Open the Identity Store and the Trust Store (**Security** → **Certificate Authentication**) to check the OPC UA Client certificates and configure them accordingly.

...continuation see next page...

Trust Stores: OPC UA Client section



Deutsch English Help ▾ Security Profile activated Integrity check successfull Logout in 18:19

Project Name:

HW: 02 FW:
MAC:

AXC F 2152
2404267

Security

Certificate Authentication

Trust Stores | Identity Stores

Security
Certificate Authentication

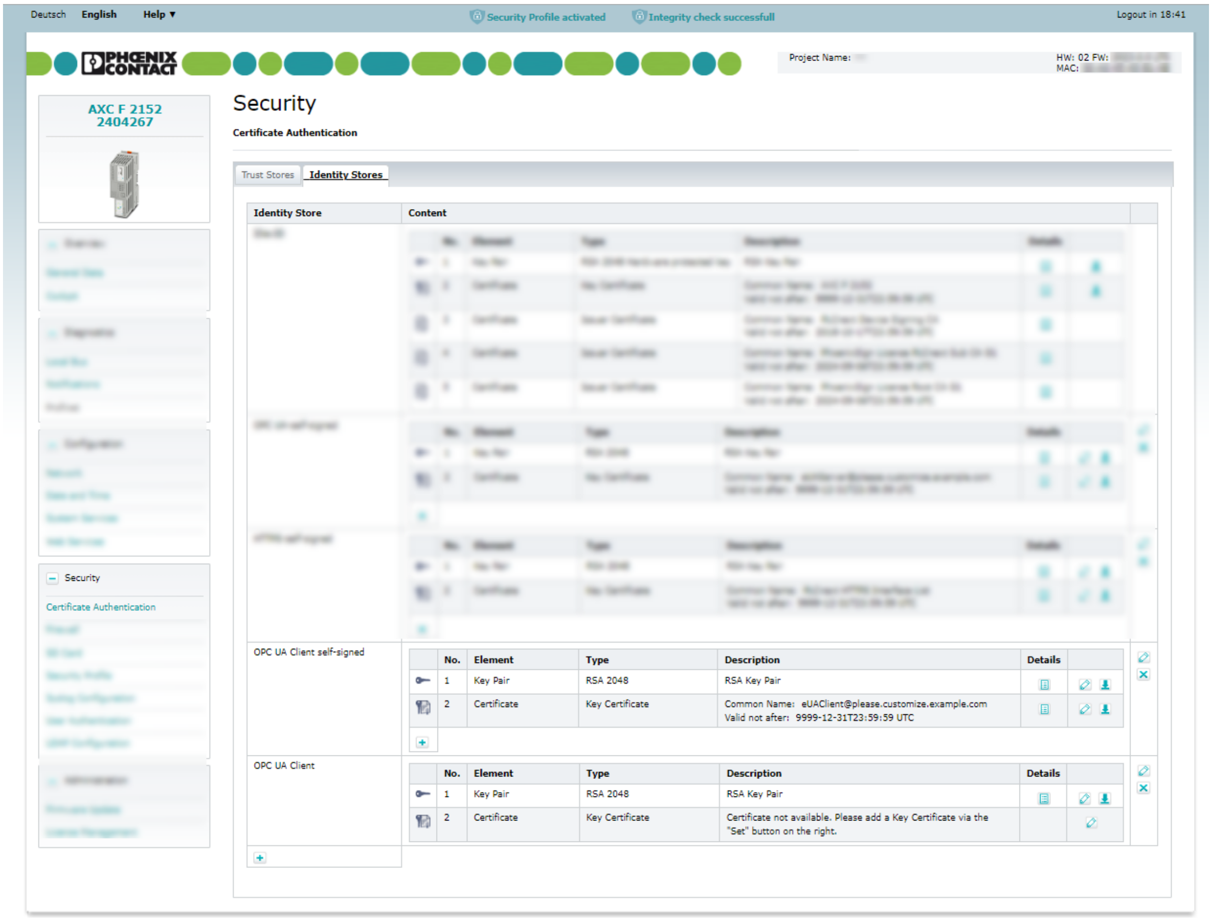
Trust Store	Content
OPC UA Client	Certificates:

No.	Type	Subject (Common Name)	Issuer (Common Name)	Valid until	Details

CRL Lists:

No.	Type	Issuer (Common Name)	This Update	Next Update	Details

Identity Stores: OPC UA Client section (self-signed and 'Application Instance Certificate')



Deutsch English Help ▾ Security Profile activated Integrity check successfull Logout in 18:41

Project Name:

HW: 02 FW:
MAC:

AXC F 2152
2404267

Security

Certificate Authentication

Trust Stores | Identity Stores

Security
Certificate Authentication

Identity Store	Content
OPC UA Client self-signed	

No.	Element	Type	Description	Details
1	Key Pair	RSA 2048	RSA Key Pair	
2	Certificate	Key Certificate	Common Name: eUAClient@please.customize.example.com Valid not after: 9999-12-31T23:59:59 UTC	

Identity Store	Content
OPC UA Client	

No.	Element	Type	Description	Details
1	Key Pair	RSA 2048	RSA Key Pair	
2	Certificate	Key Certificate	Certificate not available. Please add a Key Certificate via the "Set" button on the right.	

Further information can be found in the OPC UA Client documentation.

Activating HMI

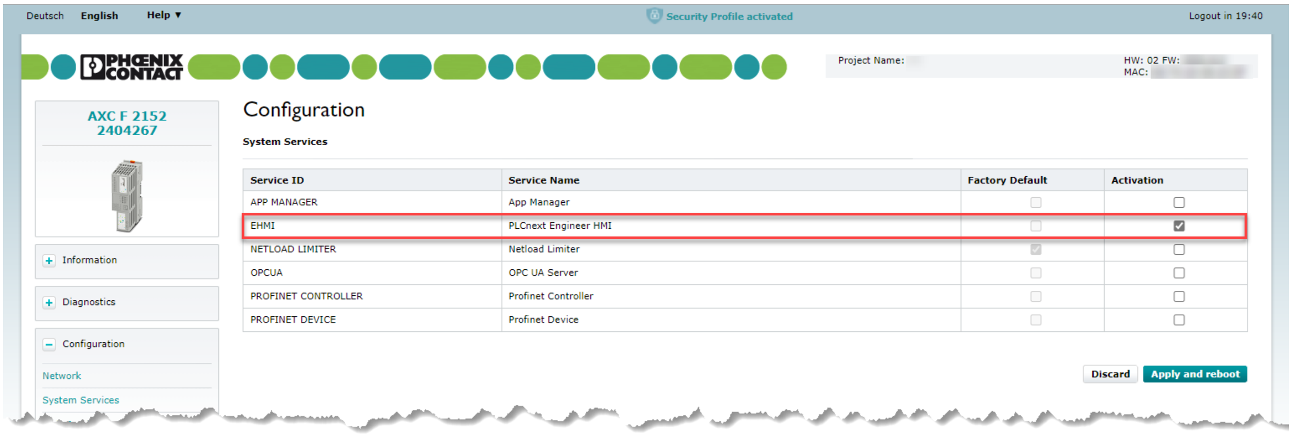
Activating PLCnext Engineer HMI

ℹ For information on how to create a PLCnext Engineer HMI application, refer to the topic Creating a PLCnext Engineer HMI application in the PLCnext Technology - Info Center.

ℹ For information on user roles and permissions, refer to the User Authentication WBM topic in the main PLCnext Technology - Info Center.

Before you can use an HMI application with an activated Security Profile, you must activate the PLCnext Engineer HMI. To do this, proceed as follows:

- Log in to the WBM.
- Open the **System Services** page (**Configuration** → **System Services**) in the WBM.
- Activate the checkbox of the PLCnext Engineer HMI.
- Click the **Apply and reboot** button.



Configuration

System Services

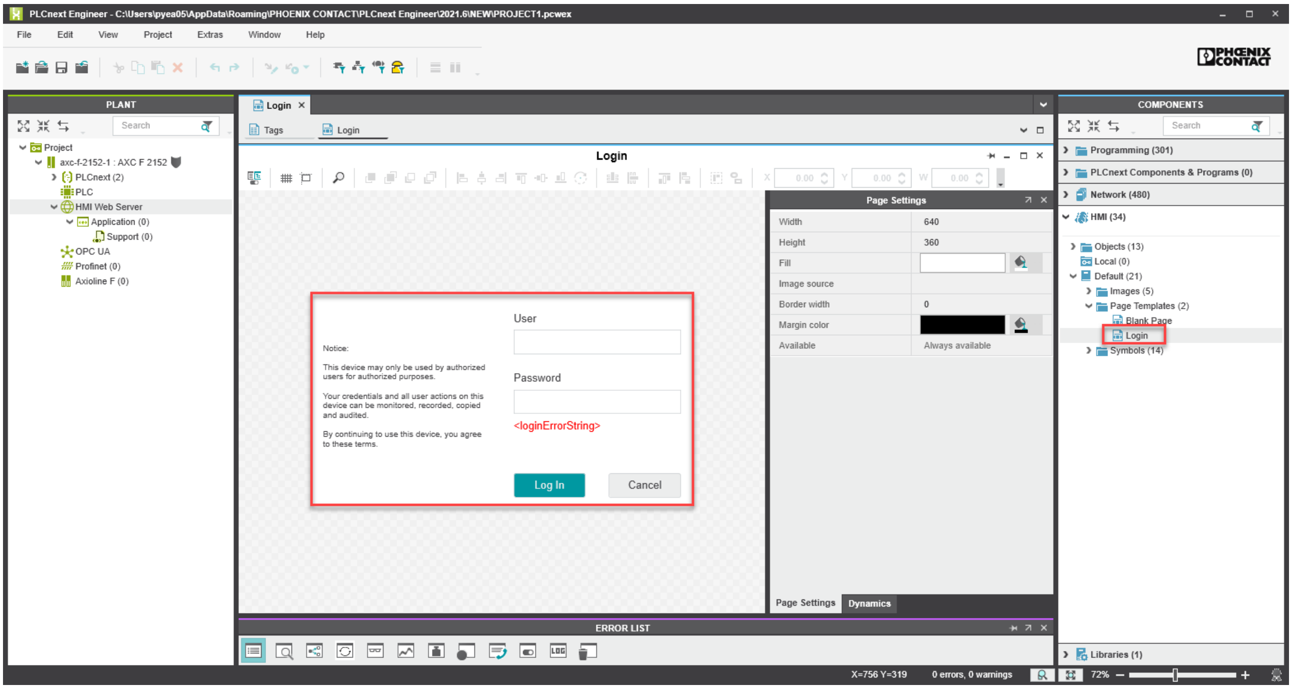
Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	□	□
EHMI	PLCnext Engineer HMI	□	☑
NETLOAD LIMITER	Netload Limiter	☑	□
OPCUA	OPC UA Server	□	□
PROFINET CONTROLLER	Profinet Controller	□	□
PROFINET DEVICE	Profinet Device	□	□

After the PLCnext Control has rebooted, you can use your HMI application.

...continuation see next page...

Adding and editing the login dialog

In the security context, every access to an HMI application must be secured via a login dialog. This must contain a corresponding system use notification. PLCnext Engineer provides a page template with a login dialog with a system use notification that you can insert into your project.



PLCnext Engineer - C:\Users\pyea05\AppData\Roaming\PHOENIX CONTACT\PLCnext Engineer\2021.6\NEW\PROJECT1.pcwex

Notice:

This device may only be used by authorized users for authorized purposes.

Your credentials and all user actions on this device can be monitored, recorded, copied and audited.

By continuing to use this device, you agree to these terms.

User

Password

<loginErrorString>

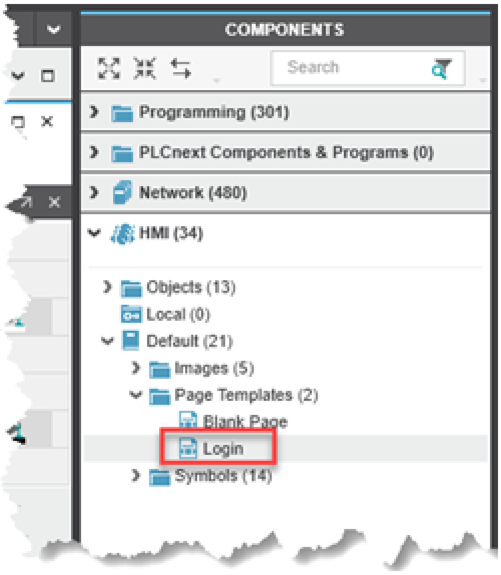
Page Settings

Width	640
Height	360
Fill	
Image source	
Border width	0
Margin color	
Available	Always available

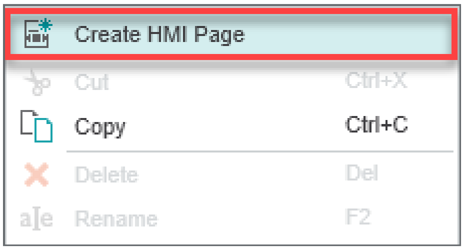
X=756 Y=319   0 errors, 0 warnings   72%

To insert the login page template into your project, proceed as follows:

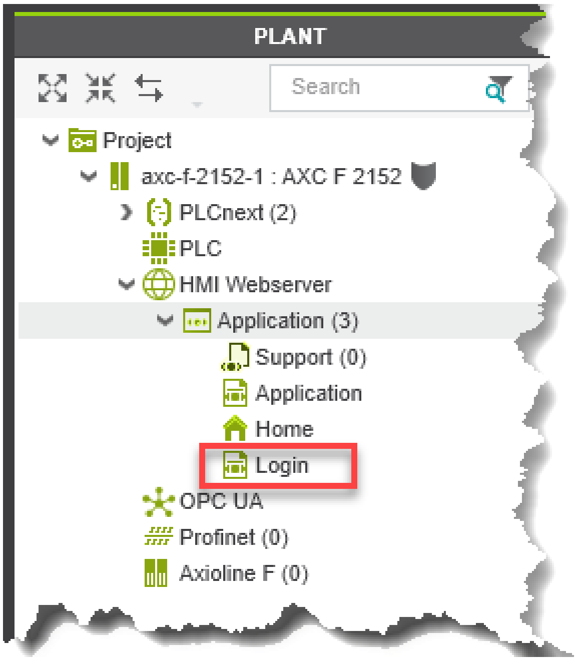
- Open your project in PLCnext Engineer.
- In the COMPONENTS area, right-click the **Login** page template (**Components** → **HMI** → **Default** → **Page Templates** → **Login**).



- Click **Create HMI Page**.

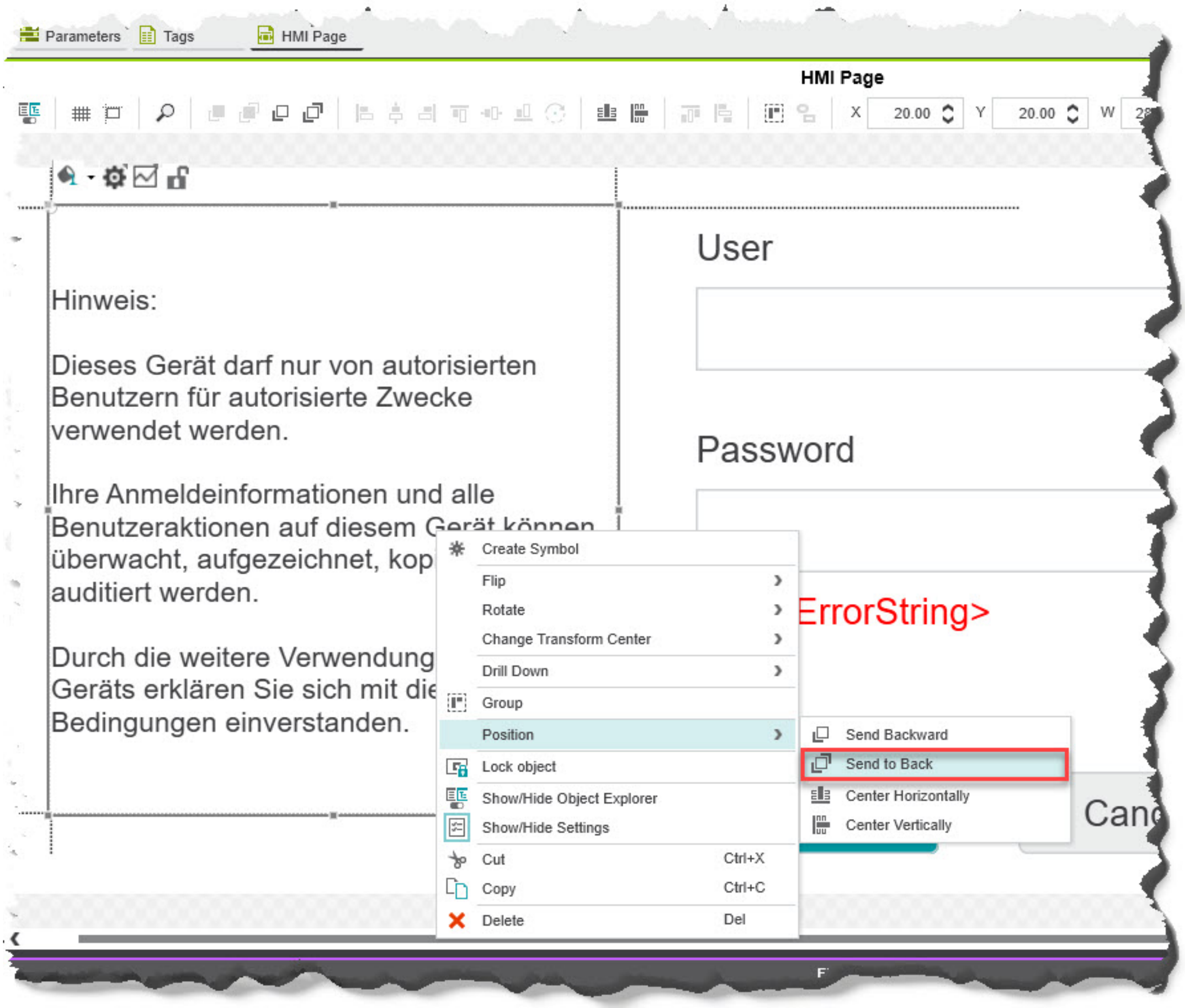


↪ The login page template is now a child element of the **HMI Webserver** node in the PLANT area.



- In the PLANT area, double-click the login page template.
  ↪The HMI editor group with the associated editors is opened.
- On the **HMI Page** tab, read the contained system use notification and check whether the text is valid for the respective application in the respective jurisdiction and adapt it if necessary. If necessary, consider the respective national language.
- To edit the default system use notification, double-click the text.

- You can create different language variants of the system use notification. To display the system use notification in another language, select the **Send to Back** menu item in the context menu.



Hinweis:

Dieses Gerät darf nur von autorisierten Benutzern für autorisierte Zwecke verwendet werden.

Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Gerät können überwacht, aufgezeichnet, kop auditiert werden.

Durch die weitere Verwendung Geräts erklären Sie sich mit die Bedingungen einverstanden.

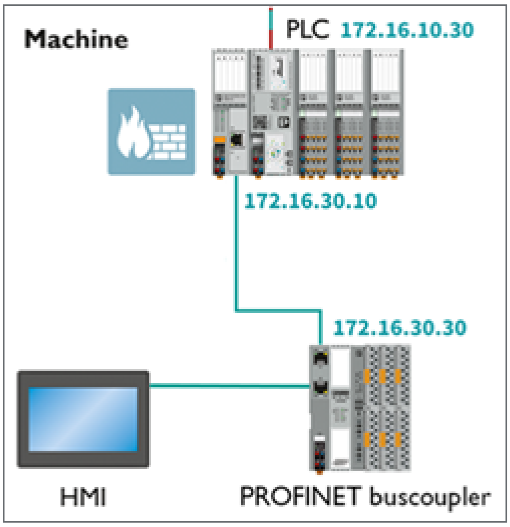
- Save your project.

↪ The login dialog is ready for use in the security context.

Activating PROFINET

A large port range is required for the use of PROFINET as the system automatically selects the required ports depending on the network configuration.
To restrict access to the PROFINET interfaces, the IP addresses of the PROFINET devices must be configured so that only the controller and the device, and possibly also the engineering (supervisor), can communicate with each other.
From the controller perspective, the PROFINET buscoupler must be configured in the firewall as an input rule (**Interface** and **From IP**).
The output rule generally defines the ports from which data is sent and the PROFINET buscoupler (**To IP**) is defined as the recipient of the data.

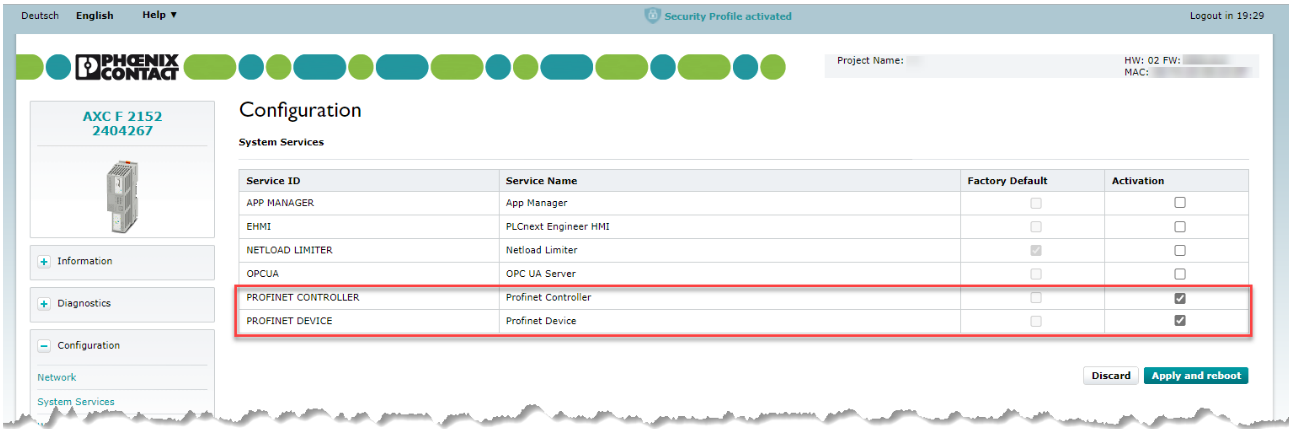
In the security context in the "Machine" subnetwork, the PROFINET buscoupler has the IP address 172.16.30.30, which must be configured.
Firewall rules for the device, if available (e.g. AXC F2152 as PROFINET device), must be set in the same way.



(See topic Security context for embedding in the wider context and topic Deriving IP addresses for the assignment of IP addresses.)

After you have performed a threat analysis and implemented appropriate protective measures from the security context, you can activate PROFINET.

- Log in to the WBM.
- Open the **System Services** page (**Configuration** → **System Services**) in the WBM.
- Activate the checkboxes of the PROFINET Controller and the PROFINET Device (depending on what is needed).
- Click the **Apply and reboot** button.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

Configuration

System Services

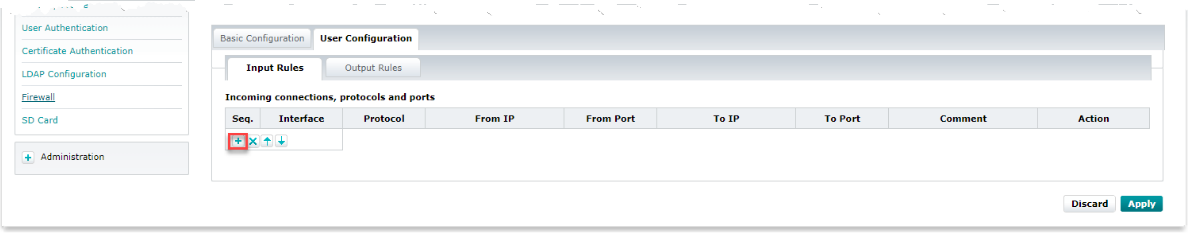
Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	□	□
EHMI	PLCnext Engineer HMI	□	□
NETLOAD LIMITER	Netload Limiter	☑	□
OPCUA	OPC UA Server	□	□
PROFINET CONTROLLER	Profinet Controller	□	☑
PROFINET DEVICE	Profinet Device	□	☑

After the PLCnext Control has rebooted, you must configure the firewall input and output rules. To do this, proceed as follows:

Input rules

> **Note:** To select the correct interfaces, please refer to the corresponding PLCnext Control topic in the appendix (e. g. AXC F 2152).

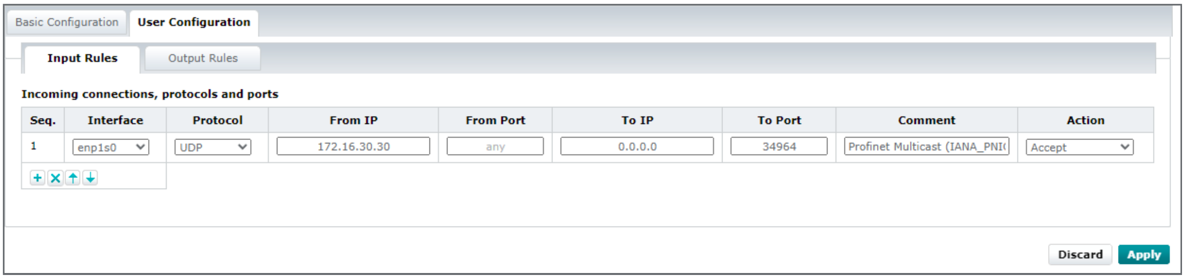
- Open the **Firewall** page (**Security** → **Firewall**) in the WBM.
- Open the **User Configuration** tab.
- On the **Input Rules** tab, add a new rule via the **+** .



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action

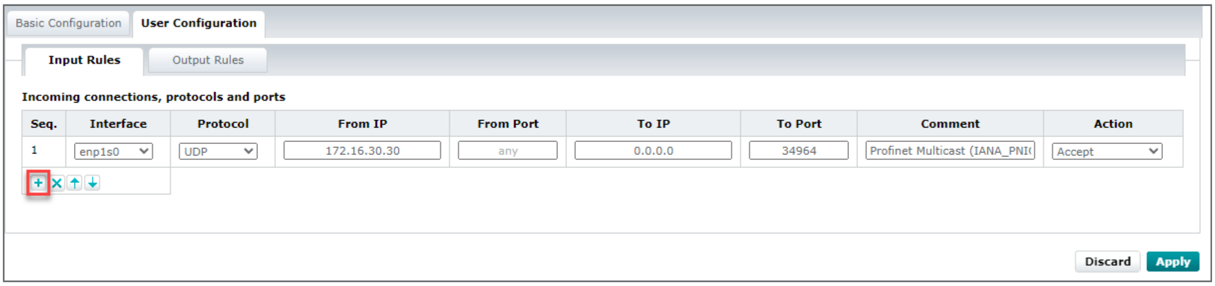
- Provide the following information:
  - Select the interface.
  - Select the protocol.
  - Enter the IP address range.
  - Enter a target port.
  - Select the action **Accept**.



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	enp1s0	UDP	172.16.30.30	any	0.0.0.0	34964	Profinet Multicast (IANA_PNI(	Accept

- Click the **Apply** button.
- On the **Input Rules** tab, add another new rule via the **+** .

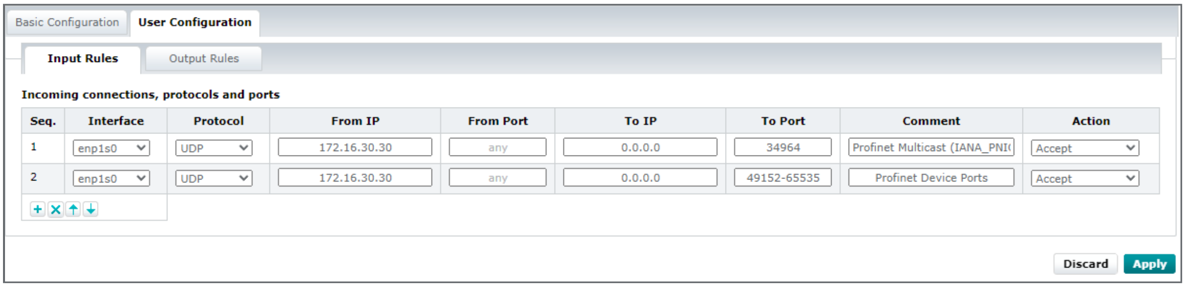


Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	enp1s0	UDP	172.16.30.30	any	0.0.0.0	34964	Profinet Multicast (IANA_PNI(	Accept

- Provide the following information:

  - Select the interface.
  - Select the protocol.
  - Enter the IP address range.
  - Enter a target port.
  - Select the action **Accept**.



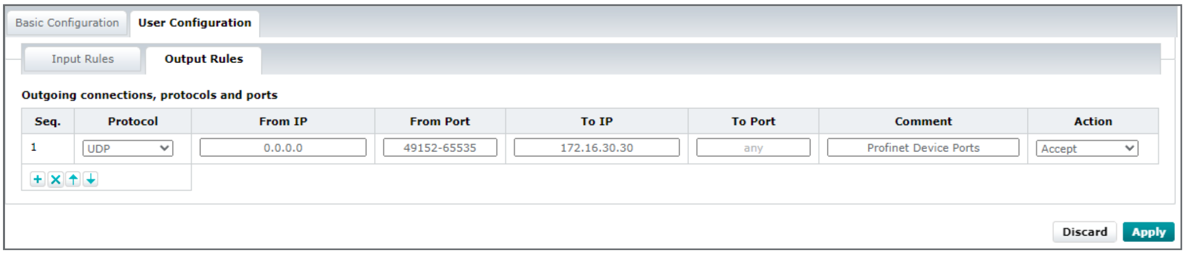
Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	enp1s0	UDP	172.16.30.30	any	0.0.0.0	34964	Profinet Multicast (IANA_PNI(	Accept
2	enp1s0	UDP	172.16.30.30	any	0.0.0.0	49152-65535	Profinet Device Ports	Accept

- Click the **Apply** button.

Output rules

- Open the **Firewall** page (**Security** → **Firewall**) in the WBM.
- Open the **User Configuration** tab.
- On the **Output Rules** tab, add a new rule via the ✚.
- Provide the following information:
  - Select the interface.
  - Select the protocol.
  - Enter the IP address range.
  - Enter a target port.
  - Select the action **Accept**.



Outgoing connections, protocols and ports

Seq.	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	UDP	0.0.0.0	49152-65535	172.16.30.30	any	Profinet Device Ports	Accept

- Click the **Apply** button.

> **Note:** To make sure that all newly applied input and output rules are actively used (even for connections that have already been established), **restart** the PLCnext Control.

Activating the App Manager

NOTICE

Installing apps can compromise security

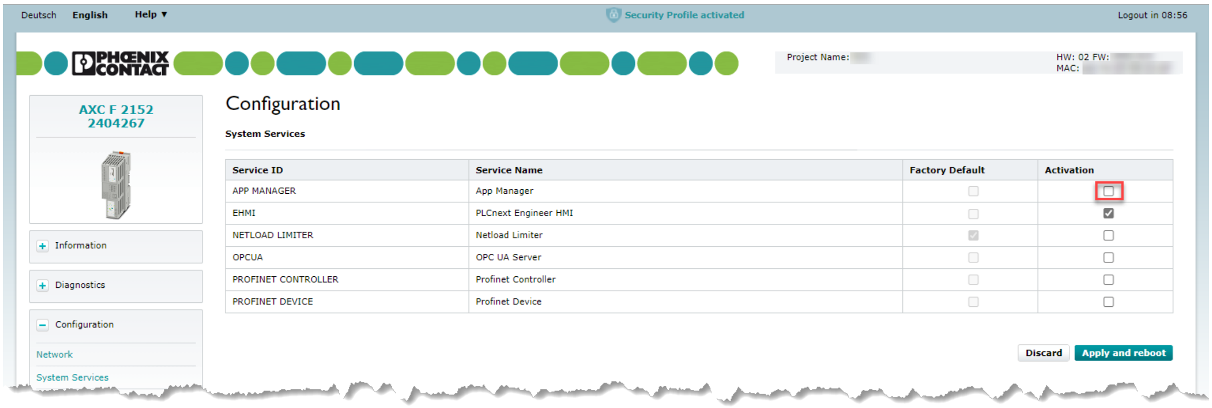
Before installing an app, you must perform a risk analysis of the app and its impact on the security of the device and the application, taking into account the overall security context. In particular, investigate the following effects on the device and application:

- Data critically estimation
- Data in rest
- Data in transmission
- Integrity and authenticity
- PLCnext User Management
- Communication configuration (e. g. network interfaces, ports) and firewall integration
- Least functionality strategy
- Notifications
- Mobile and malicious code protection

To install apps, you must have admin rights. Otherwise, it is not possible to check and adjust the configurations in the WBM that may have been changed by the app due to the lack of access to the App Manager.

To install and license apps from the PLCnext Store, you must first activate the App Manager. Proceed as follows:

- Log in to the WBM.
- Open the System Services page (Configuration System → Services).
- Activate the checkbox of the App Manager.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

AXC F 2152
2404267

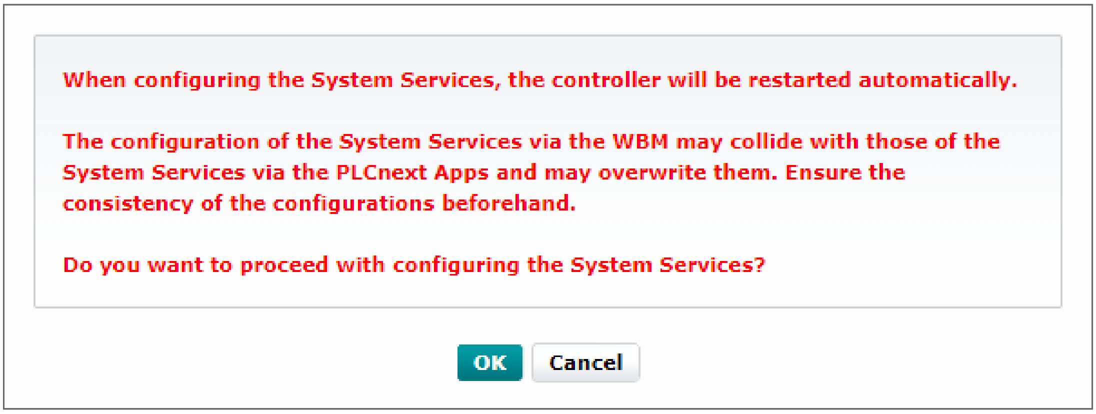
Configuration

System Services

Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	□	□
EHMI	PLCnext Engineer HMI	□	☑
NETLOAD LIMITER	Netload Limiter	☑	□
OPCUA	OPC UA Server	□	□
PROFINET CONTROLLER	Profinet Controller	□	□
PROFINET DEVICE	Profinet Device	□	□

- Click the Apply and reboot button.

A warning note opens.



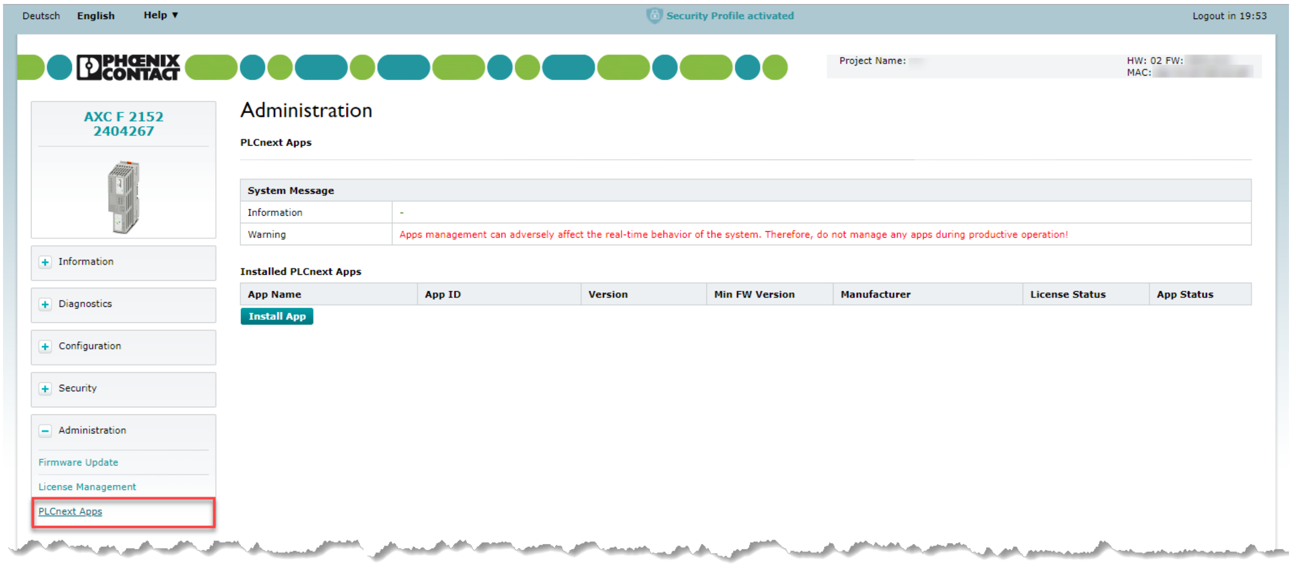
When configuring the System Services, the controller will be restarted automatically.

The configuration of the System Services via the WBM may collide with those of the System Services via the PLCnext Apps and may overwrite them. Ensure the consistency of the configurations beforehand.

Do you want to proceed with configuring the System Services?

- Read the warning note and if you want to proceed, click the OK button.

After the PLCnext Control has been restarted, the PLCnext Apps page is available (Administration → PLCnext Apps).



Administration

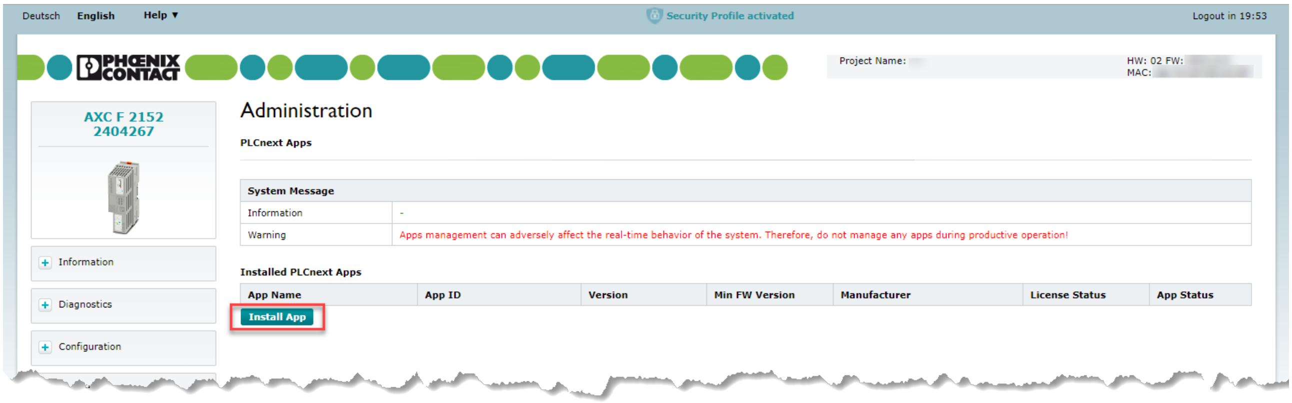
PLCnext Apps

System Message	
Information	-
Warning	Apps management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation!

Installed PLCnext Apps

App Name	App ID	Version	Min FW Version	Manufacturer	License Status	App Status

- Install apps via the Install App button.



Administration

PLCnext Apps

System Message	
Information	-
Warning	Apps management can adversely affect the real-time behavior of the system. Therefore, do not manage any apps during productive operation!

Installed PLCnext Apps

App Name	App ID	Version	Min FW Version	Manufacturer	License Status	App Status

Note: You may need to install licenses.

Security note

To make sure that software or firmware files downloaded via internet have not been corrupted or tampered, perform an integrity check of the downloaded files. You can find further information in Integrity check of downloaded files.

For information on license management, refer to the main PLCnext Technology - Info Center or to the PLCnext Store - Info Center.

After you have installed the app, you must check which user rights, firewall settings and System Services the app requires.

- Make the required settings in the WBM, taking into account the risk analysis performed.
- After app installation, check the System Services settings.
  Apps can enable or disable System Services during installation. For example, when you launch container apps, the controller automatically reboots. This causes the App Manger to be disabled if a Security Profile is active. You must re-enable the App Manger to check the installed apps or to install additional apps.

Note: Before you start up the system after installing apps, you must deactivate the App Manager in the WBM!

Note: The integrity of libraries can be checked with hash values.

Activating software updates

Central software updates will be possible via the Device and Update Management Service. You must first activate the service on the System Services page in the WBM.

- Log in to the WBM.
- Open the **System Services** page (**Configuration** → **System Services**) in the WBM.
- Activate the checkboxes of the OPC UA® Server and the Software Update via Device and Update Management.
- Click the **Apply and reboot** button.

After the PLCnext Control has rebooted, you must enable the port range to be able to communicate with the OPC UA® devices. To do this, proceed as follows:

- Open the **Firewall** page (**Security** → **Firewall**) in the WBM.
- Open the **Basic Configuration** tab.
- In the **Basic Rules** section, select **Continue** from the drop-down list for OPC UA ports in the **Action** column.
- Click the **Apply** button.
- Open the **User Configuration** tab.
- On the **Input Rules** tab, add a new rule via the +.
- Provide the following information:
  - Select the interface.
  - Select the protocol.
  - Enter the IP address range.
  - Enter the target port 4840.
  - Select the action **Accept**.
- Click the **Apply** button.

Perform backup and restore

General information

Backup and restore mechanisms are used for fast recommissioning after a possible system failure or device reset. The backups are signed and managed by the Device and Update Management (DaUM) and transferred to it.

The following data are included in the backup:

- Application
- Configuration

Note: The firmware is not included in the backup. Before restore, you must validate the appropriate firmware version and install it via the DaUM according to the application and configuration requirements.

The following application data are included in the backup:

- PLC program
- Safety PLC program
- eHMI application
- APP application default data (depending on app development)

The following configuration data (top level view) are included in the backup:

- Network
- Time configuration
- System services
- Web services
- Certificates
- Firewall
- SD card
- Security Profile
- Users
- Syslog
- APPs
- SSH access

Note: The licenses can be installed separately depending on the level of restore. Licences are bound to the hardware or the SD card. For more information on licenses, refer to the PLCnext Store Info Center.

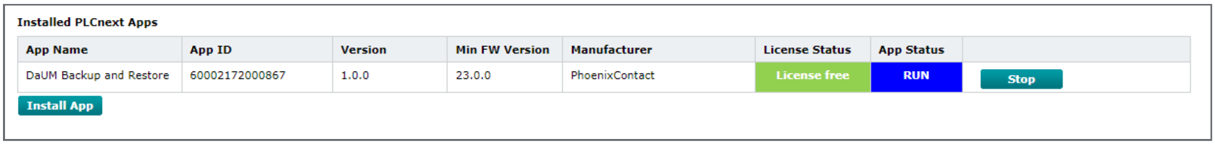
Backup and restore

To perform a backup and restore in this security context, use the ***DaUM Backup and Restore*** app. You can get the app via the PLCnext Storeand use it via the Device and Update Management.

Note:

- You need admin rights to install and use the app.
- To perform a backup, you must first create a new user named "DeviceBackup" with the following rights: FileReader, FileWriter, SoftwareUpdate.
  For more information on the different users, roles and rights, refer to the User Authentication topic in the main PLCnext Technology - Info Center.
- To perform a restore, you need admin rights.

- Make sure the App Manager is activated.
- Log in to the WBM.
- Open the **PLCnext Apps** page (**Administration** → **PLCnext Apps**), install and start the app.

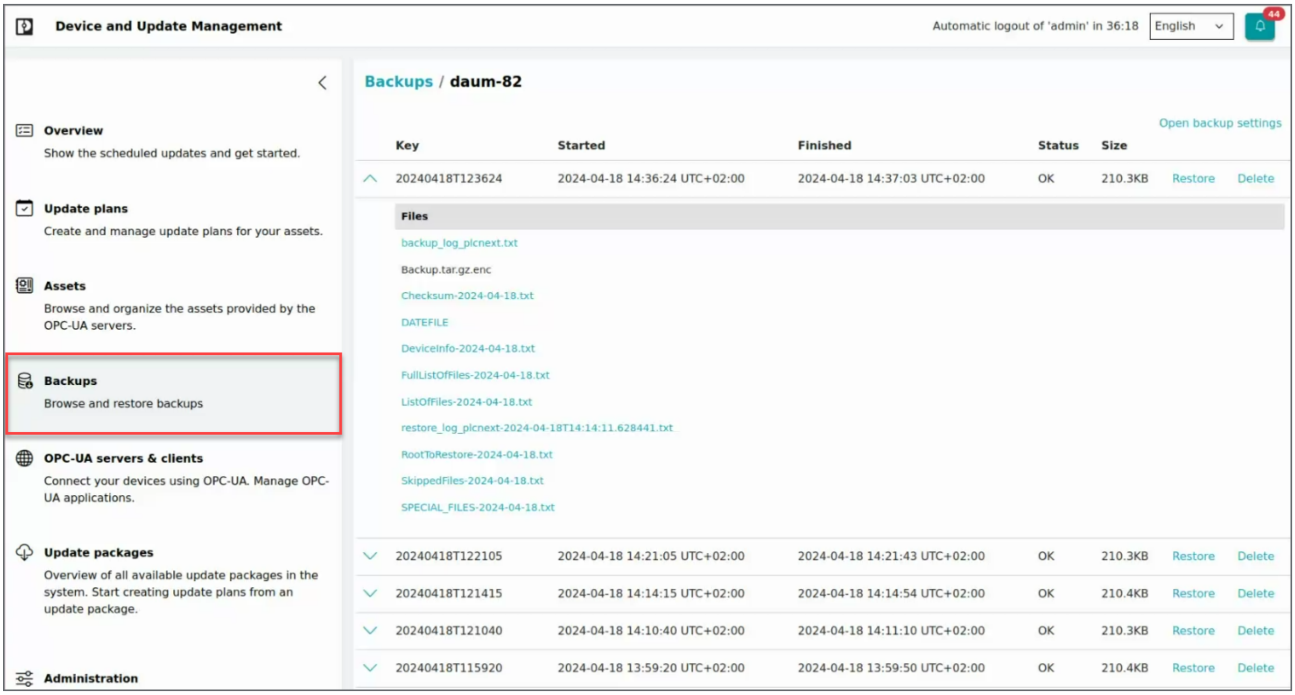


Installed PLCnext Apps

App Name	App ID	Version	Min FW Version	Manufacturer	License Status	App Status	
DaUM Backup and Restore	60002172000867	1.0.0	23.0.0	PhoenixContact	License free	RUN	Stop

- Open the Device and Update Management and proceed as described in the main PLCnext Technology - Info Center.

Note: Backups can be generated during normal operation of the application. However, the application must be designed in such a way that a backup that is started at maximum CPU and memory load does not impair execution or trigger a watchdog.



Device and Update Management

Automatic logout of 'admin' in 36:18

Overview
Show the scheduled updates and get started.

Update plans
Create and manage update plans for your assets.

Assets
Browse and organize the assets provided by the OPC-UA servers.

Backups
Browse and restore backups

OPC-UA servers & clients
Connect your devices using OPC-UA. Manage OPC-UA applications.

Update packages
Overview of all available update packages in the system. Start creating update plans from an update package.

Administration

Backups / daum-82

Key	Started	Finished	Status	Size		
20240418T123624	2024-04-18 14:36:24 UTC+02:00	2024-04-18 14:37:03 UTC+02:00	OK	210.3KB	Restore	Delete

Files

backup_log_plcnext.txt
Backup.tar.gz.enc
Checksum-2024-04-18.txt
DATEFILE
DeviceInfo-2024-04-18.txt
FullListOfFiles-2024-04-18.txt
ListOfFiles-2024-04-18.txt
restore_log_plcnext-2024-04-18T14:14:11.628441.txt
RootToRestore-2024-04-18.txt
SkippedFiles-2024-04-18.txt
SPECIAL_FILES-2024-04-18.txt

Key	Started	Finished	Status	Size		
20240418T122105	2024-04-18 14:21:05 UTC+02:00	2024-04-18 14:21:43 UTC+02:00	OK	210.3KB	Restore	Delete
20240418T121415	2024-04-18 14:14:15 UTC+02:00	2024-04-18 14:14:54 UTC+02:00	OK	210.4KB	Restore	Delete
20240418T121040	2024-04-18 14:10:40 UTC+02:00	2024-04-18 14:11:10 UTC+02:00	OK	210.3KB	Restore	Delete
20240418T115920	2024-04-18 13:59:20 UTC+02:00	2024-04-18 13:59:50 UTC+02:00	OK	210.4KB	Restore	Delete

Account management

Account management

Operating a PLCnext Control in a security context includes the following steps regarding account management:

- Creating users
- Password complexity rules
- Checking the validity of passwords
- Configuring authentication errors and sessions
- Configuring Active Directory Connection

Configuring Active Directory Connection

With PLCnext you are able to connect Active Directory servers via LDAP.

ℹ For further information, refer to the topic LDAP configuration in the main PLCnext Technology - Info Center.

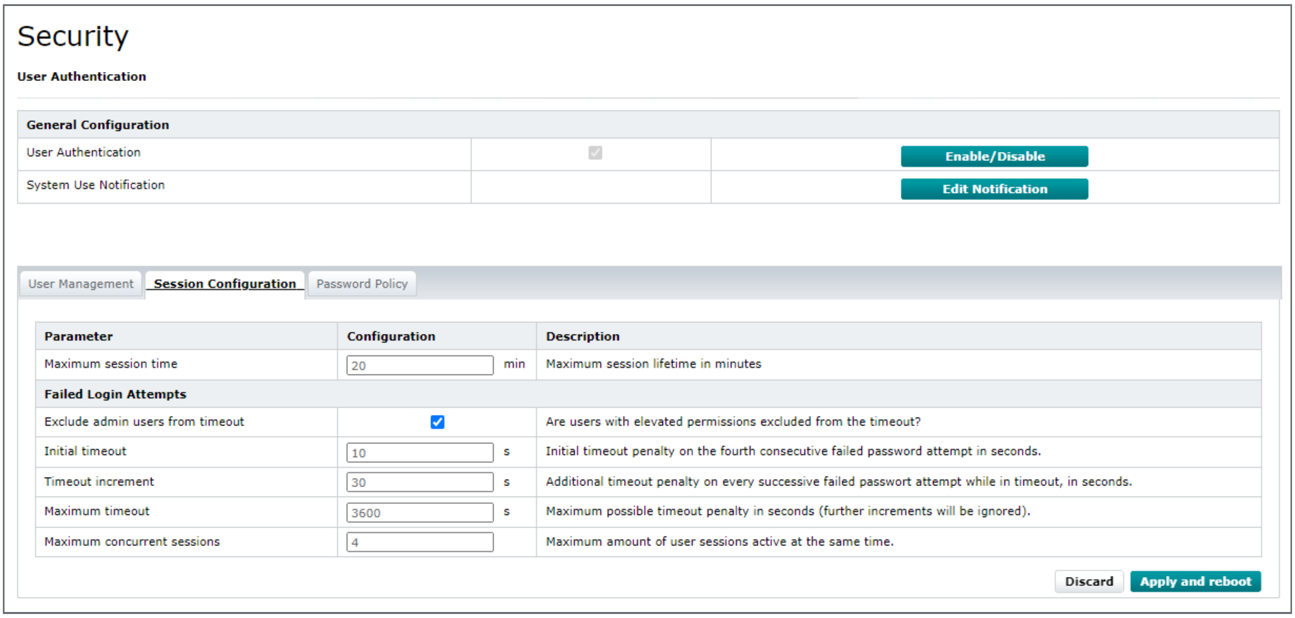
Configuring authentication errors and sessions

Session Configuration

- Log in to the WBM.
- Open the **User authentication** page (**Security** → **User authentication**).

On the **Session Configuration** tab, you configure the maximum session time, the timeout penalty times and the maximum number of concurrent sessions.

In the following screenshot you see the default settings:



Security

User Authentication

General Configuration		
User Authentication	☑	Enable/Disable
System Use Notification		Edit Notification

Parameter	**Configuration**		**Description**
Maximum session time	20	min	Maximum session lifetime in minutes
Failed Login Attempts			
Exclude admin users from timeout	☑		Are users with elevated permissions excluded from the timeout?
Initial timeout	10	s	Initial timeout penalty on the fourth consecutive failed password attempt in seconds.
Timeout increment	30	s	Additional timeout penalty on every successive failed passwort attempt while in timeout, in seconds.
Maximum timeout	3600	s	Maximum possible timeout penalty in seconds (further increments will be ignored).
Maximum concurrent sessions	4		Maximum amount of user sessions active at the same time.

- **Maximum session time** : After 20 minutes of inactivity the session is automatically closed.
- **Exclude admin users from timeout** : This setting applies to all users for whom the "Admin Ruleset" ruleset is stored.

> **Note:** Check if you really want to exclude users from the timeout and adjust the setting if necessary.

- **Initial timeout** : After three failed password attempts, there is a penalty time of 10 seconds.
- **Timeout increment** : After four failed password attempts, there is an additional penalty time of 30 seconds.
- **Maxiumum timeout** : The maximum timeout is 3600 seconds. This means that you can then start another password attempt every 3600 seconds.
  Alternatively, you can ask the admin to delete your user and create a new one. Then you can start entering the password again.
- **Maximum concurrent sessions** : With this configuration, you define how many communication channels may exist simultaneously. Adjust the value to your circumstances if necessary. Keep in mind the principle of least functionality!

Checking the validity of passwords

Changing the default password

After the admin has created a user account with password, you must change the default password. If you do not change the default password, you will receive appropriate warnings.

Password expiration

If a password is about to expire or has already expired, appropriate warnings are displayed.

Checking password validity in the WBM

- Log in to the WBM.
- Open the **Cockpit** page (**Diagnostics** → **Cockpit**) in the WBM.

Based on the messages, you can check whether the passwords are still valid and whether a user has already changed his default password.

Password complexity rules

The password complexity rules are predefined and depend on the rights of each user. You may need to adjust the rule set to meet the needs of your application.

Pre-defined rule sets

With firmware 2022.0 LTS and 2023.0 LTS, the "Admin Ruleset" and the "Default Ruleset" are pre-defined as described below.

- Adapt the rule set to the conditions of your application.

Admin Ruleset

We advise that the user roles Admin, SecurityAdmin, SecurityAuditor, UserManager, CertificateManager and Engineer have the rule set "Admin Ruleset" by default. The following password rules are set:

- The username must not be included in the password.
- The last five passwords must not be reused.
- The password must contain at least ten characters.
- The password must contain at least one uppercase letter and one lowercase letter.
- The password must contain at least one number.
- The password must contain at least one symbol. The allowed symbols are: `{}()[]#,;.:^?!|_'~@$%/\=+-*&`

Default Ruleset

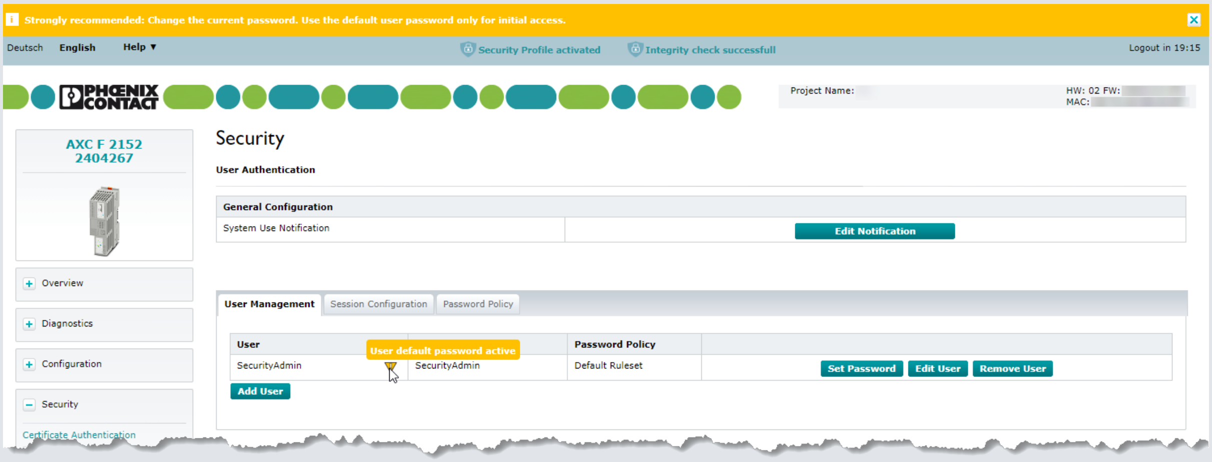
All other user roles may have the rule set "Default Ruleset" by default:

- The username must not be included in the password.
- The last five passwords must not be reused.
- The password must contain at least eight characters.
- The password must contain at least one uppercase letter and one lowercase letter.
- The password must contain at least one number.

Creating users

The SecurityAdmin can only configure the system. All other activities must be performed by other users with other roles. You need at least a Security Auditor to access the security notifications, an Engineer to program in PLCnext Engineer and an Operator to operate an HMI. Below you will see how to add these users with their specific roles.

> **Note:** It is strongly recommended that you only use the default user password for the first access. Change the default password immediately after the first access. Observe the password complexity rules .
>
> If you have created a user, you will see a corresponding message in the WBM to change the default password (from firmware 2024.0 LTS).



Strongly recommended: Change the current password. Use the default user password only for initial access.

Security Profile activated

Integrity check successfull

Logout in 19:15

Project Name:

HW: 02 FW:
MAC:

AXC F 2152
2404267

Security

User Authentication

General Configuration	
System Use Notification	Edit Notification

User		Password Policy	
SecurityAdmin	SecurityAdmin	Default Ruleset	Set Password Edit User Remove User

User default password active

ℹ For more information on the different users, roles and rights, refer to the User Authentication topic in the main PLCnext Technology - Info Center.

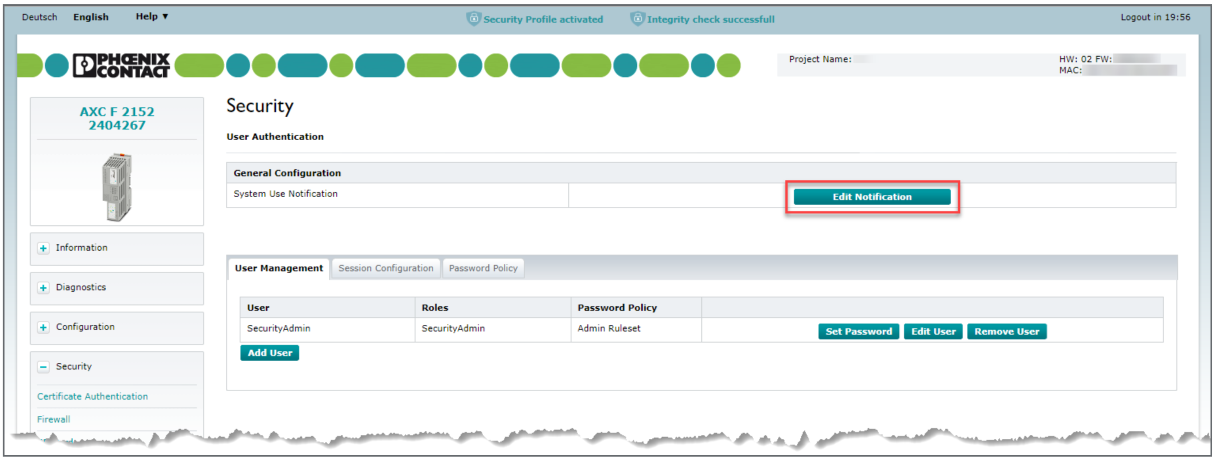
For the following procedures you need **access to the Web-based Management** on the PLCnext Control.

System Use Notification

The system use notification is displayed each time a user wants to log on to the controller. The system use notification is independent of the language of the user interface in WBM and PLCnext Engineer. You should therefore take all required languages into account when editing.

To edit the system use notification, proceed as follows:

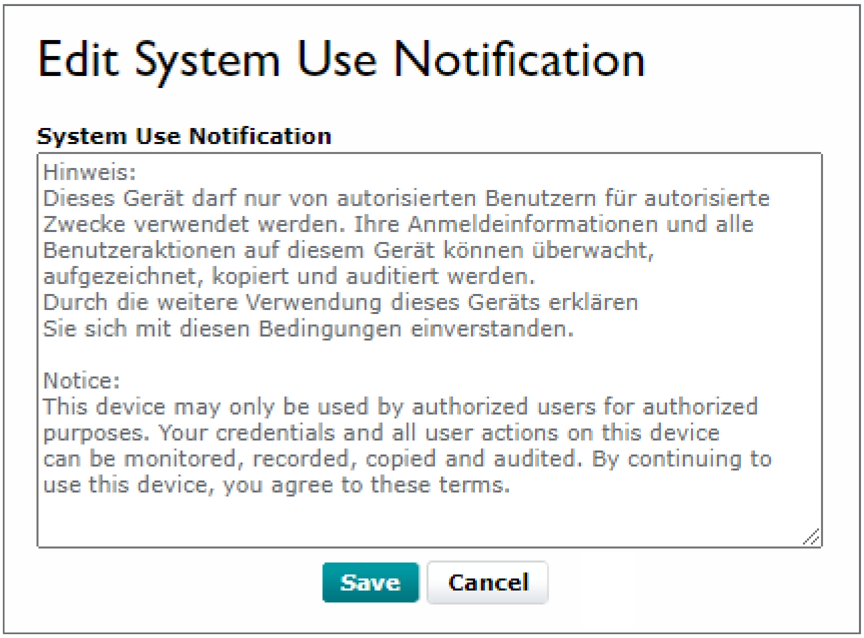
- Click the Edit Notification button.



User	Roles	Password Policy
SecurityAdmin	SecurityAdmin	Admin Ruleset

↪ An input window opens.

- Edit the System Use Notification.



Hinweis:
Dieses Gerät darf nur von autorisierten Benutzern für autorisierte Zwecke verwendet werden. Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Gerät können überwacht, aufgezeichnet, kopiert und auditiert werden.
Durch die weitere Verwendung dieses Geräts erklären Sie sich mit diesen Bedingungen einverstanden.

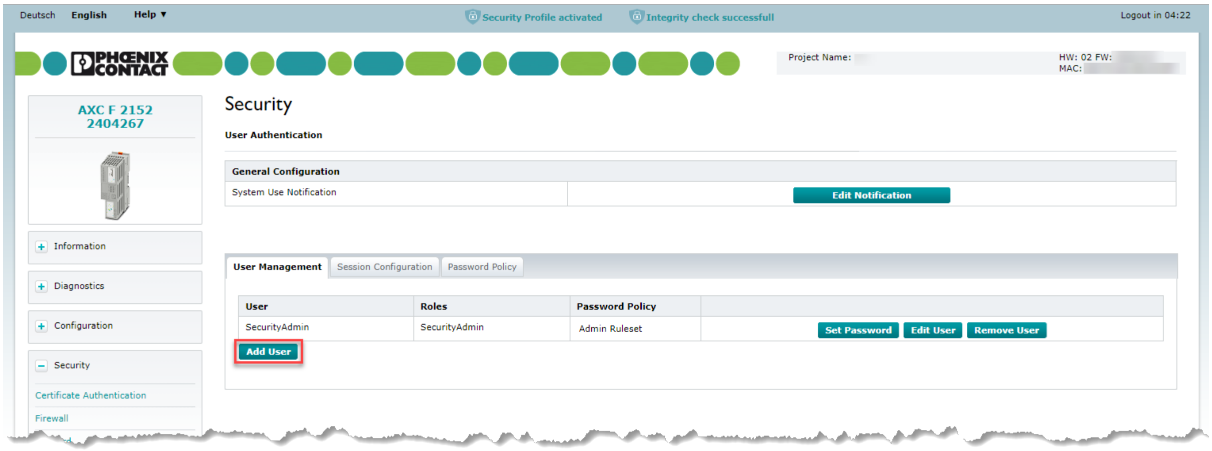
Notice:
This device may only be used by authorized users for authorized purposes. Your credentials and all user actions on this device can be monitored, recorded, copied and audited. By continuing to use this device, you agree to these terms.

- Confirm the entry by clicking the Save button.
↪ The text is then transferred to the controller and stored.

Adding a Security Auditor

To add a Security Auditor, proceed as follows:

- Log in to the WBM.
- Open the Security → User Authentication page in the WBM.
- Click the Add User button.



Security

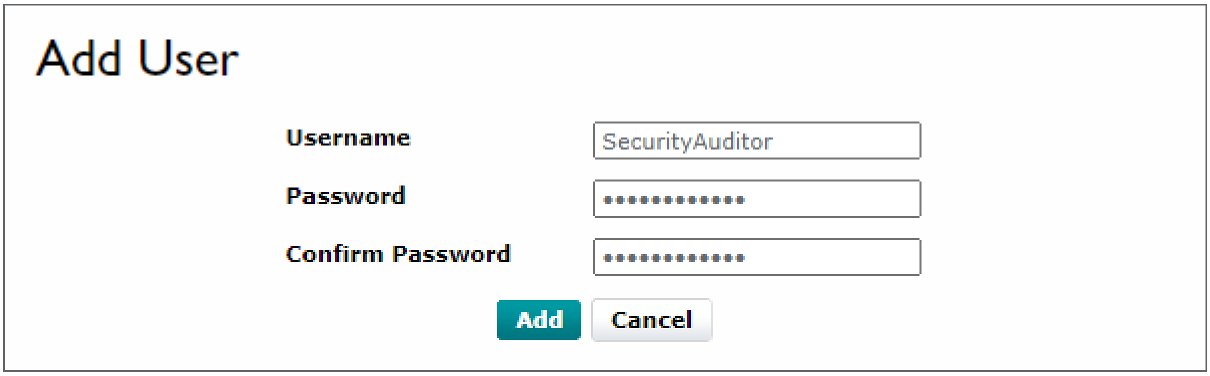
User Authentication

General Configuration	
System Use Notification	Edit Notification

User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User

↪ The dialog Add User opens.

- Enter a username and a password following the password complexity rules.



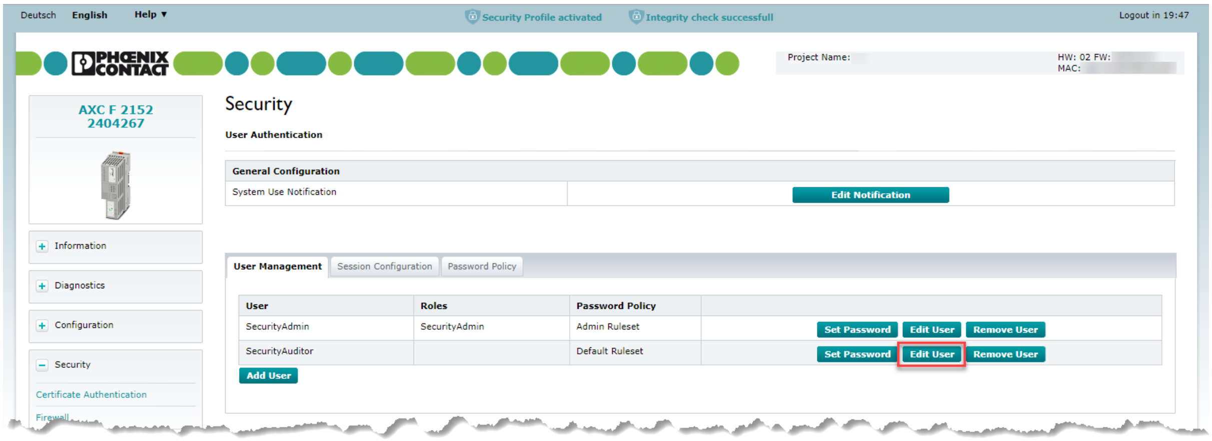
Add User

Username: SecurityAuditor

Password: ●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●

- Click the Add button.
- In the added row SecurityAuditor, click the Edit User button.



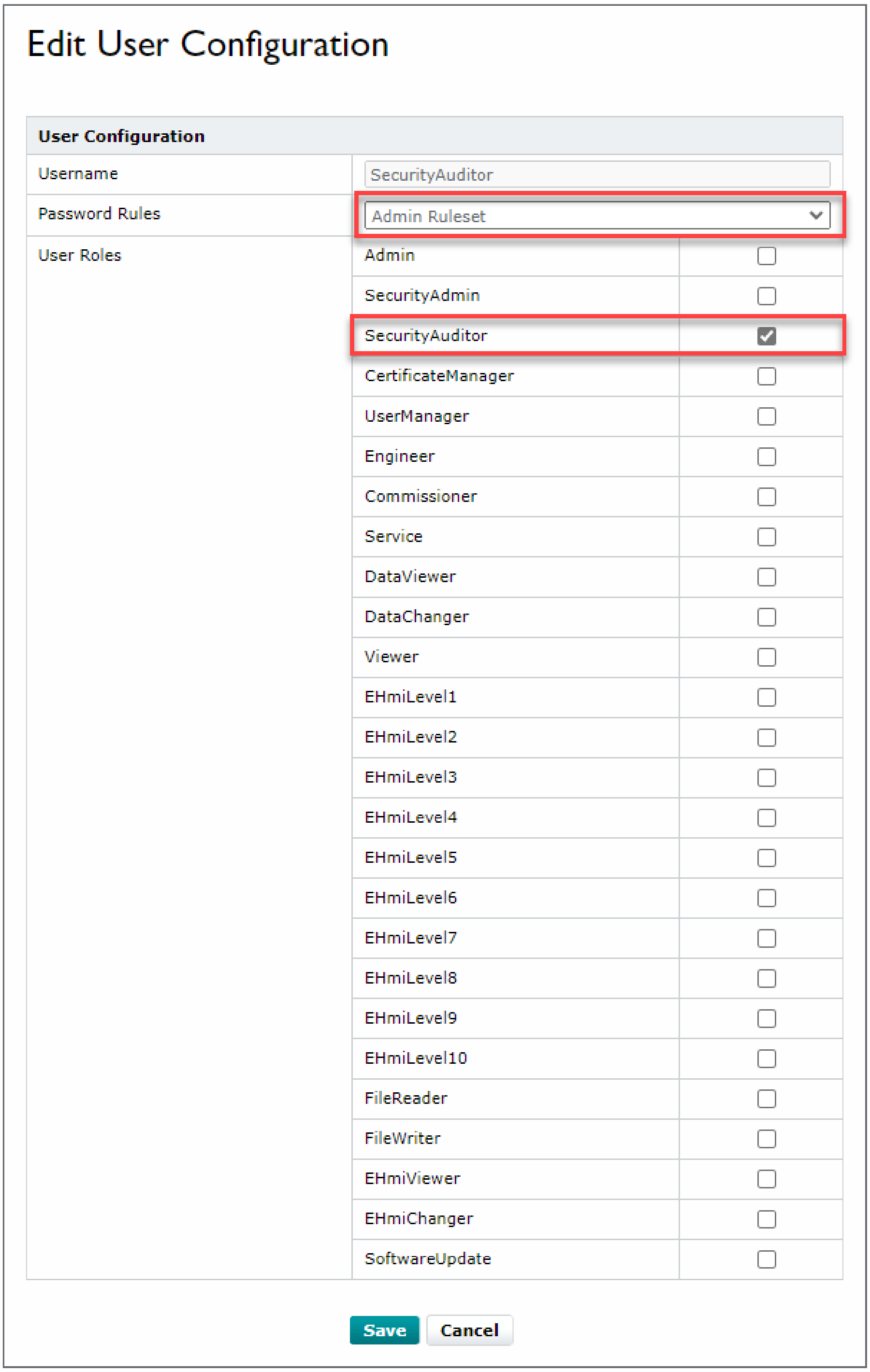
Security

User Authentication

General Configuration	
System Use Notification	Edit Notification

User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
SecurityAuditor		Default Ruleset	Set Password Edit User Remove User

- In the dialog that opens, select a ruleset (**Password rules** ; we advise the "Admin Ruleset") and the appropriate role (**User Roles**) by activating the checkbox at **SecurityAuditor**.



Edit User Configuration

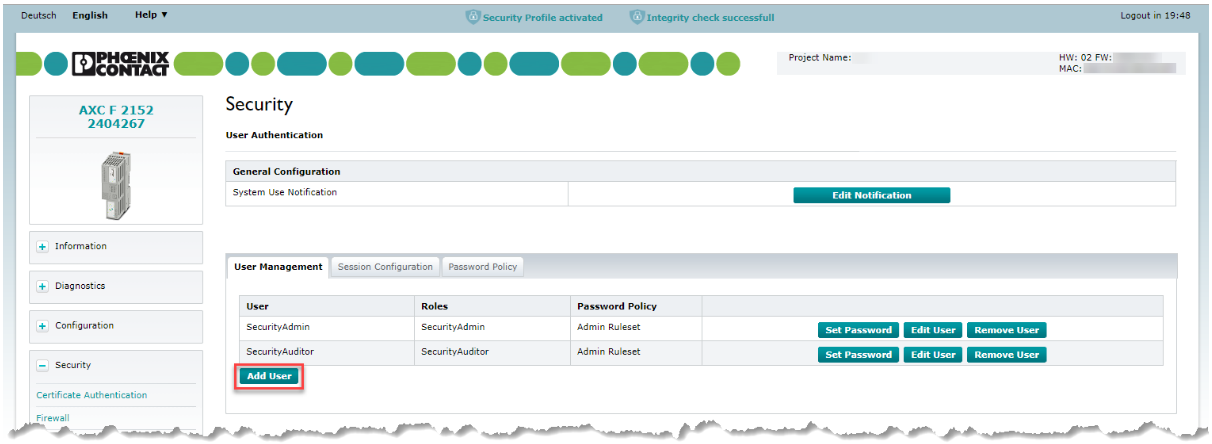
User Configuration		
Username	SecurityAuditor	
Password Rules	Admin Ruleset	
User Roles	Admin	☐
	SecurityAdmin	☐
	SecurityAuditor	☑
	CertificateManager	☐
	UserManager	☐
	Engineer	☐
	Commissioner	☐
	Service	☐
	DataViewer	☐
	DataChanger	☐
	Viewer	☐
	EHmiLevel1	☐
	EHmiLevel2	☐
	EHmiLevel3	☐
	EHmiLevel4	☐
	EHmiLevel5	☐
	EHmiLevel6	☐
	EHmiLevel7	☐
	EHmiLevel8	☐
	EHmiLevel9	☐
	EHmiLevel10	☐
	FileReader	☐
	FileWriter	☐
	EHmiViewer	☐
	EHmiChanger	☐
	SoftwareUpdate	☐

- Click the **Save** button.
↪ You've added a Security Auditor.

Adding an Engineer

To add an Engineer, proceed as follows:

- Log in to the WBM.
- Open the Security → User Authentication page in the WBM.
- Click the Add User button.



Security

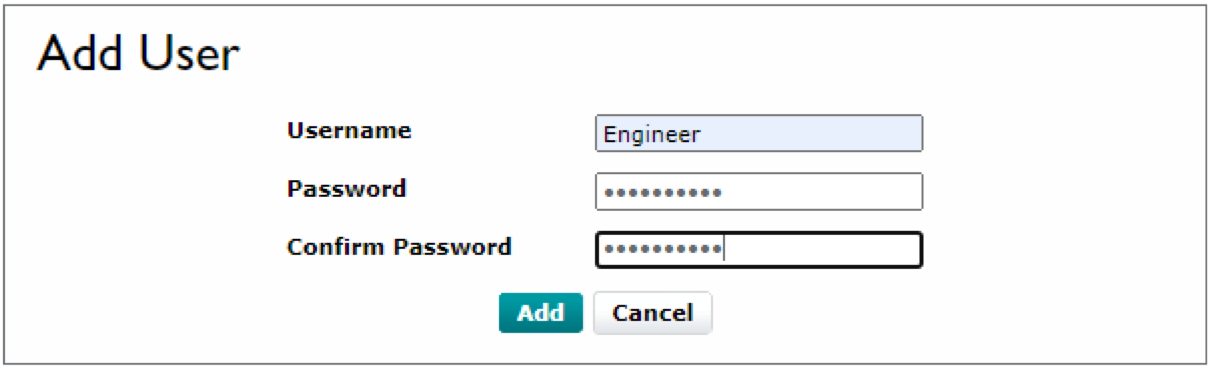
User Authentication

General Configuration	
System Use Notification	Edit Notification

User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
SecurityAuditor	SecurityAuditor	Admin Ruleset	Set Password Edit User Remove User

↪ The dialog Add User opens.

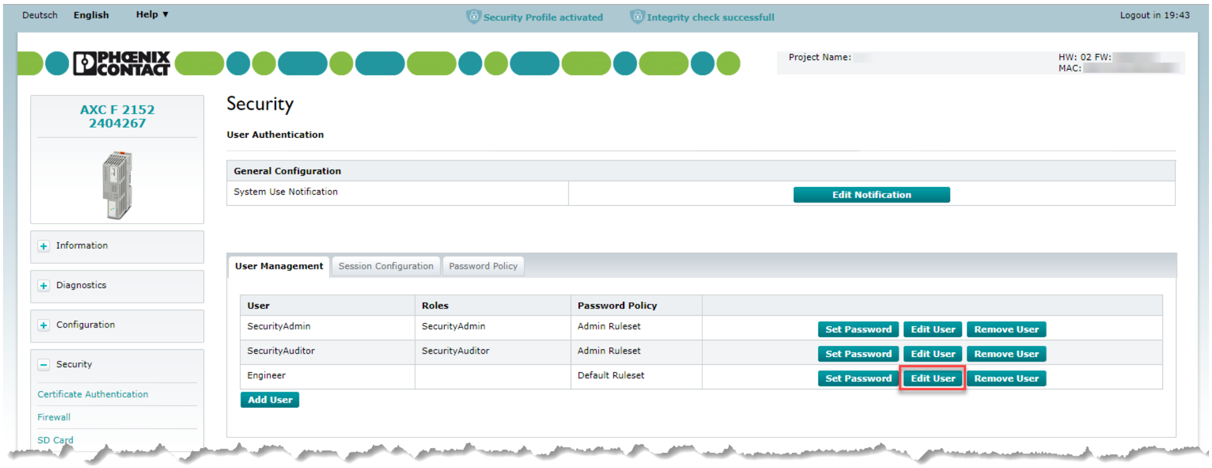
- Enter a username and a password following the password complexity rules.



Add User

Username	Engineer
Password	••••••••••
Confirm Password	••••••••••

- Click the Add button.
- In the added row Engineer, click the Edit User button.



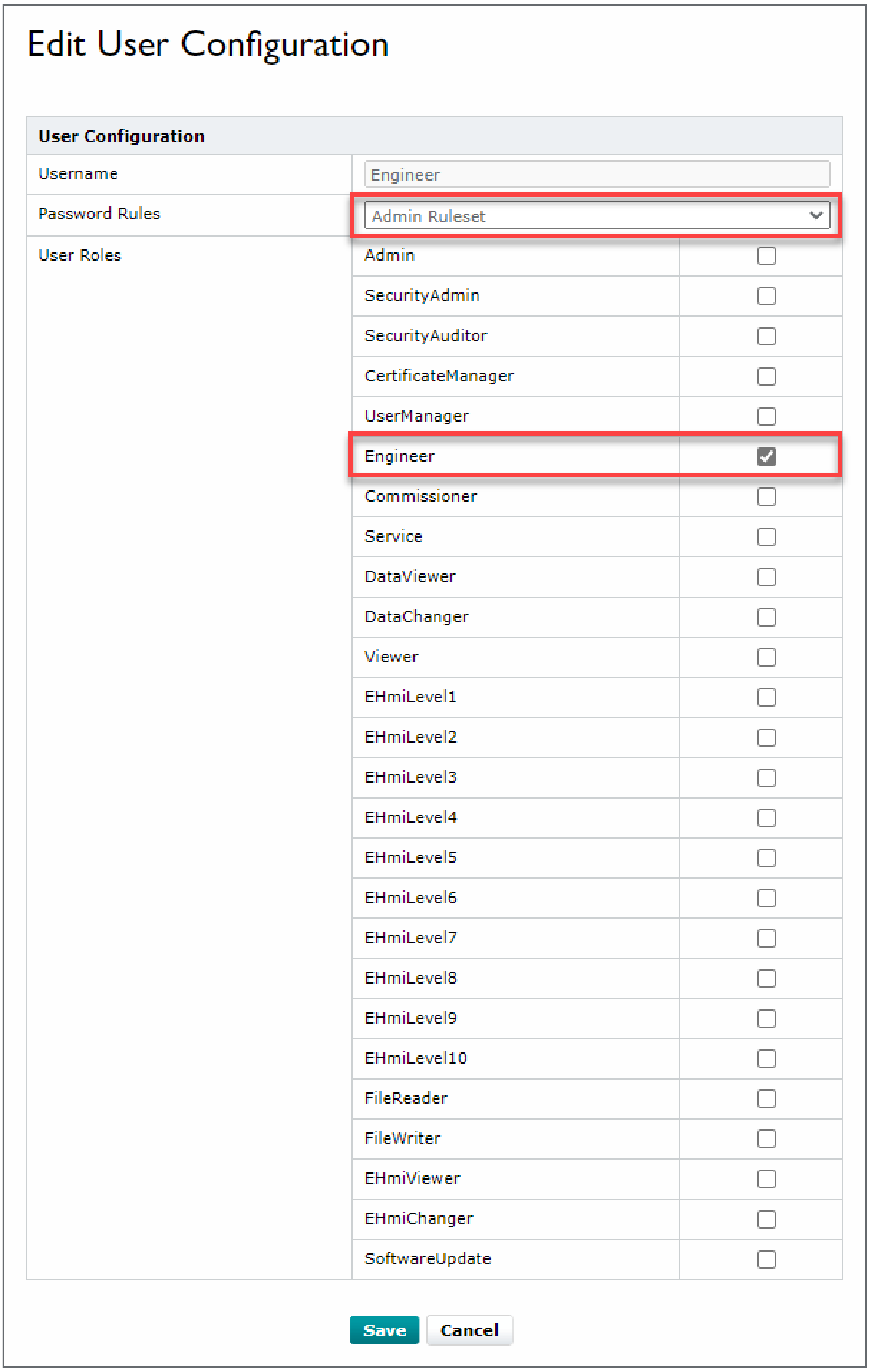
Security

User Authentication

General Configuration	
System Use Notification	Edit Notification

User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
SecurityAuditor	SecurityAuditor	Admin Ruleset	Set Password Edit User Remove User
Engineer		Default Ruleset	Set Password Edit User Remove User

- In the dialog that opens, select a ruleset (**Password rules** ; we advise the "Admin Ruleset") and the appropriate role (**User Roles**) by activating the checkbox at **Engineer** .



Edit User Configuration

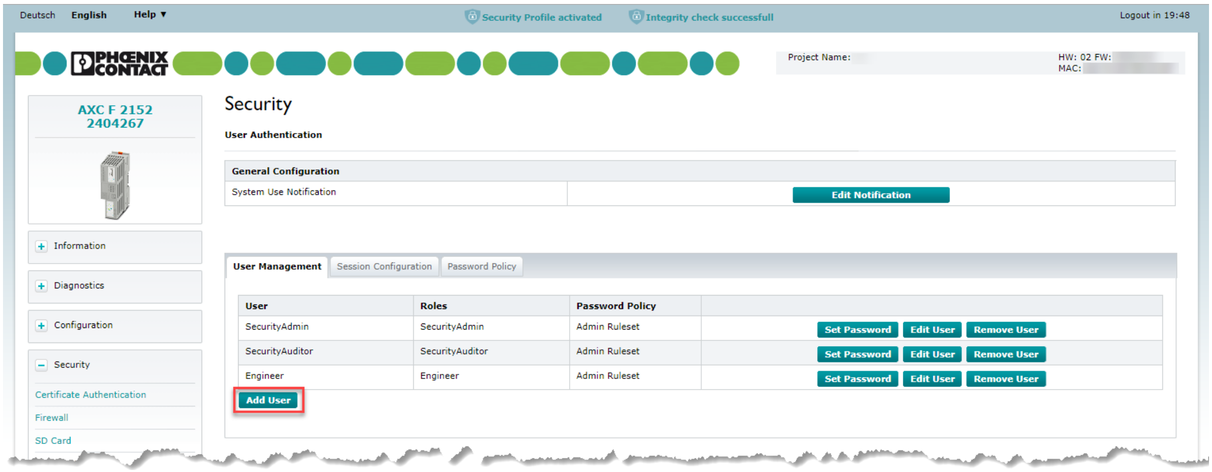
User Configuration		
Username	Engineer	
Password Rules	Admin Ruleset	
User Roles	Admin	☐
	SecurityAdmin	☐
	SecurityAuditor	☐
	CertificateManager	☐
	UserManager	☐
	Engineer	☑
	Commissioner	☐
	Service	☐
	DataViewer	☐
	DataChanger	☐
	Viewer	☐
	EHmiLevel1	☐
	EHmiLevel2	☐
	EHmiLevel3	☐
	EHmiLevel4	☐
	EHmiLevel5	☐
	EHmiLevel6	☐
	EHmiLevel7	☐
	EHmiLevel8	☐
	EHmiLevel9	☐
	EHmiLevel10	☐
	FileReader	☐
	FileWriter	☐
	EHmiViewer	☐
	EHmiChanger	☐
	SoftwareUpdate	☐

- Click the **Save** button.
↪ You've added an Engineer.

Adding an Operator

To add an Engineer, proceed as follows:

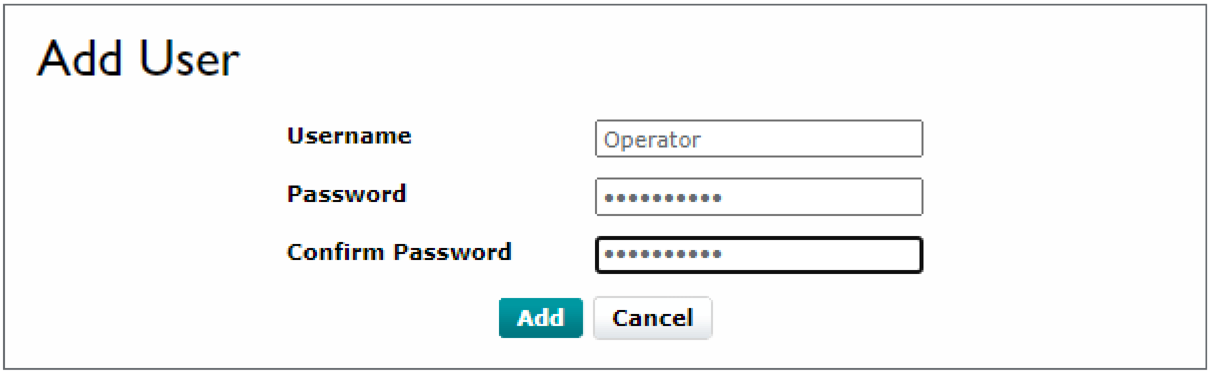
- Log in to the WBM.
- Open the **Security** → **User Authentication** page in the WBM.
- Click the **Add User** button.



User	Roles	Password Policy
SecurityAdmin	SecurityAdmin	Admin Ruleset
SecurityAuditor	SecurityAuditor	Admin Ruleset
Engineer	Engineer	Admin Ruleset

↪ The dialog **Add User** opens.

- Enter a username and a password following the password complexity rules.



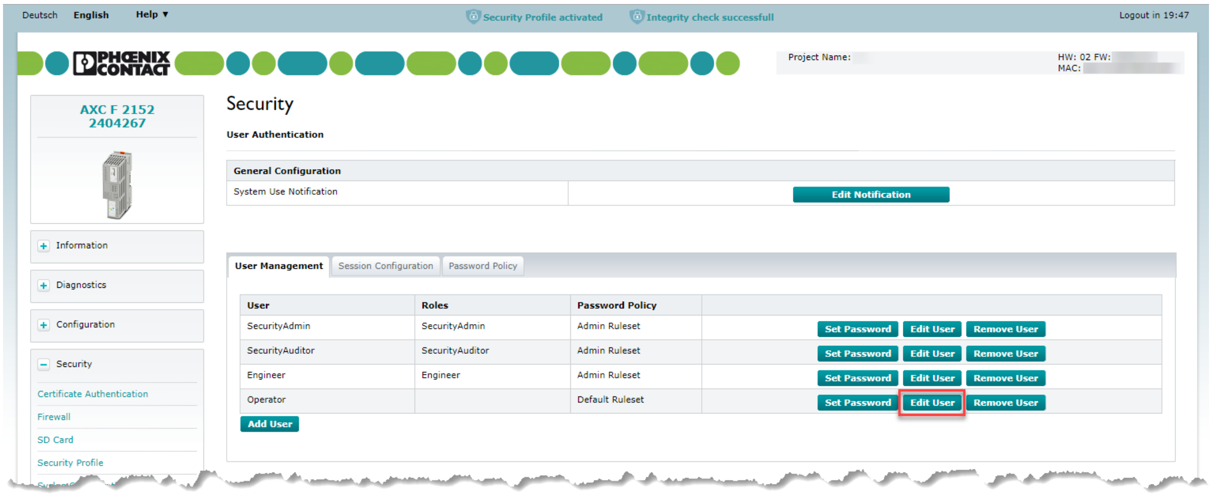
Add User

Username: Operator

Password: ••••••••••

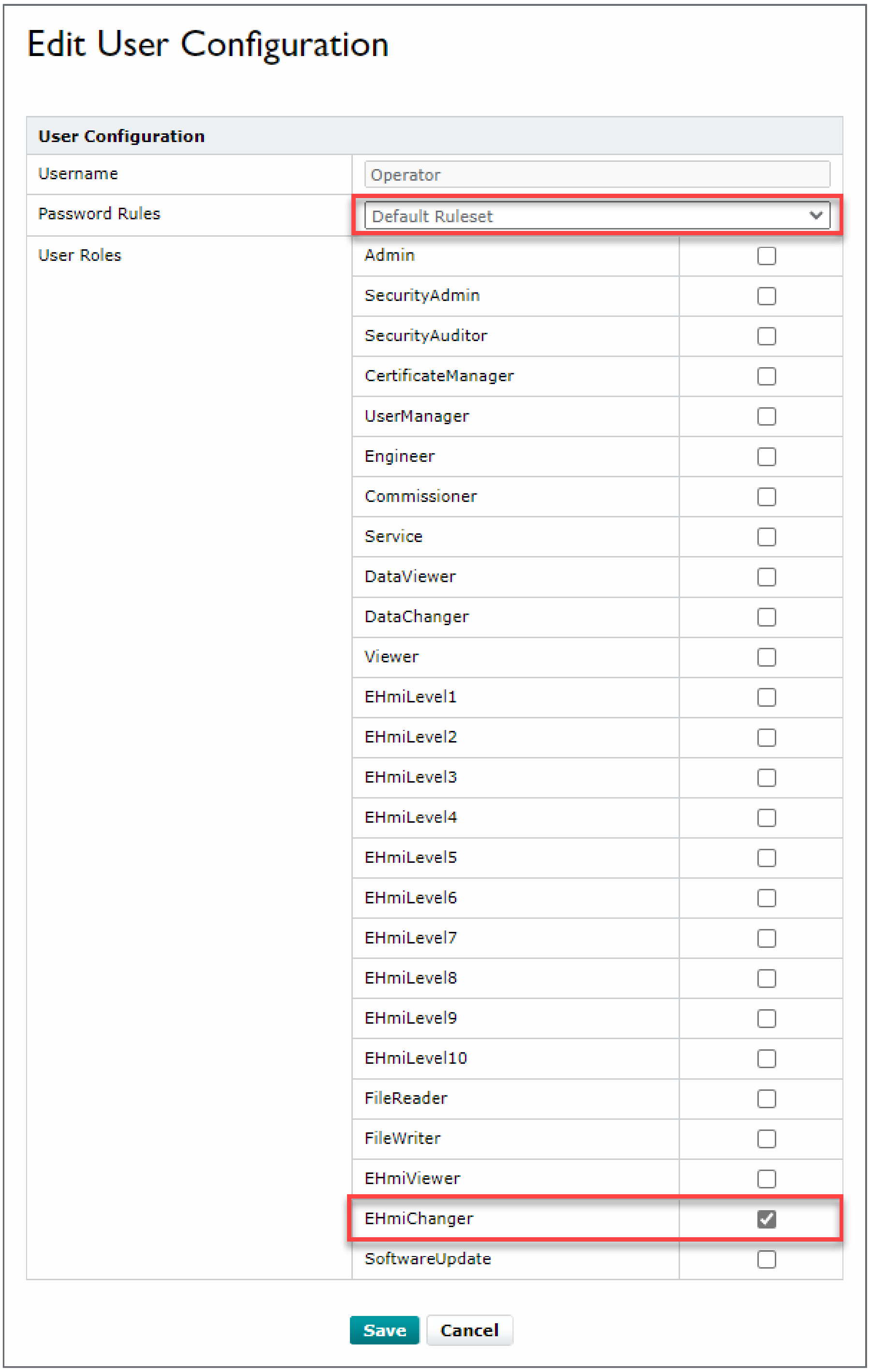
Confirm Password: ••••••••••

- Click the **Add** button.
- In the added row **Operator**, click the **Edit User** button.



User	Roles	Password Policy
SecurityAdmin	SecurityAdmin	Admin Ruleset
SecurityAuditor	SecurityAuditor	Admin Ruleset
Engineer	Engineer	Admin Ruleset
Operator		Default Ruleset

- In the dialog that opens, select the appropriate role by activating the checkbox at **EHmiChanger**.



Edit User Configuration

User Configuration		
Username	Operator	
Password Rules	Default Ruleset	
User Roles	Admin	☐
	SecurityAdmin	☐
	SecurityAuditor	☐
	CertificateManager	☐
	UserManager	☐
	Engineer	☐
	Commissioner	☐
	Service	☐
	DataViewer	☐
	DataChanger	☐
	Viewer	☐
	EHmiLevel1	☐
	EHmiLevel2	☐
	EHmiLevel3	☐
	EHmiLevel4	☐
	EHmiLevel5	☐
	EHmiLevel6	☐
	EHmiLevel7	☐
	EHmiLevel8	☐
	EHmiLevel9	☐
	EHmiLevel10	☐
	FileReader	☐
	FileWriter	☐
	EHmiViewer	☐
	EHmiChanger	☑
	SoftwareUpdate	☐

- Click the **Save** button.
↪ You've added an Operator.

Changing the password

Note: Users must change their passwords following the password complexity rules when they log in with their role for the first time.

Adding more users

If necessary, set up additional users. The number and the roles of the respective users depend on your system and the respective application.

Local user management

You can set up the users locally.

However, a global user management via LDAP is possible. When working with multiple devices (more than 3), Phoenix Contact suggests a global, network-based user management via active directory server (LDAP).

ℹ For more information on LDAP, refer to the LDAP connection - file-based configuration topic in the PLCnext Technology - Info Center.

Information about the Admin

Even if the Security Profile is enabled, the Admin is allowed to make changes via SSH, e.g. the Netload Limiter configuration or the VPN configuration. For the commissioning phase it is possible to configure the Admin to make changes to PLCnext Technology configuration files. Afterwards the Admin must be deleted again in the User Manager!

⚠ **CAUTION**

Unauthenticated access

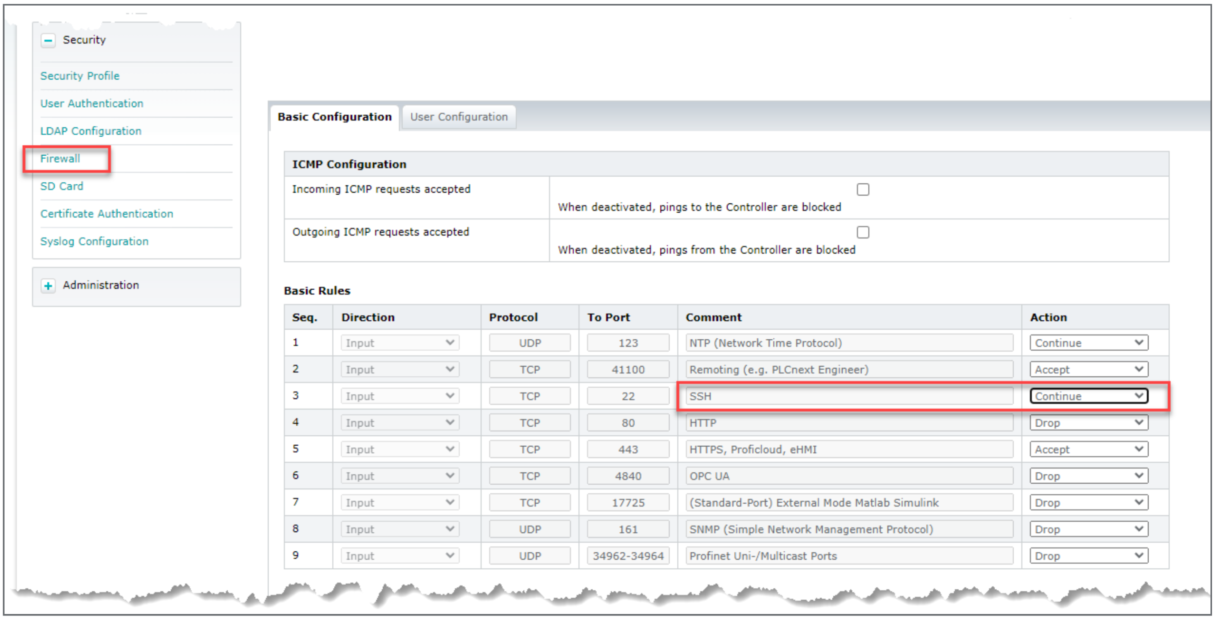
More accesses are possible via the Admin. This can disrupt production and reduce security.

- Do not start any plant with activated Admin!

With the Admin user, you can also use SSH to check the NTP connection. To do this, you must enable SSH in the firewall basic configurations (for more information, refer to the firewall basic configurations) and set an input rule:

...continuation see next page...

Basic Configuration:



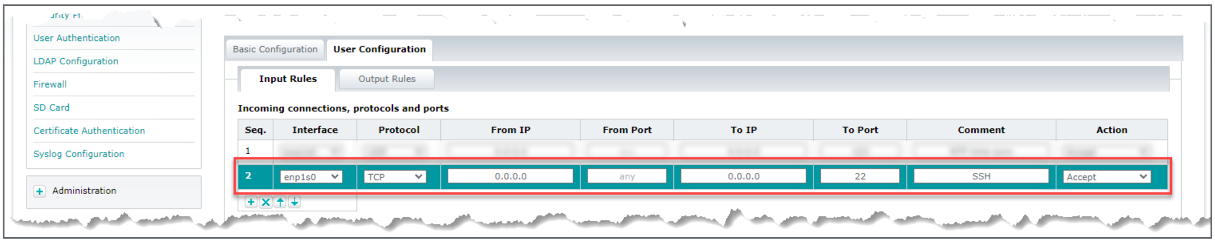
ICMP Configuration

Incoming ICMP requests accepted	□ When deactivated, pings to the Controller are blocked
Outgoing ICMP requests accepted	□ When deactivated, pings from the Controller are blocked

Basic Rules

Seq.	Direction	Protocol	To Port	Comment	Action
1	Input	UDP	123	NTP (Network Time Protocol)	Continue
2	Input	TCP	41100	Remoting (e.g. PLCnext Engineer)	Accept
3	Input	TCP	22	SSH	Continue
4	Input	TCP	80	HTTP	Drop
5	Input	TCP	443	HTTPS, Proficloud, eHMI	Accept
6	Input	TCP	4840	OPC UA	Drop
7	Input	TCP	17725	(Standard-Port) External Mode Matlab Simulink	Drop
8	Input	UDP	161	SNMP (Simple Network Management Protocol)	Drop
9	Input	UDP	34962-34964	Profinet Uni-/Multicast Ports	Drop

Input Rule:

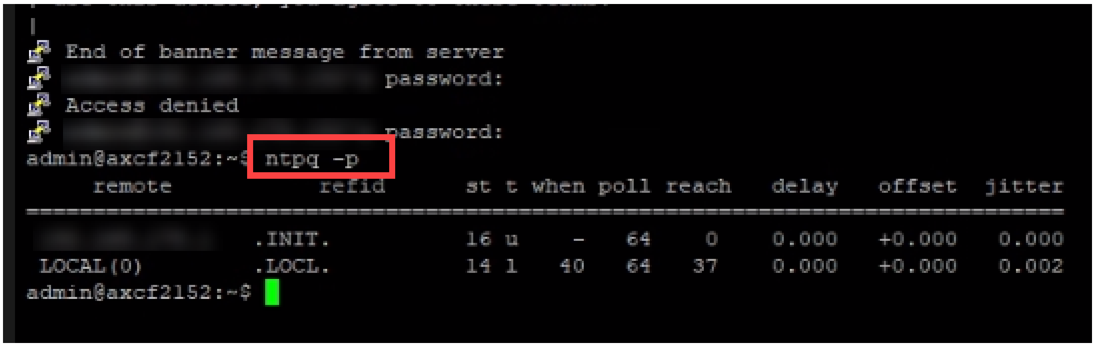


Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
2	enp1s0	TCP	0.0.0.0	any	0.0.0.0	22	SSH	Accept

Note: Configure the IP addresses in the firewall so that SSH access can only take place from the defined device.

Using the console, you can now check whether the connection has been established by using the `ntpq -p` command.



```
|
  End of banner message from server
  [redacted]                       password:
  Access denied
  [redacted]                       password:
admin@axcf2152:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 [redacted]         .INIT.       16 u    -   64    0    0.000   +0.000   0.000
 LOCAL(0)           .LOCL.       14 l   40   64   37    0.000   +0.000   0.002
admin@axcf2152:~$
```

Checking password validity in the WBM

- Log in to the WBM.
- Open the `Cockpit` page (`Diagnostics` → `Cockpit`) in the WBM.

Based on the messages, you can check whether the passwords are still valid and whether a user has already changed his default password.

Secure disposal

You must safely decommission the controller so that no sensitive, confidential and/or manufacturer-specific data and software remain on the device. Check the national GDPR (General Data Protection Regulations) to comply with and make sure that attackers can't access confidential security information's from the deinstalled or disposed devices.

For safe decommissioning, proceed as follows:

- Before you start disassembling the controller, you must remove all data from the device. To do this, perform a reset 2.
- Disassemble the hardware as described in the manuals of the respective controllers, taking into account the warnings given there.
  ℹ The manuals can be found in the download area of the respective product on the Phoenix Contact website , (e. g. for the AXC F 2152).

Controller disposal

The controller contains components such as TPM, secure elements, and internal mass storage modules. These components may contain confidential data for which special care has to be taken in to account when a device is deinstalled or disposed.

- Do not dispose of the device with household waste.
- To ensure that no one can recover the data, provide for data-safe disposal in accordance with the applicable national regulations.

Packaging disposal

- Dispose of packaging materials that are no longer needed (cardboard packaging, paper, bubble wrap sheets, etc.) with household waste in accordance with the currently applicable national regulations.

SD card disposal

Sensitive data is stored on the SD card. This data can even be restored after reformatting the SD card. To ensure that your data does not fall into unauthorized hands, you should physically destroy the SD card before disposal.

- Physically destroy the SD card, e.g., by cutting up the SD card.
- Dispose of the irreparably damaged SD card in accordance with the applicable national regulations.

How to reset the controller

For information on how to reset the controller, refer to the respective hardware information (e. g. AXC F 2152).

PLCnext Security amd Safety Guideline

PLCnext Security and Safety Guideline

To achieve security in an automation system with safety-related components, the holistic approach of the security concept must be adapted. In addition to the measures already listed, there are the following to consider:

- Security and safety context
- Security and safety hardening
- Secure and safe operation

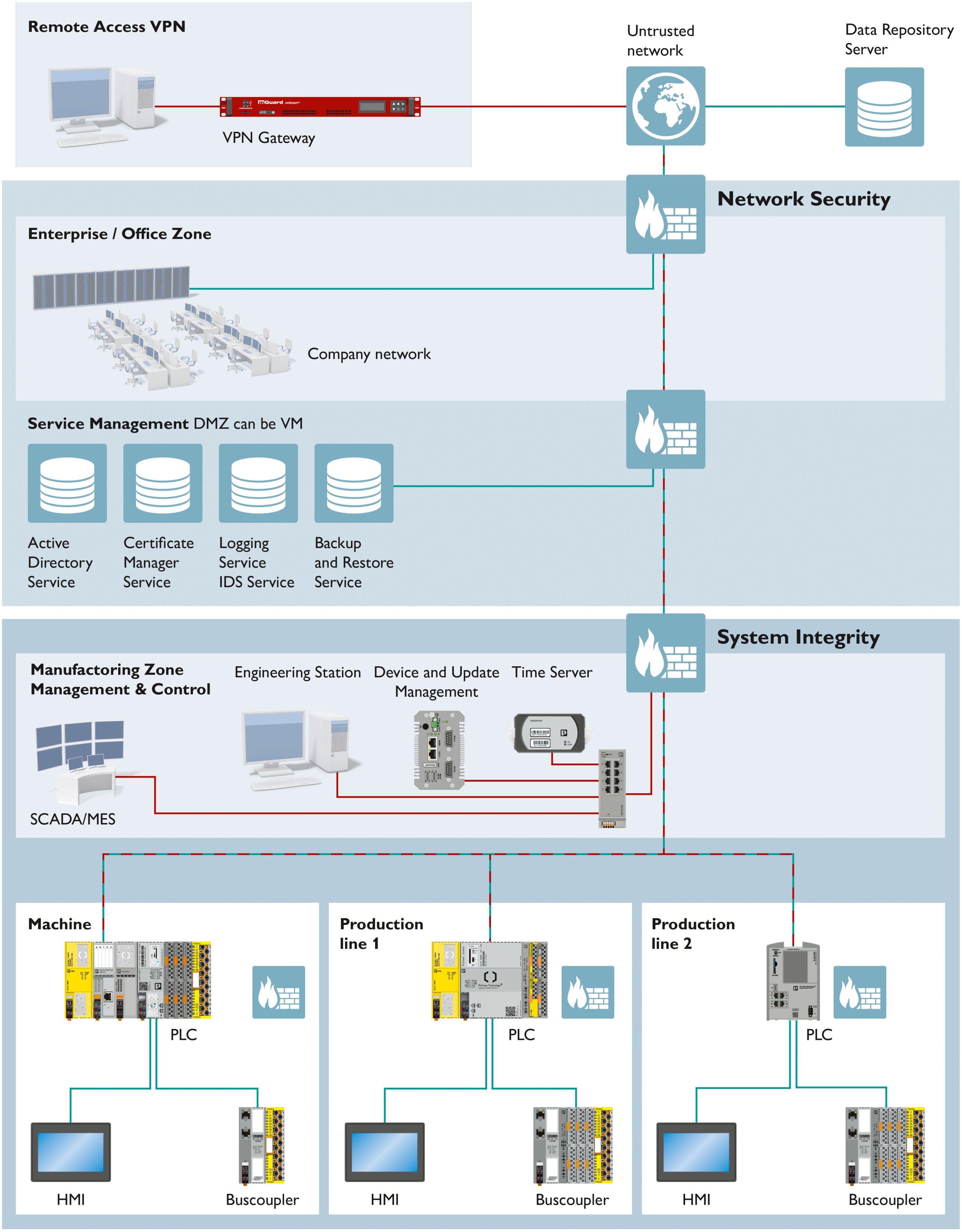
Security and safety context

Generic context 1

Controllers used in this context:

- Machine: SPLC 1000, AXC F XT ETH 1TX, AXC F XT EXP, AXC F 2152
- Production line 1: SPLC 1000, AXC F 3152
- Production line 2: RFC 4072S with integrated iSPNS 3000

...continuation see next page...

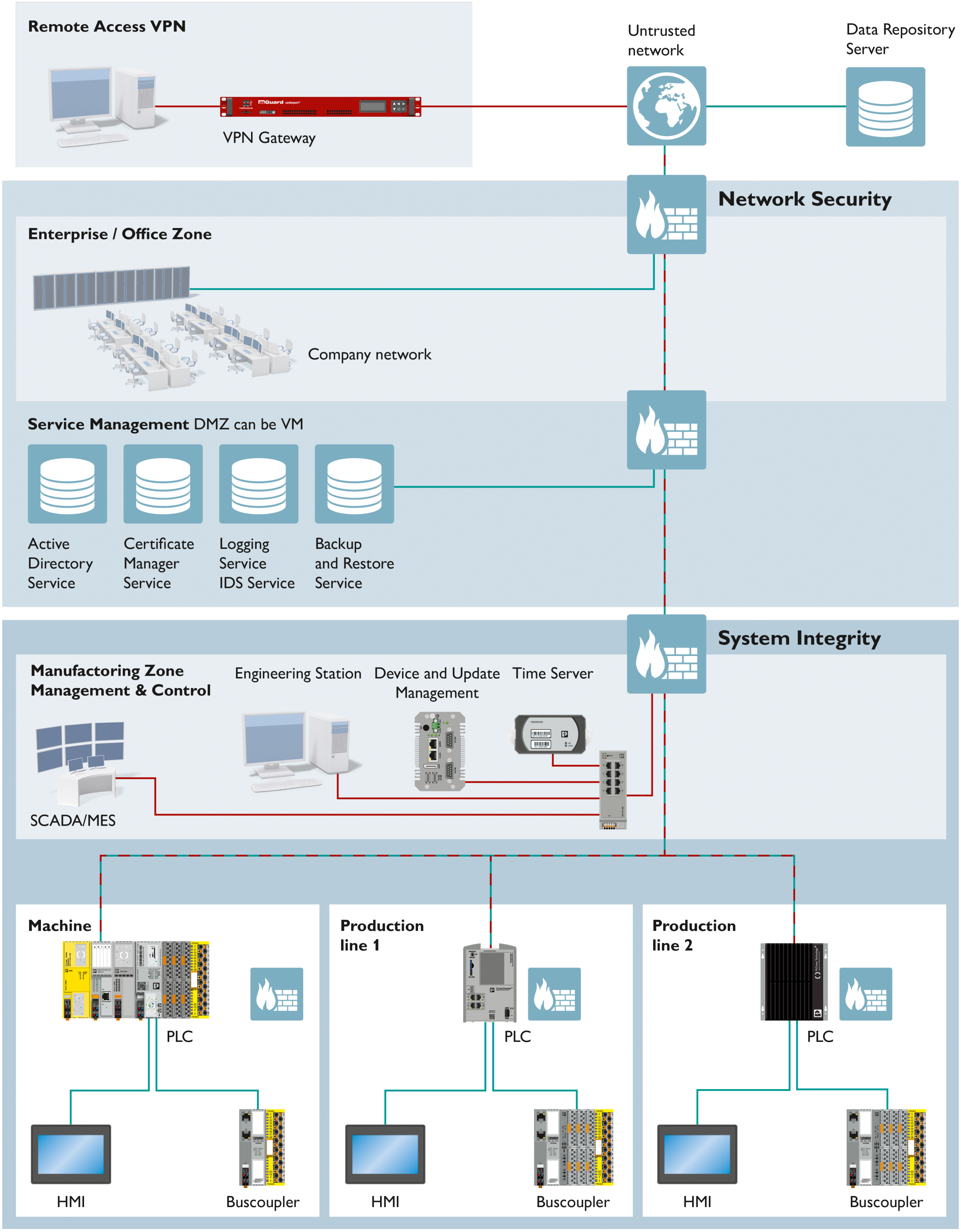

Remote Access VPN
VPN Gateway
Untrusted network
Data Repository Server
Network Security
Enterprise / Office Zone
Company network
Service Management DMZ can be VM
Active Directory Service
Certificate Manager Service
Logging Service IDS Service
Backup and Restore Service
System Integrity
Manufactoring Zone Management & Control
Engineering Station
Device and Update Management
Time Server
SCADA/MES
Machine
PLC
HMI
Buscoupler
Production line 1
PLC
HMI
Buscoupler
Production line 2
PLC
HMI
Buscoupler

Generic context 2

Controllers used in this context:

- Machine: SPLC 1000, AXC F XT ETH 1TX, AXC F 2152
- Production line 1: RFC 4072S with integrated iSPNS 3000
- Production line 2: BPC 9102S with integrated iSPNS 3000

...continuation see next page...


Remote Access VPN
VPN Gateway
Untrusted network
Data Repository Server
Network Security
Enterprise / Office Zone
Company network
Service Management DMZ can be VM
Active Directory Service
Certificate Manager Service
Logging Service IDS Service
Backup and Restore Service
System Integrity
Manufactoring Zone Management & Control
Engineering Station
Device and Update Management
Time Server
SCADA/MES
Machine
PLC
HMI
Buscoupler
Production line 1
PLC
HMI
Buscoupler
Production line 2
PLC
HMI
Buscoupler

Security and safety hardening

To use PLCnext Technology as an IEC 62443-4-1/4-2 certified component, the activation of the Security Profile is mandatory. In addition, the automation system design must fit the security context and the generic use cases described in this PLCnext Technology - Security Info Center.

With activated Security Profile PLCnext Technology supports the following functions as shown in the topic PLCnext Technology security hardening .

Additional security measures for functional safety:

- Additional user roles (SafetyEngineer and SafetyFirmwareUpdater)
- Protected file system area by special access rights
- PROFINET / PROFIsafe®

Measures for functional safety:

- Left-alignable safety-oriented control SPLC 1000
- Dual password protection:
  - Safety PLC Password to access the safety controller
  - Project password to enable safety-related editing of the project
- Safety logs are accessable via PLCnext Engineer, see the online help of PLCnext Engineer.
- In PLCnext Engineer, the safety-related and the standard application are separated, see the online help of PLCnext Engineer.
- Combined or distinguished download of standard project and safety-related project

For further information, refer to the topic Configuring PLCnext Engineer (combined safety).

Security and safety architecture

To fulfill the IEC 62443-4-1 requirements a threat analysis of the PLCnext Runtime System and PLCnext Technology hardware is an important task. The PLCnext Technology threat analysis is based on the *STRIDE* model which consists of the identification of these security threats in these categories: spoofing, tampering, repudiation, Information disclosure, denial of service, elevation of privilege.

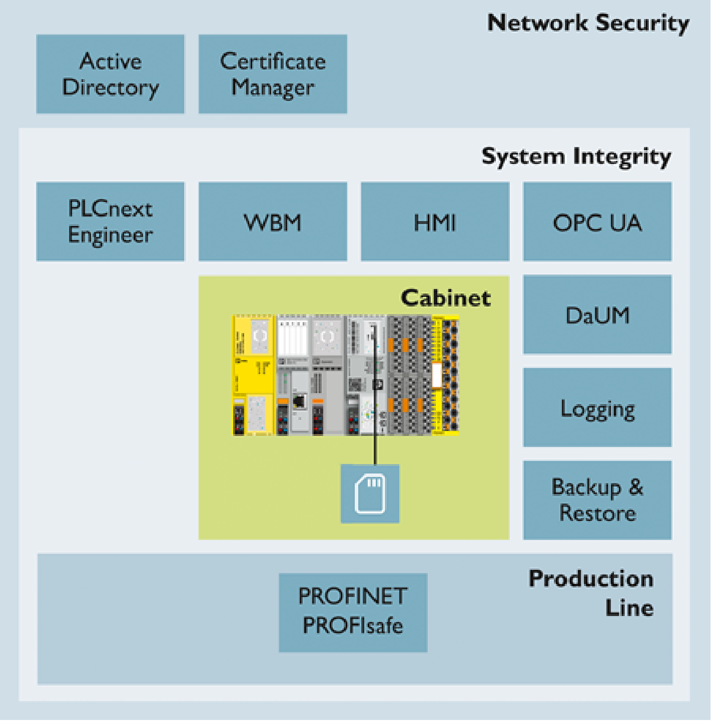
As a prerequisite the security context defined in this PLCnext Technology - Security Info Center and the implemented Security Level 2 (SL2) feature set are used.

One key element of the threat analysis is to review the integrity and authenticity of the data in rest and data in transmission. Another key element is the authorization of human users and software components to access the data. In addition, the firewall protects the access to the communication interfaces, or supports *denial of service* protection.

PLCnext Technology provides TLS 1.2 or TLS 1.3 based communication on necessary communication interfaces (e.g. HTTPS, OPC UA®, PLCnext Engineer).

For other communication channels like LDAP or Syslog-ng, TLS can be activated according the users’ needs.

The authorization is handled by an RBAC user management for human users, and/or certificate management for software components.



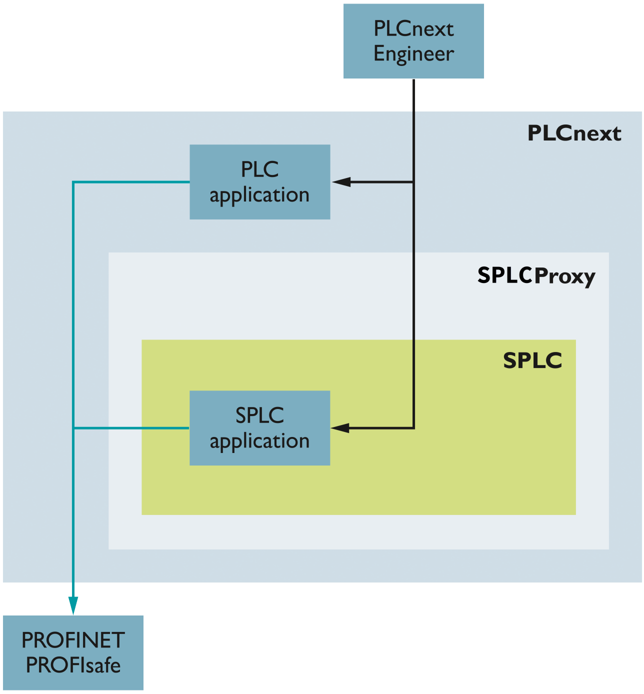
Functional safety with PROFINET / PROFIsafe® communication

PLCnext can be enhanced by a powerful two-channel safety-related controller for PROFIsafe®. Either as left assignable modular hardware module or an additional functional safety hardware module designed in the housing of the controller by default.

Secure and safe communication is handled via PROFINET and PROFIsafe® technology. The PROFIsafe® functional safety protocol is transmitted via the PLCnext Control device using the PROFINET network by the black channel principle.

Before setting up a PROFINET network a risk analysis must be done and an sufficient security context must be designed. Please refer to your PLCnext Control description (e. g. AXC F 2152) and the controller manual to setup a secured and segmented PROFINET network.

The functional safety controller (SPLC) is protected by a defense-in-depth layer approach. The IEC 62443-4-2 certified PLCnext Control protects the SPLC against security attacks (see Certified secure development lifecycle). An SPLCProxy layer is providing security extensions, dedicated safety roles and file system access rights to protect the SPLC. The SPLC has no direct connection to the network nor is storing data in rest on an own mass storage. It's executing the functional safety logic downloaded by the PLCnext Engineer as well as using PROFIsafe® to manage the safety I/Os. SPLC is certified by IEC 61508 SIL3 (see Functional Safety Certificate) The security measures enhance the black channel security but don't interfere the functional safety.



Security and safety measures

Data in rest

PLCnext Technology's data is stored on an internal (non-removable) SD card. The detailed description of the data and directory structure can be found in the main PLCnext Technology - Info Center at the Directories of the firmware components.

The SPLC only uses data of the SD card of the standard PLC, which is protected via the SPLCProxy, for data storage.

The controller can be expanded via an external SD card. An external SD card enables an easy device replacement with licenses transferred via that storage medium. You also get additional space for your automation project data.

From firmware 2022.0 LTS, a set of special SD cards are available supporting the distribution of licenses:

- SD FLASH 8GB PLCNEXT MEMORY **LIC** (item no. 1151112)
- SD FLASH 32GB PLCNEXT MEMORY **LIC** (item no. 1151111)
- SD FLASH PLCNEXT MEMORY **LIC CFG** (item no. 1308064)

From firmware 2024.0 LTS, these special SD cards provide data protection, and therefore can be used together with the Security Profile.

Some controllers require an SD card for operation. Check in the topic of the respective controller whether your controller requires an SD card.

Phoenix Contact recommends to secure the slot for SD card on the PLCnext Control with a lead seal against manipulation. For further information about protecting the SD card, refer to the topics Protection against physical access and Secure disposal and the topic of the respective controller (e.g. AXC F 2152).

Data in transmission

To support secure communication e.g. via TLS, different options of cryptographic keys can be configured. For further information, refer to the topic PLCnext Technology security hardening .

User Management

PLCnext Technology’s User Management provides authentication and authorization on each communication interface. Only authorized users can access (read/write) data via a communication interface.

In the context of functional safety, PLCnext offers additional user roles. See the topic Creating users (combined safety) for more information.

Software information integrity and authenticity

Software information security is provided by different mechanisms. For further information, refer to the topic PLCnext Technology security hardening .

For information about the dedicated measures for functional safety, refer to the hardware documentation of your safety controller (Product range).

Mobile and malicious code protection

Authentication and authorization are provided by the User Management: Only authorized users get access (read/write) to the SPLC's data.

PLCnext Engineer enforces the user to enter his credentials before accessing the controller. Only authorized users can download an application to the SPLC device. See the topic Creating users (combined safety) for more information.

Safety projects are checked via CRC before download, see the topic Security logging (combined safety).

Standard projects are checked via hashes, see the topic Checking project data integrity.

See also the topic Configuring PLCnext Engineer (combined safety) for measures of functional safety.

Access protection

Protection against physical access

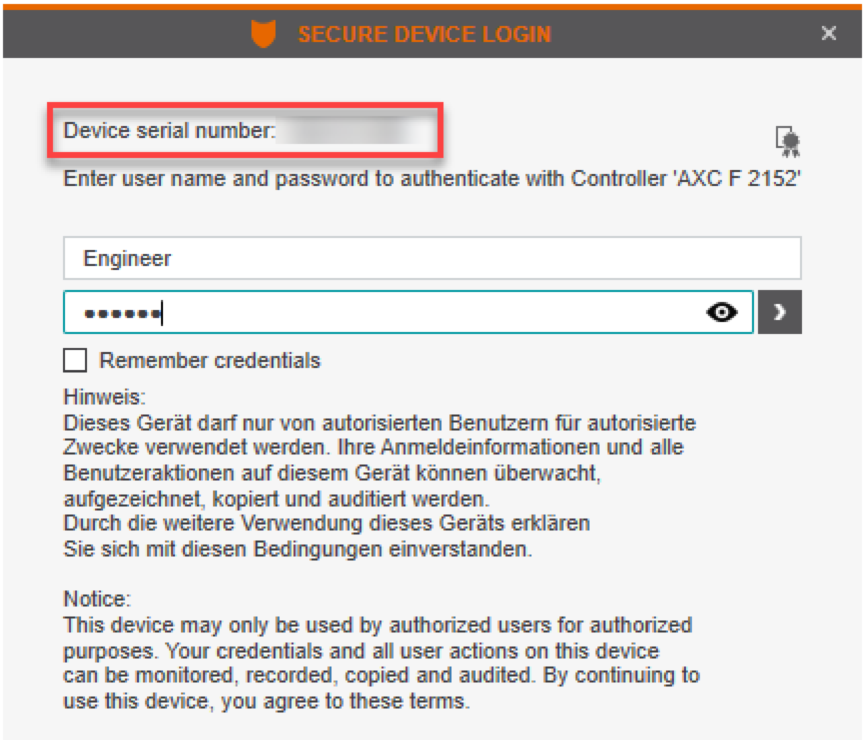
- Install the PLCnext Control in a lockable housing or a lockable control cabinet.
- Consider the information from the topic Protection against physical access.

Protection against unauthorized data access

To protect against unauthorized data access, a log in is required e. g. via PLCnext Engineer.

Every user has specific user roles managed via the user management. To have access to the data, the user must have access rights to standard and functional safety data. Therefor, the user "Engineer" can be configured to have two user roles (Engineer for standard data and SafetyEngineer for functional safety data), see the topic Creating users (combined safety).

In PLCnext Engineer, every user has to log in to have access to the PLCnext Control:



Device serial number: [redacted]

Enter user name and password to authenticate with Controller 'AXC F 2152'

Engineer

••••••

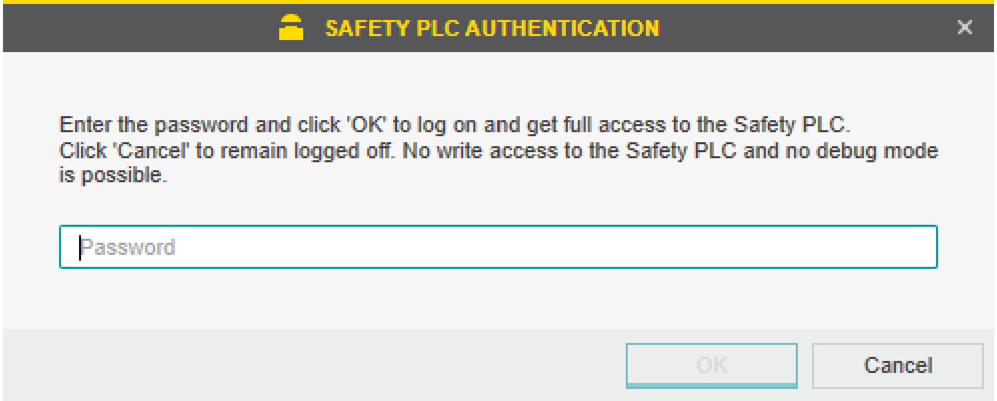
□ Remember credentials

Hinweis:
Dieses Gerät darf nur von autorisierten Benutzern für autorisierte Zwecke verwendet werden. Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Gerät können überwacht, aufgezeichnet, kopiert und auditiert werden.
Durch die weitere Verwendung dieses Geräts erklären Sie sich mit diesen Bedingungen einverstanden.

Notice:
This device may only be used by authorized users for authorized purposes. Your credentials and all user actions on this device can be monitored, recorded, copied and audited. By continuing to use this device, you agree to these terms.

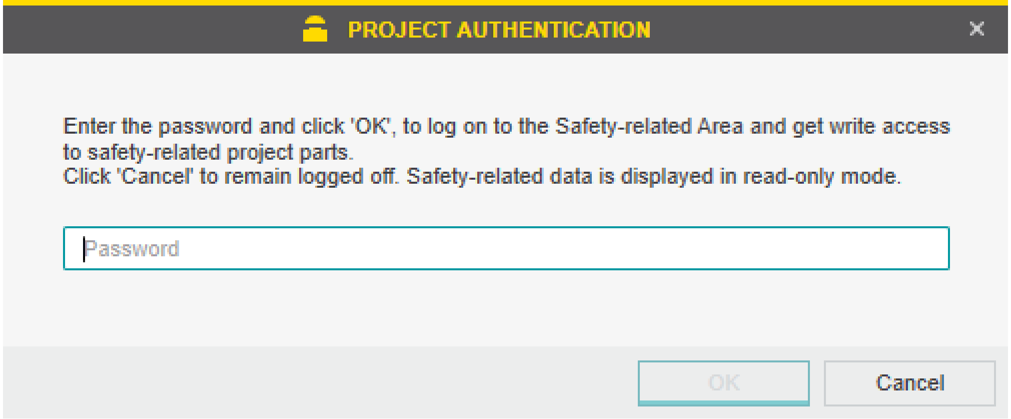
As an additional measure for functional safety, dual password protection is offered.

The safety PLC is protected by a controller password. Writing data to the safety PLC, switching its operation mode or executing debug commands is only possible after entering the controller password in PLCnext Engineer.



Enter the password and click 'OK' to log on and get full access to the Safety PLC.
Click 'Cancel' to remain logged off. No write access to the Safety PLC and no debug mode is possible.

The safety-related project data are protected by a project password. Safety-related parts of the project can only be edited while being logged in.

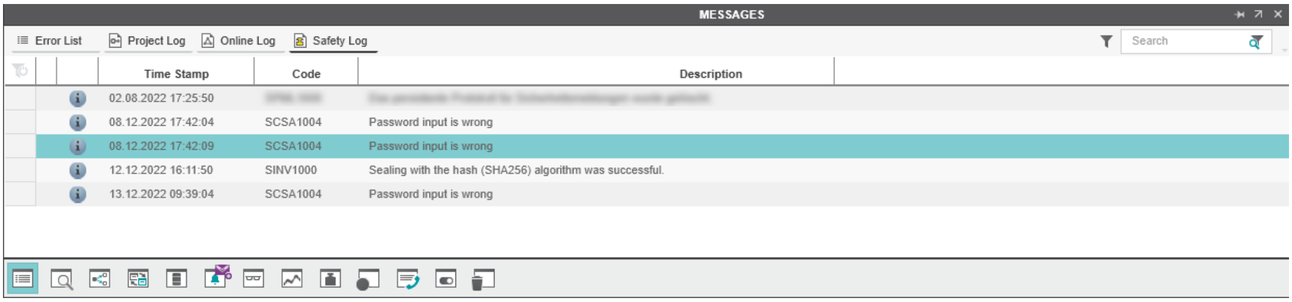


Enter the password and click 'OK', to log on to the Safety-related Area and get write access to safety-related project parts.
Click 'Cancel' to remain logged off. Safety-related data is displayed in read-only mode.

For further information about dual password protection, refer to the online help of PLCnext Engineer.

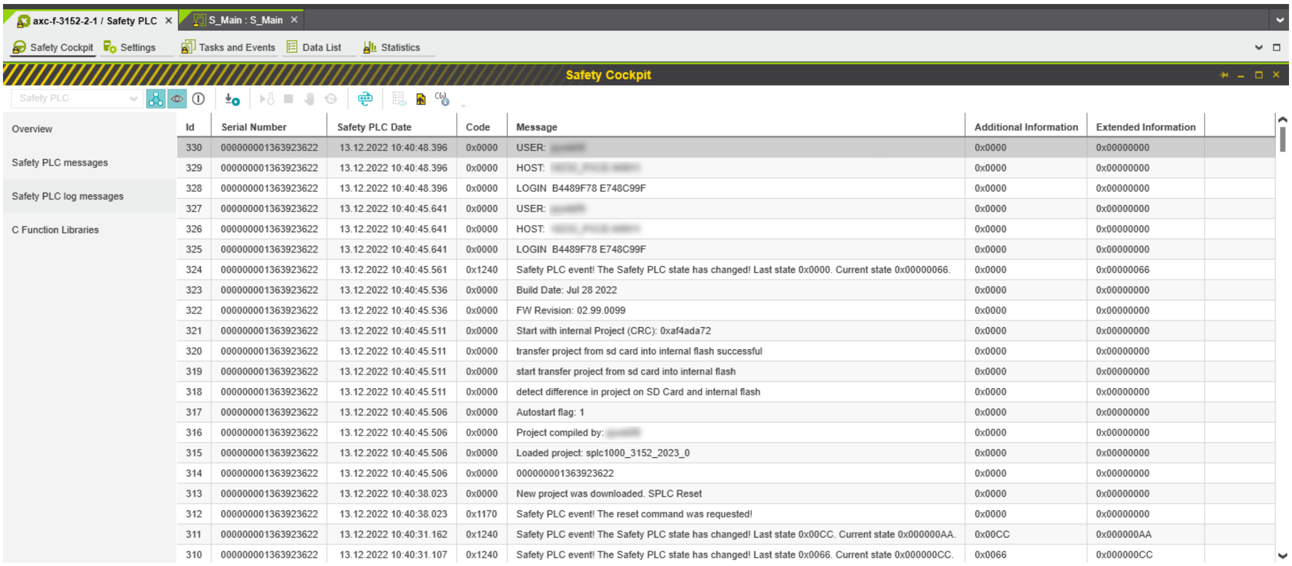
Safety logs in PLCnext Engineer

Any editing operations and messages in PLCnext Engineer that relate to safety-related project parts are written to the persistent safety message log, or safety log in short.



Time Stamp	Code	Description
02.08.2022 17:25:50	[illegible]	[illegible]
08.12.2022 17:42:04	SCSA1004	Password input is wrong
08.12.2022 17:42:09	SCSA1004	Password input is wrong
12.12.2022 16:11:50	SINV1000	Sealing with the hash (SHA256) algorithm was successful.
13.12.2022 09:39:04	SCSA1004	Password input is wrong

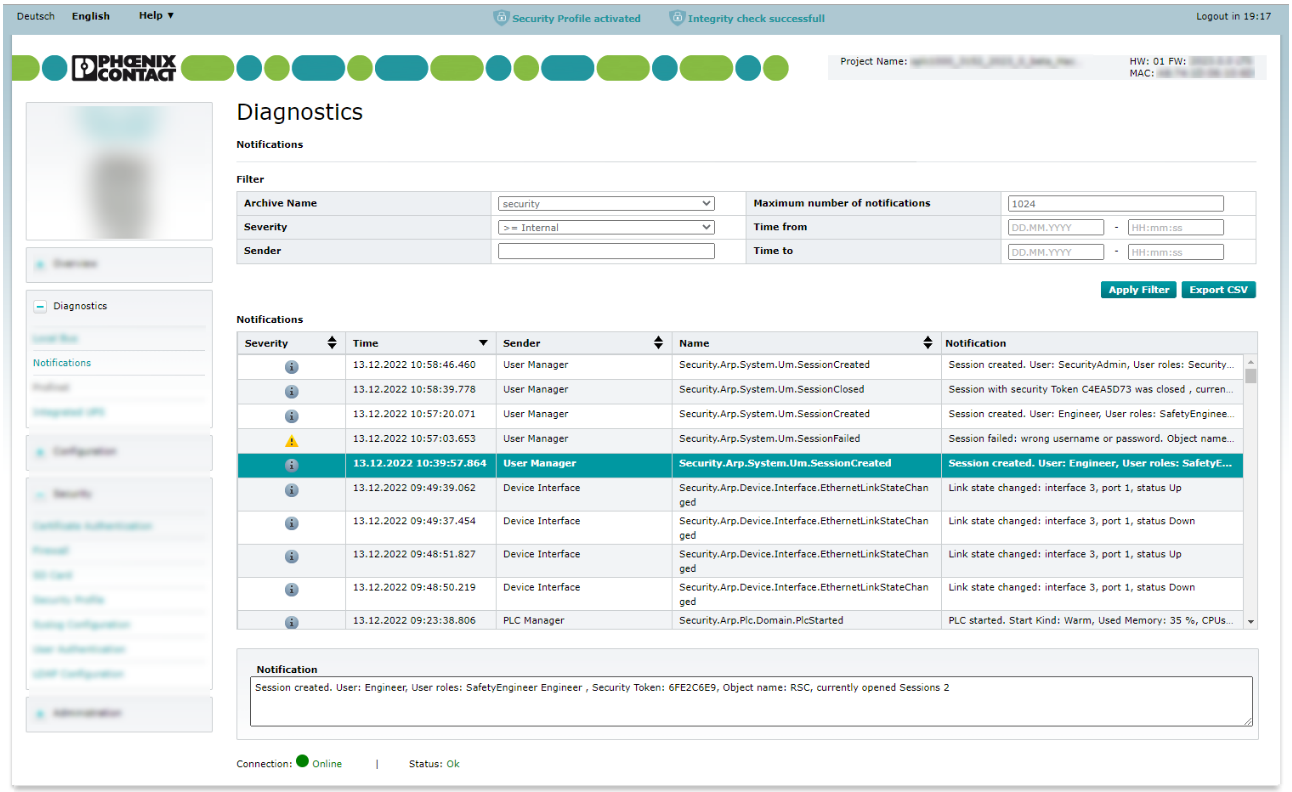
The **safety PLC log messages** editor page lists the entries which have been read from the log book of the safety PLC. In the log book, the safety PLC records device-related events such as state changes and errors.



Id	Serial Number	Safety PLC Date	Code	Message	Additional Information	Extended Information
330	000000001363923622	13.12.2022 10:40:48.396	0x0000	USER: [redacted]	0x0000	0x00000000
329	000000001363923622	13.12.2022 10:40:48.396	0x0000	HOST: [redacted]	0x0000	0x00000000
328	000000001363923622	13.12.2022 10:40:48.396	0x0000	LOGIN B4489F78 E748C99F	0x0000	0x00000000
327	000000001363923622	13.12.2022 10:40:45.641	0x0000	USER: [redacted]	0x0000	0x00000000
326	000000001363923622	13.12.2022 10:40:45.641	0x0000	HOST: [redacted]	0x0000	0x00000000
325	000000001363923622	13.12.2022 10:40:45.641	0x0000	LOGIN B4489F78 E748C99F	0x0000	0x00000000
324	000000001363923622	13.12.2022 10:40:45.561	0x1240	Safety PLC event! The Safety PLC state has changed! Last state 0x0000. Current state 0x00000066.	0x0000	0x00000066
323	000000001363923622	13.12.2022 10:40:45.536	0x0000	Build Date: Jul 28 2022	0x0000	0x00000000
322	000000001363923622	13.12.2022 10:40:45.536	0x0000	FW Revision: 02.99.0099	0x0000	0x00000000
321	000000001363923622	13.12.2022 10:40:45.511	0x0000	Start with internal Project (CRC): 0xaf4ada72	0x0000	0x00000000
320	000000001363923622	13.12.2022 10:40:45.511	0x0000	transfer project from sd card into internal flash successful	0x0000	0x00000000
319	000000001363923622	13.12.2022 10:40:45.511	0x0000	start transfer project from sd card into internal flash	0x0000	0x00000000
318	000000001363923622	13.12.2022 10:40:45.511	0x0000	detect difference in project on SD Card and internal flash	0x0000	0x00000000
317	000000001363923622	13.12.2022 10:40:45.506	0x0000	Autostart flag: 1	0x0000	0x00000000
316	000000001363923622	13.12.2022 10:40:45.506	0x0000	Project compiled by: [redacted]	0x0000	0x00000000
315	000000001363923622	13.12.2022 10:40:45.506	0x0000	Loaded project: splc1000_3152_2023_0	0x0000	0x00000000
314	000000001363923622	13.12.2022 10:40:45.506	0x0000	000000001363923622	0x0000	0x00000000
313	000000001363923622	13.12.2022 10:40:38.023	0x0000	New project was downloaded. SPLC Reset	0x0000	0x00000000
312	000000001363923622	13.12.2022 10:40:38.023	0x1170	Safety PLC event! The reset command was requested!	0x0000	0x00000000
311	000000001363923622	13.12.2022 10:40:31.162	0x1240	Safety PLC event! The Safety PLC state has changed! Last state 0x00CC. Current state 0x000000AA.	0x00CC	0x000000AA
310	000000001363923622	13.12.2022 10:40:31.107	0x1240	Safety PLC event! The Safety PLC state has changed! Last state 0x0066. Current state 0x000000CC.	0x0066	0x000000CC

Security logging PLCnext

The SecurityAuditor has access to the notifications on the **Notifications** page (**Diagnostics** → **Notifications**) in the WBM. He can view all activities of the logged-in users and their user roles.



Project Name: [redacted] HW: 01 FW: [redacted] MAC: [redacted]

Diagnostics

Notifications

Filter

Archive Name	security	Maximum number of notifications	1024
Severity	>= Internal	Time from	DD.MM.YYYY - HH:mm:ss
Sender		Time to	DD.MM.YYYY - HH:mm:ss

Notifications

Severity	Time	Sender	Name	Notification
i	13.12.2022 10:58:46.460	User Manager	Security.Arp.System.Um.SessionCreated	Session created. User: SecurityAdmin, User roles: Security...
i	13.12.2022 10:58:39.778	User Manager	Security.Arp.System.Um.SessionClosed	Session with security Token C4EA5D73 was closed , curren...
i	13.12.2022 10:57:20.071	User Manager	Security.Arp.System.Um.SessionCreated	Session created. User: Engineer, User roles: SafetyEnginee...
⚠	13.12.2022 10:57:03.653	User Manager	Security.Arp.System.Um.SessionFailed	Session failed: wrong username or password. Object name...
i	13.12.2022 10:39:57.864	User Manager	Security.Arp.System.Um.SessionCreated	Session created. User: Engineer, User roles: SafetyE...
i	13.12.2022 09:49:39.062	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 3, port 1, status Up
i	13.12.2022 09:49:37.454	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 3, port 1, status Down
i	13.12.2022 09:48:51.827	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 3, port 1, status Up
i	13.12.2022 09:48:50.219	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 3, port 1, status Down
i	13.12.2022 09:23:38.806	PLC Manager	Security.Arp.Plc.Domain.PlcStarted	PLC started. Start Kind: Warm, Used Memory: 35 %, CPUs...

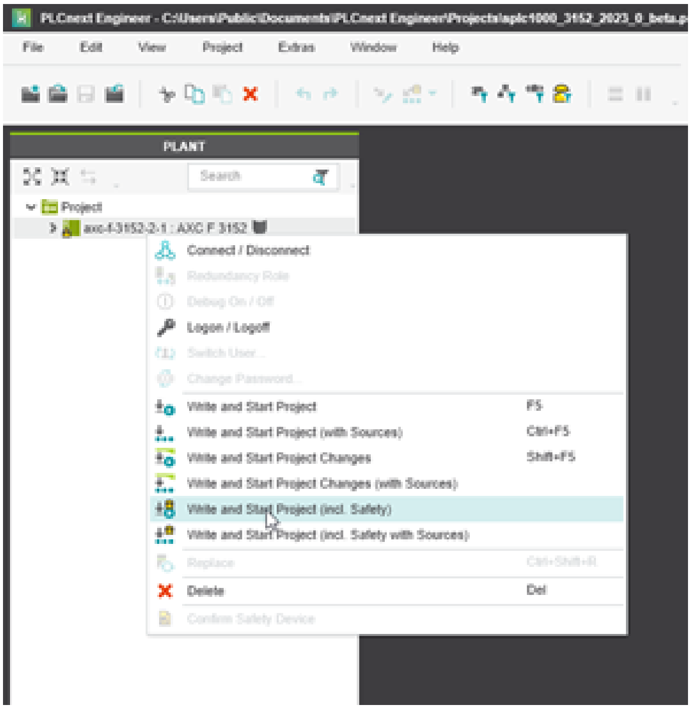
Notification

Session created. User: Engineer, User roles: SafetyEngineer Engineer , Security Token: 6FE2C6E9, Object name: RSC, currently opened Sessions 2

Connection: ● Online | Status: Ok

Combined or separated download of standard project and safety-related project

In PLCnext Engineer, you can download the standard project and the safety-related project combined or separated.


PLCnext Engineer - C:\Users\Public\Documents\PLCnext Engineer\Projects\aplc1000_3152_2023_0_beta.p
File
Edit
View
Project
Extras
Window
Help
PLANT
Search
Project
axc-f-3152-2-1 : AXC F 3152
Connect / Disconnect
Redundancy Role
Debug On / Off
Logon / Logoff
Switch User...
Change Password...
Write and Start Project F5
Write and Start Project (with Sources) Ctrl+F5
Write and Start Project Changes Shift+F5
Write and Start Project Changes (with Sources)
Write and Start Project (incl. Safety)
Write and Start Project (incl. Safety with Sources)
Replace Ctrl+Shift+R
Delete Del
Confirm Safety Device

In order to perform a combined download, you have to configure the write and start commands first (see the topic Configuring PLCnext Engineer (combined safety)).

Secure and safe operation

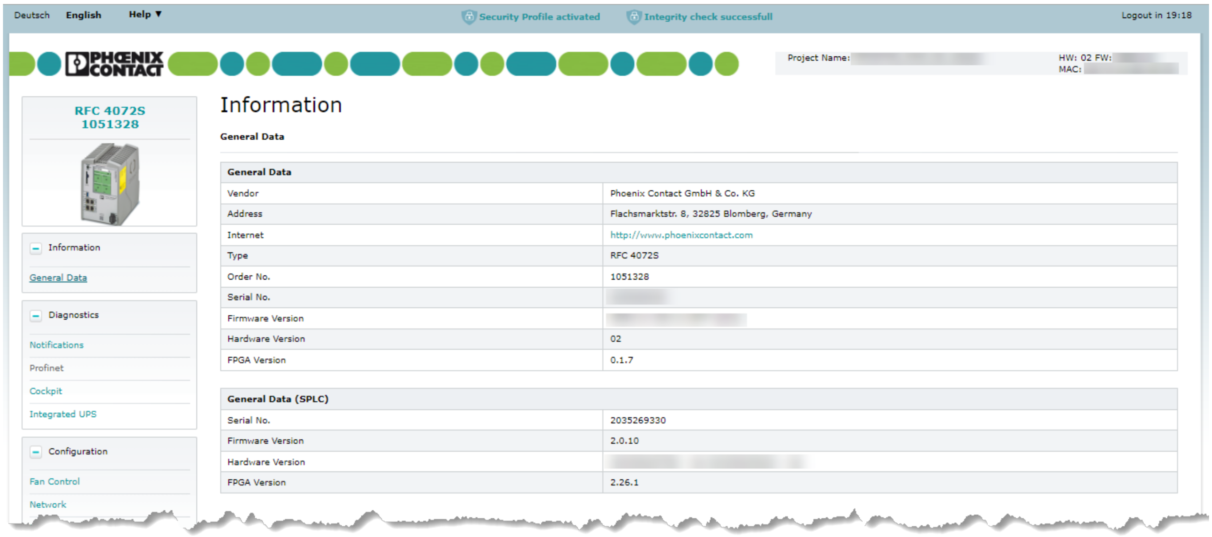
Secure and safe operation

The secure and safe operation of PLCnext Control in your specific safety-related application context requires a defined procedure. You will find the safety-specific steps in the following sections:

- Checking the device (combined safety)
- Checking the integrity state (combined safety)
- Creating users (combined safety)
- Configuring PLCnext Engineer (combined safety)
- Security logging (combined safety)

Checking the device (combined safety)

- Log in to the WBM.
- Open the **General Data** page (**Information** → **General Data**).
- Check whether you are working on the correct device:
  - PLCnext Control RFC 4072S , Order No. 1051328
  - Serial No. as printed on the device
  - Firmware Version min. 2022 LTS
  - Hardware Version min. 02



Information

General Data

General Data	
Vendor	Phoenix Contact GmbH & Co. KG
Address	Flachsmarktstr. 8, 32825 Blomberg, Germany
Internet	http://www.phoenixcontact.com
Type	RFC 4072S
Order No.	1051328
Serial No.	[redacted]
Firmware Version	[redacted]
Hardware Version	02
FPGA Version	0.1.7

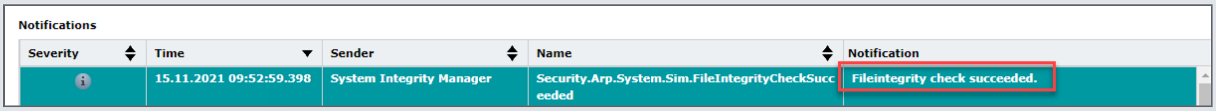
General Data (SPLC)	
Serial No.	2035269330
Firmware Version	2.0.10
Hardware Version	[redacted]
FPGA Version	2.26.1

Checking the integrity state (combined safety)

If the Security Profile is activated, an integrity state check is performed after each boot and log-in to the WBM.

The integrity state is displayed in the WBM in the page header line right to the Security Profile state field.

Note: Every event is logged. On the `Notifications` page in the WBM, you can see whether the file integrity check was successful.

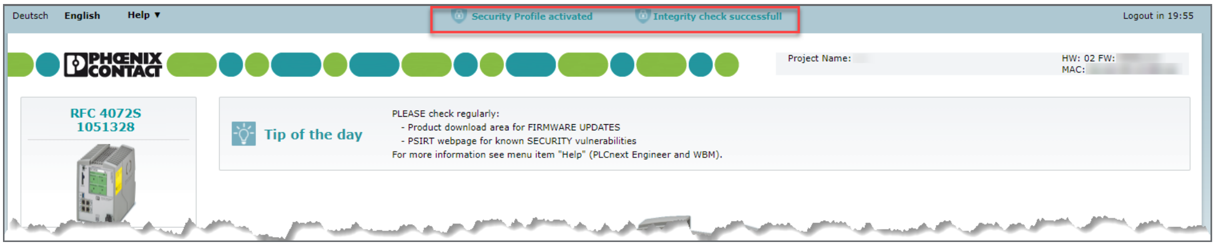


Notifications

Severity	Time	Sender	Name	Notification
i	15.11.2021 09:52:59.398	System Integrity Manager	Security.Arp.System.Sim.FileIntegrityCheckSucceeded	Fileintegrity check succeeded.

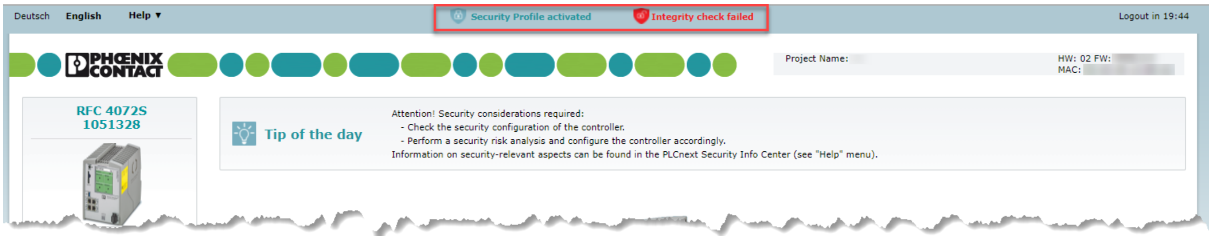
For more information on security logging, refer to the topic Security logging.

Security Profile is activated and the integrity state check is successful:



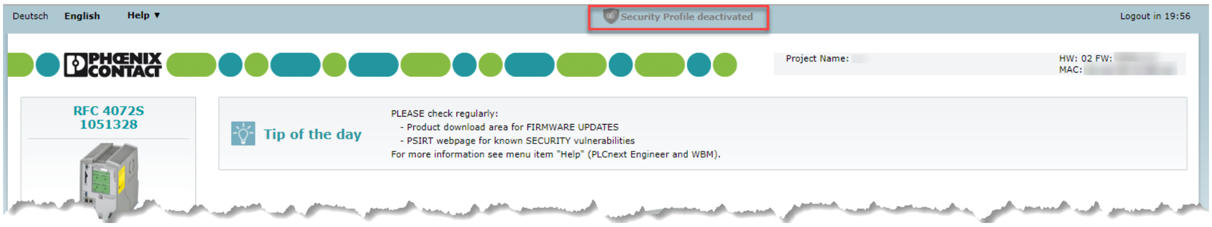
PLEASE check regularly:
- Product download area for FIRMWARE UPDATES
- PSIRT webpage for known SECURITY vulnerabilities
For more information see menu item "Help" (PLCnext Engineer and WBM).

Security Profile is activated but the integrity state check failed:



Attention! Security considerations required:
- Check the security configuration of the controller.
- Perform a security risk analysis and configure the controller accordingly.
Information on security-relevant aspects can be found in the PLCnext Security Info Center (see "Help" menu).

Security Profile is deactivated, the integrity state field is hidden:



PLEASE check regularly:
- Product download area for FIRMWARE UPDATES
- PSIRT webpage for known SECURITY vulnerabilities
For more information see menu item "Help" (PLCnext Engineer and WBM).

Creating users (combined safety)

For more information on the user management, refer to the general topic Creating users .

Additional safety user roles

SafetyEngineer

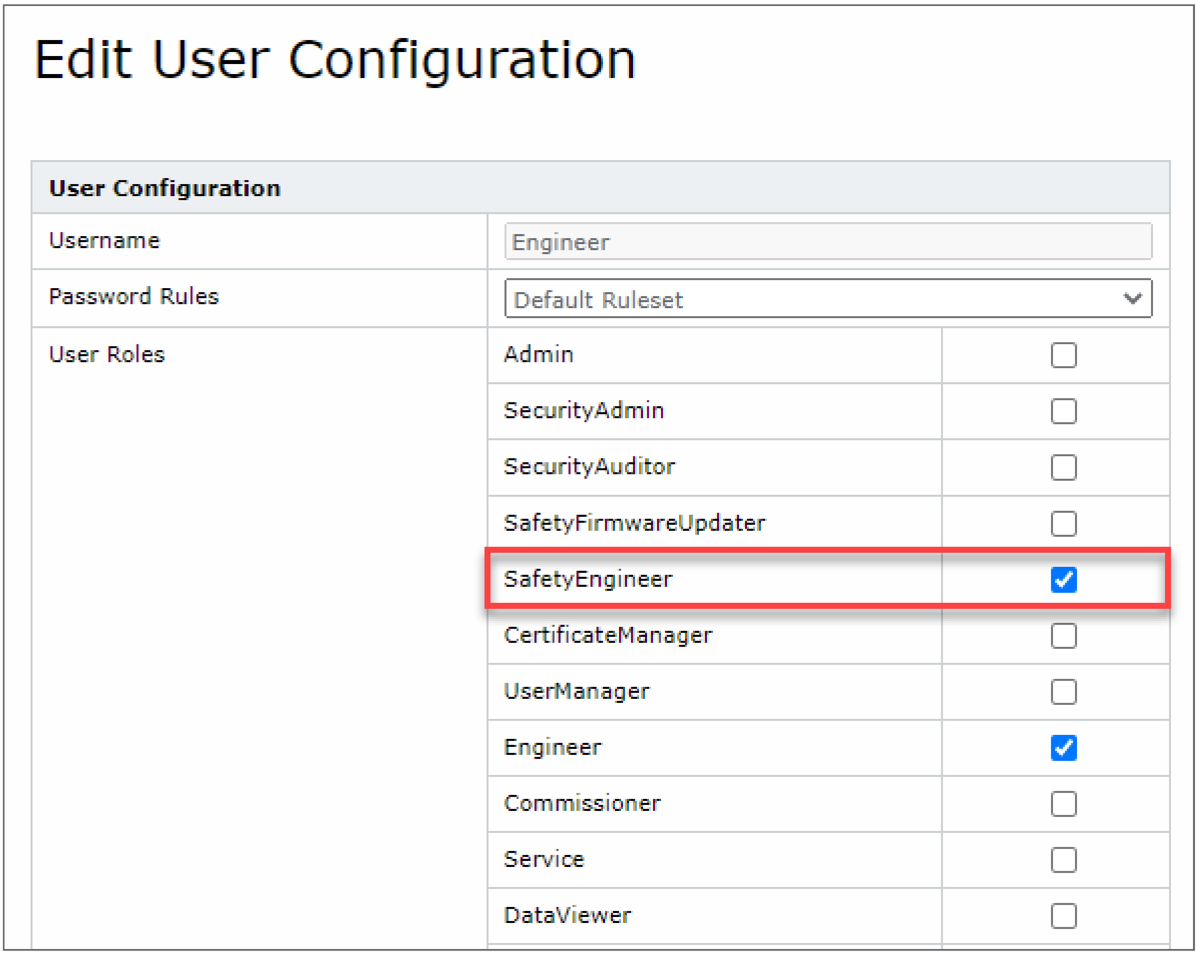
There is a special user role for downloading safety programs: the SafetyEngineer.

Note: You must always assign the SafetyEngineer user role additionally to the Engineer user role, or to another user role that fits your application.; e.g.:

- Commissioner user role combined with SafetyEngineer can only download a non-safety project and can work with the safety project.
- Service user role combined with SafetyEngineer cannot download a non-safety project but can work with the safety project.

As of firmware 2023.0 LTS, safety permissions for the Engineer role are always enabled.

- If safety programs are used and have to be downloaded, set up this user role.

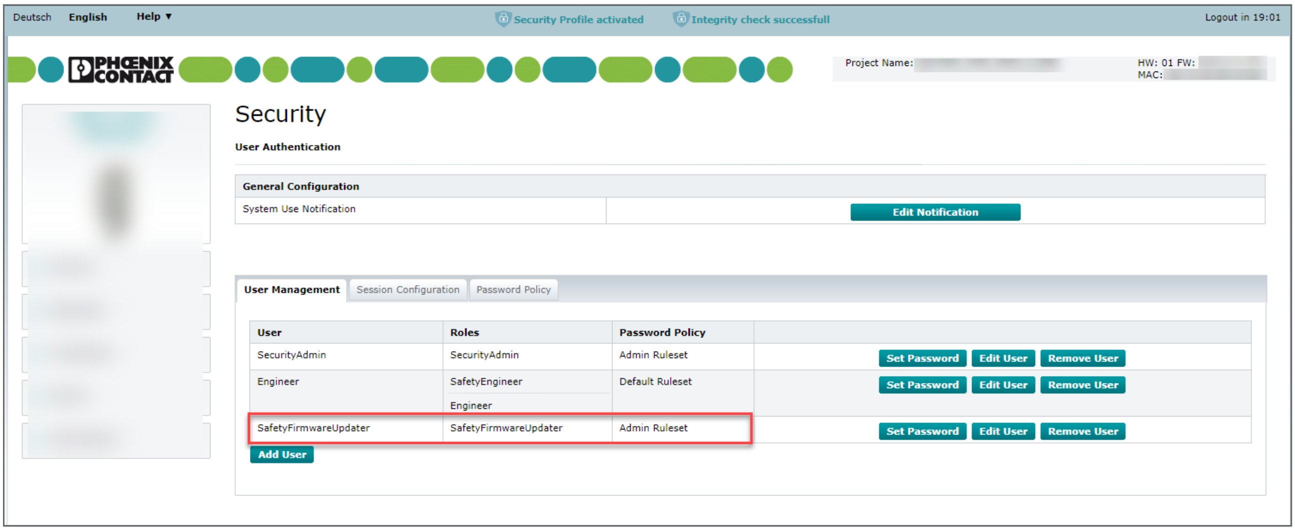


Edit User Configuration

User Configuration		
Username	Engineer	
Password Rules	Default Ruleset	
User Roles	Admin	☐
	SecurityAdmin	☐
	SecurityAuditor	☐
	SafetyFirmwareUpdater	☐
	SafetyEngineer	☑
	CertificateManager	☐
	UserManager	☐
	Engineer	☑
	Commissioner	☐
	Service	☐
	DataViewer	☐

SafetyFirmwareUpdater

Phoenix Contact will provide you with instructions for updating the safety controller on request. You should configure the SafetyFirmwareUpdater user role in advance.



Project Name: [redacted]

HW: 01 FW: [redacted]

MAC: [redacted]

Security

User Authentication

General Configuration	
System Use Notification	Edit Notification

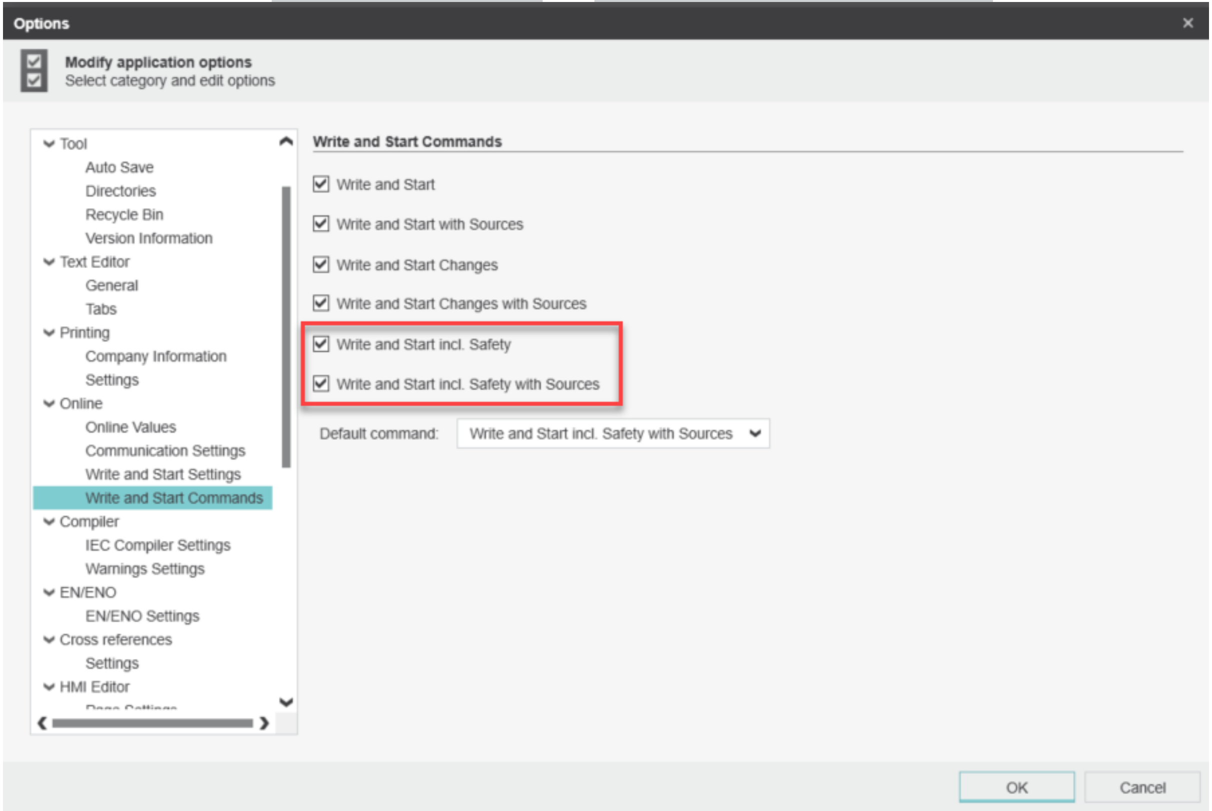
User	Roles	Password Policy	
SecurityAdmin	SecurityAdmin	Admin Ruleset	Set Password Edit User Remove User
Engineer	SafetyEngineer Engineer	Default Ruleset	Set Password Edit User Remove User
SafetyFirmwareUpdater	SafetyFirmwareUpdater	Admin Ruleset	Set Password Edit User Remove User

Configuring PLCnext Engineer (combined safety)

Write and Start Commands

To include the safety-related project when downloading (writing and starting) a project, you must activate the respective checkboxes in the options menu. To do this, proceed as follows:

- In PLCnext Engineer, open the options menu: **Extras** → **Options...**
- Open to **Online** drop-down menu.
- Click on **Write and Start Commands**.
- Activate the checkboxes **Write and Start incl. Safety** and **Write and Start incl. Safety with Sources**:



Write and Start Commands

☑ Write and Start

☑ Write and Start with Sources

☑ Write and Start Changes

☑ Write and Start Changes with Sources

☑ Write and Start incl. Safety

☑ Write and Start incl. Safety with Sources

Default command: Write and Start incl. Safety with Sources

- Click the **OK** button.

ℹ For more information on configuring PLCnext Engineer, refer to the general topic Configuring PLCnext Engineer .

ℹ For more information on PLCnext Engineer, refer to the online help of PLCnext Engineer.

These topics in the online helpmay be of particular interest to you now:

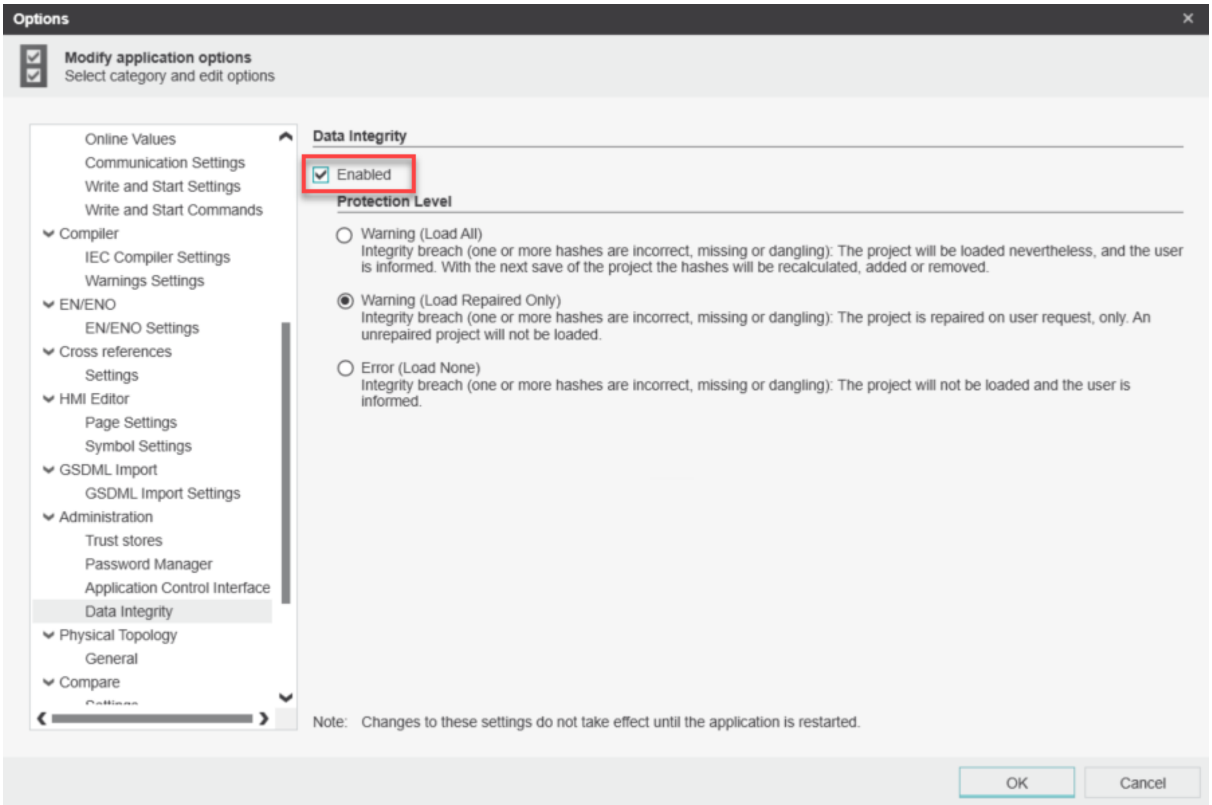
- [Safety-Related Application/Area]
- [Safety PLC Commissioning: From Compiling to Debugging]
- [Safety PLC Runtime Configuration]
- [Safety PLC Password Protection]

Data integrity

In PLCnext Engineer from version 2023.0, you can enable the project integrity check (hash protection of projects and libraries locally stored on your computer). With activated **Enabled** checkbox (hash protection is activated), PLCnext Engineer calculates hash codes (numeric value of fixed length that uniquely identifies data) about the project. The project's hash codes are checked for mismatching or missing hashes when opening the project. Depending on the protection level selected here, you will be informed with a warning/error message and the appropriate action will be performed.
With deactivated hash protection (**Enabled** checkbox deactivated; default setting), PLCnext Engineer does not use hash codes for comparison of project contents. No hash codes are calculated and checked. You will not be informed whether a project has or does not have hash codes.

Phoenix Contact recommends to enable the hash protection (data integrity check). Proceed as follows:

- In PLCnext Engineer, open the options menu: **Extras** → **Options...**
- Open the **Administration** drop-down menu.
- Click on **Data integrity** .
- Activate the checkbox **Enabled** :



Data Integrity

☑ Enabled

Protection Level

○ Warning (Load All)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will be loaded nevertheless, and the user is informed. With the next save of the project the hashes will be recalculated, added or removed.

● Warning (Load Repaired Only)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project is repaired on user request, only. An unrepaired project will not be loaded.

○ Error (Load None)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will not be loaded and the user is informed.

Note: Changes to these settings do not take effect until the application is restarted.

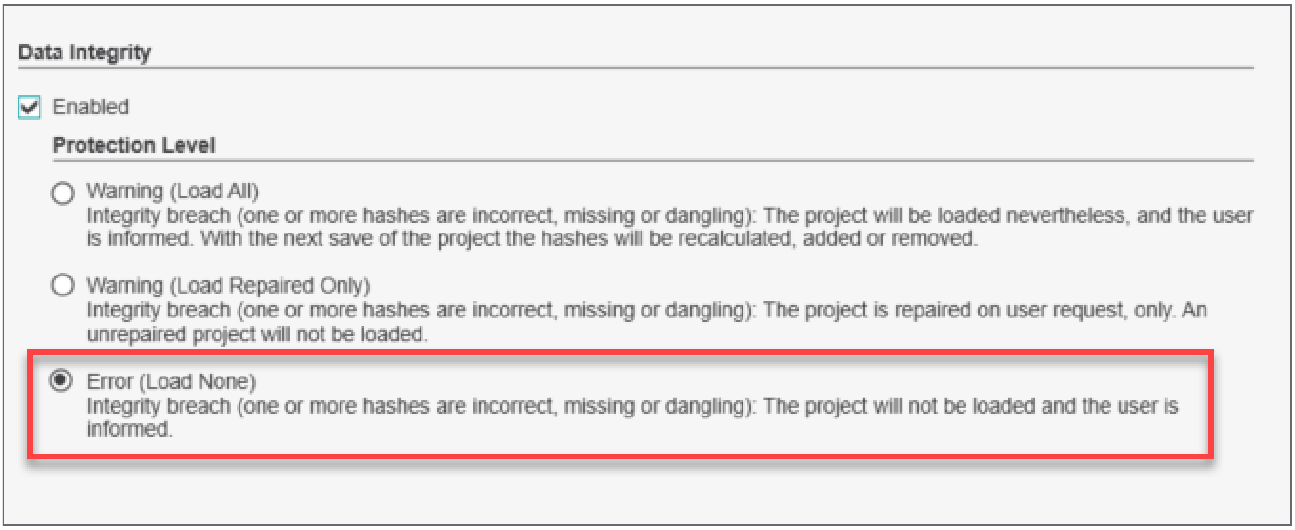
- Click the **OK** button.
- Restart PLCnext Engineer.

Protection level

Which protection level you should set depends on which project you want to open. In any case you must restart PLCnext Engineer for the changes to take effect.

New project

If you want to create a new project, set the protection level **Error (Load None)** :



Data Integrity

☑ Enabled

Protection Level

○ Warning (Load All)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will be loaded nevertheless, and the user is informed. With the next save of the project the hashes will be recalculated, added or removed.

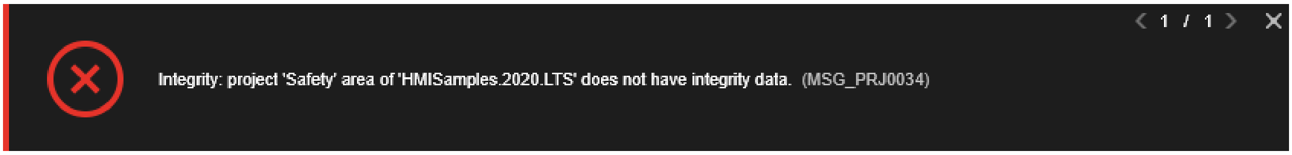
○ Warning (Load Repaired Only)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project is repaired on user request, only. An unrepaired project will not be loaded.

● Error (Load None)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will not be loaded and the user is informed.

In this case, the project is not loaded if an integrity breach is detected and you are informed by a notification in PLCnext Engineer.

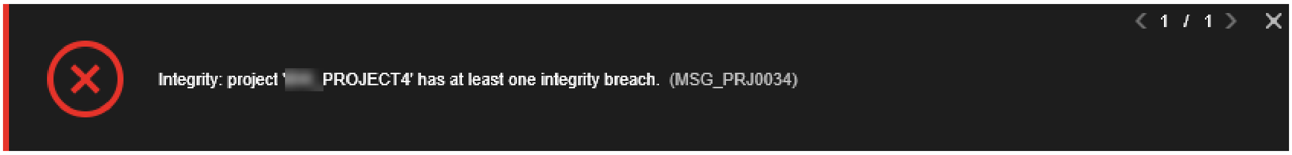
Notifications with protection level **Error (Load None)** :

This is a notification that you will see if your project has no integrity data:



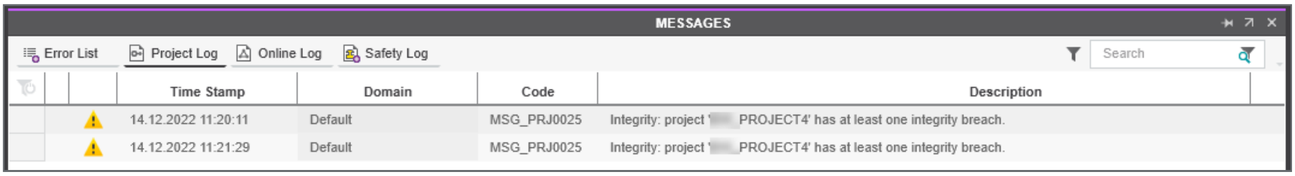
Integrity: project 'Safety' area of 'HMISamples.2020.LTS' does not have integrity data. (MSG_PRJ0034)

And this is a notification that you will see if your project has an integrity breach:



Integrity: project '[redacted] PROJECT4' has at least one integrity breach. (MSG_PRJ0034)

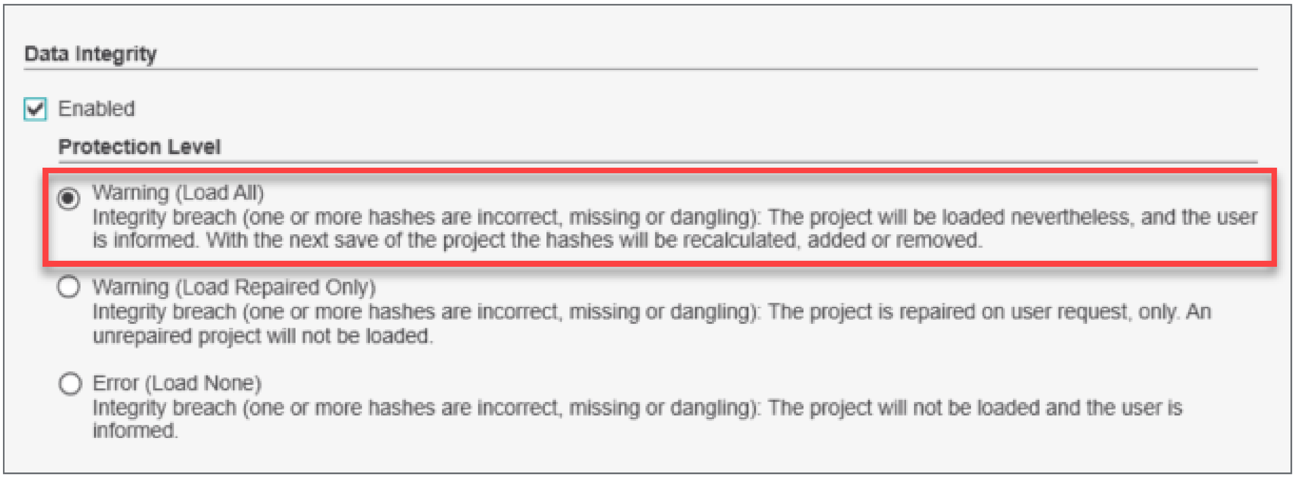
The notifications are also displayed in the messages window on the **Project log** tab (example below).



	Time Stamp	Domain	Code	Description
⚠	14.12.2022 11:20:11	Default	MSG_PRJ0025	Integrity: project '[redacted] PROJECT4' has at least one integrity breach.
⚠	14.12.2022 11:21:29	Default	MSG_PRJ0025	Integrity: project '[redacted] PROJECT4' has at least one integrity breach.

Existing project (PLCnext Engineer version up to 2023.0)

If you want to open an existing project created with a PLCnext Engineer version up to 2023.0, set the protection level `Warning (Load All)`.



Data Integrity

☑ Enabled

Protection Level

● Warning (Load All)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will be loaded nevertheless, and the user is informed. With the next save of the project the hashes will be recalculated, added or removed.

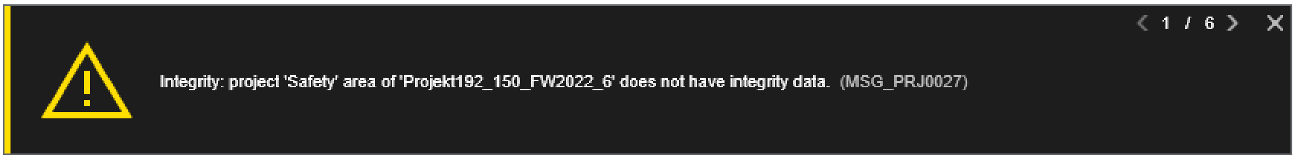
○ Warning (Load Repaired Only)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project is repaired on user request, only. An unrepaired project will not be loaded.

○ Error (Load None)
Integrity breach (one or more hashes are incorrect, missing or dangling): The project will not be loaded and the user is informed.

Single level libraries are automatically converted, multi-level libraries you have to open and save as a project (this will repair them).

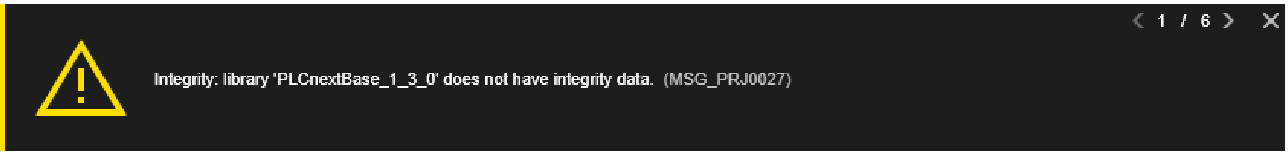
Notifications with protection level `Warning (Load All)`:

This is a notification that you will see if your project has no integrity data:

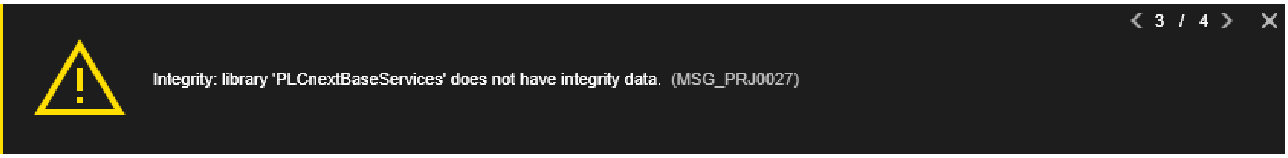


Integrity: project 'Safety' area of 'Projekt192_150_FW2022_6' does not have integrity data. (MSG_PRJ0027)

These are a notifications that you will see if libraries in your project have no integrity data:

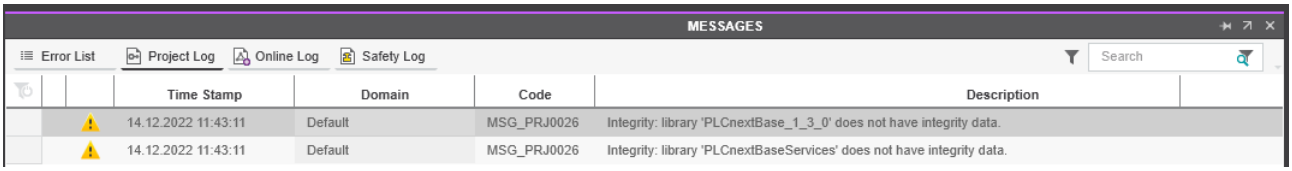


Integrity: library 'PLCnextBase_1_3_0' does not have integrity data. (MSG_PRJ0027)



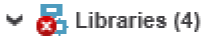
Integrity: library 'PLCnextBaseServices' does not have integrity data. (MSG_PRJ0027)

The notifications are also displayed in the messages window on the `Project log` tab (example below):

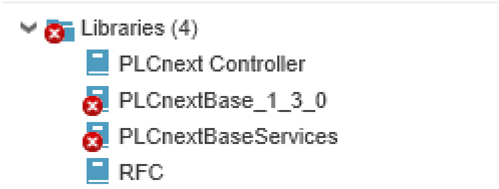


	Time Stamp	Domain	Code	Description
⚠	14.12.2022 11:43:11	Default	MSG_PRJ0026	Integrity: library 'PLCnextBase_1_3_0' does not have integrity data.
⚠	14.12.2022 11:43:11	Default	MSG_PRJ0026	Integrity: library 'PLCnextBaseServices' does not have integrity data.

Corrupt libraries are also marked in the **Components** area:



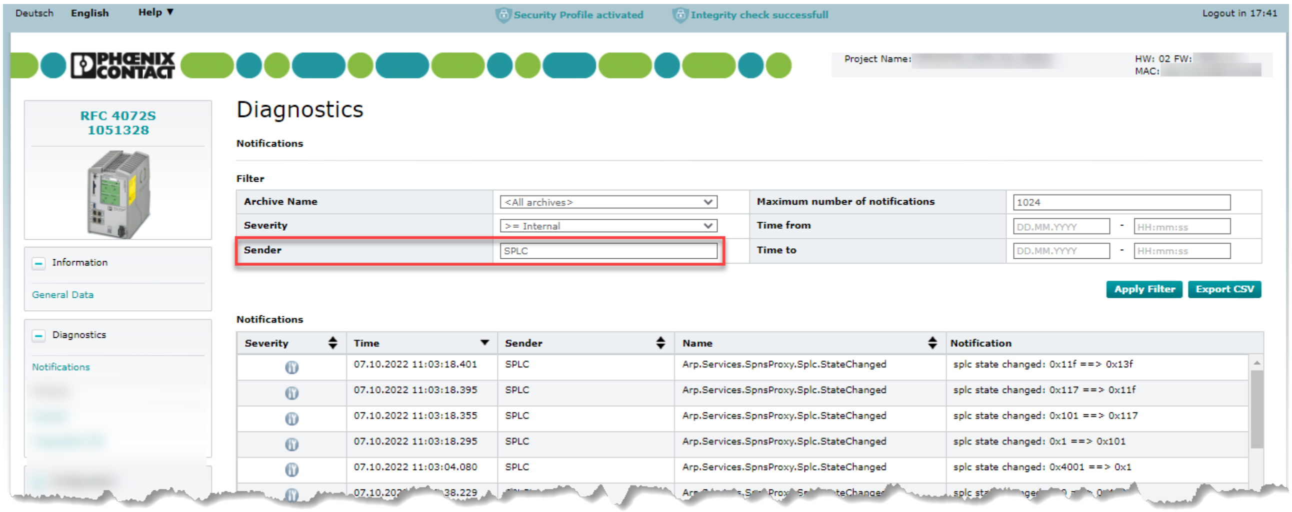
Libraries (4)



Libraries (4)
PLCnext Controller
PLCnextBase_1_3_0
PLCnextBaseServices
RFC

Security logging (combined safety)

To control specific notifications when starting the safety controller, set the filter function "Sender" to "SPLC". Then you will see the corresponding notifications, example see screenshot below.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

Diagnostics

Notifications

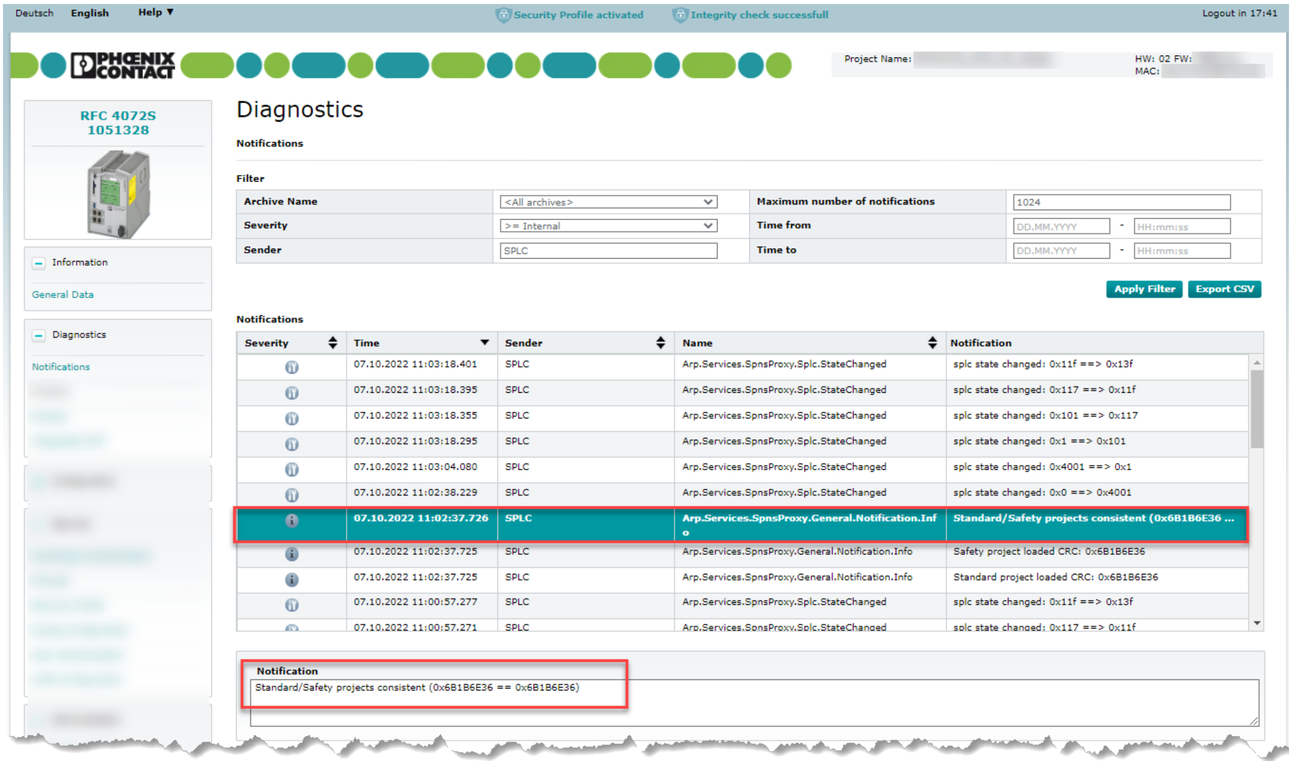
Filter

Archive Name	<All archives>	Maximum number of notifications	1024
Severity	>= Internal	Time from	DD.MM.YYYY - HH:mm:ss
Sender	SPLC	Time to	DD.MM.YYYY - HH:mm:ss

Notifications

Severity	Time	Sender	Name	Notification
	07.10.2022 11:03:18.401	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x11f ==> 0x13f
	07.10.2022 11:03:18.395	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x117 ==> 0x11f
	07.10.2022 11:03:18.355	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x101 ==> 0x117
	07.10.2022 11:03:18.295	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x1 ==> 0x101
	07.10.2022 11:03:04.080	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x4001 ==> 0x1

After starting the safety controller, check the consistency of the safe project and the standard project. Observe the corresponding notification for this, see the following screenshot.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

Diagnostics

Notifications

Filter

Archive Name	<All archives>	Maximum number of notifications	1024
Severity	>= Internal	Time from	DD.MM.YYYY - HH:mm:ss
Sender	SPLC	Time to	DD.MM.YYYY - HH:mm:ss

Notifications

Severity	Time	Sender	Name	Notification
	07.10.2022 11:03:18.401	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x11f ==> 0x13f
	07.10.2022 11:03:18.395	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x117 ==> 0x11f
	07.10.2022 11:03:18.355	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x101 ==> 0x117
	07.10.2022 11:03:18.295	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x1 ==> 0x101
	07.10.2022 11:03:04.080	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x4001 ==> 0x1
	07.10.2022 11:02:38.229	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x0 ==> 0x4001
i	**07.10.2022 11:02:37.726**	**SPLC**	**Arp.Services.SpnsProxy.General.Notification.Info**	**Standard/Safety projects consistent (0x6B1B6E36 ...**
i	07.10.2022 11:02:37.725	SPLC	Arp.Services.SpnsProxy.General.Notification.Info	Safety project loaded CRC: 0x6B1B6E36
i	07.10.2022 11:02:37.725	SPLC	Arp.Services.SpnsProxy.General.Notification.Info	Standard project loaded CRC: 0x6B1B6E36
	07.10.2022 11:00:57.277	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x11f ==> 0x13f
	07.10.2022 11:00:57.271	SPLC	Arp.Services.SpnsProxy.Splc.StateChanged	splc state changed: 0x117 ==> 0x11f

Notification

Standard/Safety projects consistent (0x6B1B6E36 == 0x6B1B6E36)

The meaning of the individual error codes can be found in the respective manual (refer to the topic Product range).

PLCnext Control

In the following you find the IEC 62443 certificates and the functional safety certificates as well as the IEC 62443-4-2 compliance list.

The following devices are certified according to IEC 62443-4-1 and IEC 62443-4-2 Full ML3 Process Profile and therefore subject of this information platform:

- AXC F 1152
- AXC F 2152
- AXC F 3152
- AXC F XT SPLC 1000 (SPLC 1000)
- RFC 4072S
- BPC 9102S

Note: The AXC F XT SPLC 3000 (SPLC 3000, item no. 1160157) is developed in compliance with the IEC 62443-4-1 process and meets the requirements of IEC 62443-4-2, as detailed in the security and safety hardening guidelines.

Officially, the SPLC 3000 will be included in the forthcoming IACS Components PLCnext Control certificate for firmware 2025.0 LTS.

You can find the Functional Safety Certificate here: Functional Safety certificates

In addition, you find the following information:

- Protection against physical access
- Port list
- PLCnext roles and rights list
- OPC UA security compliance list

Certificates

Certificates

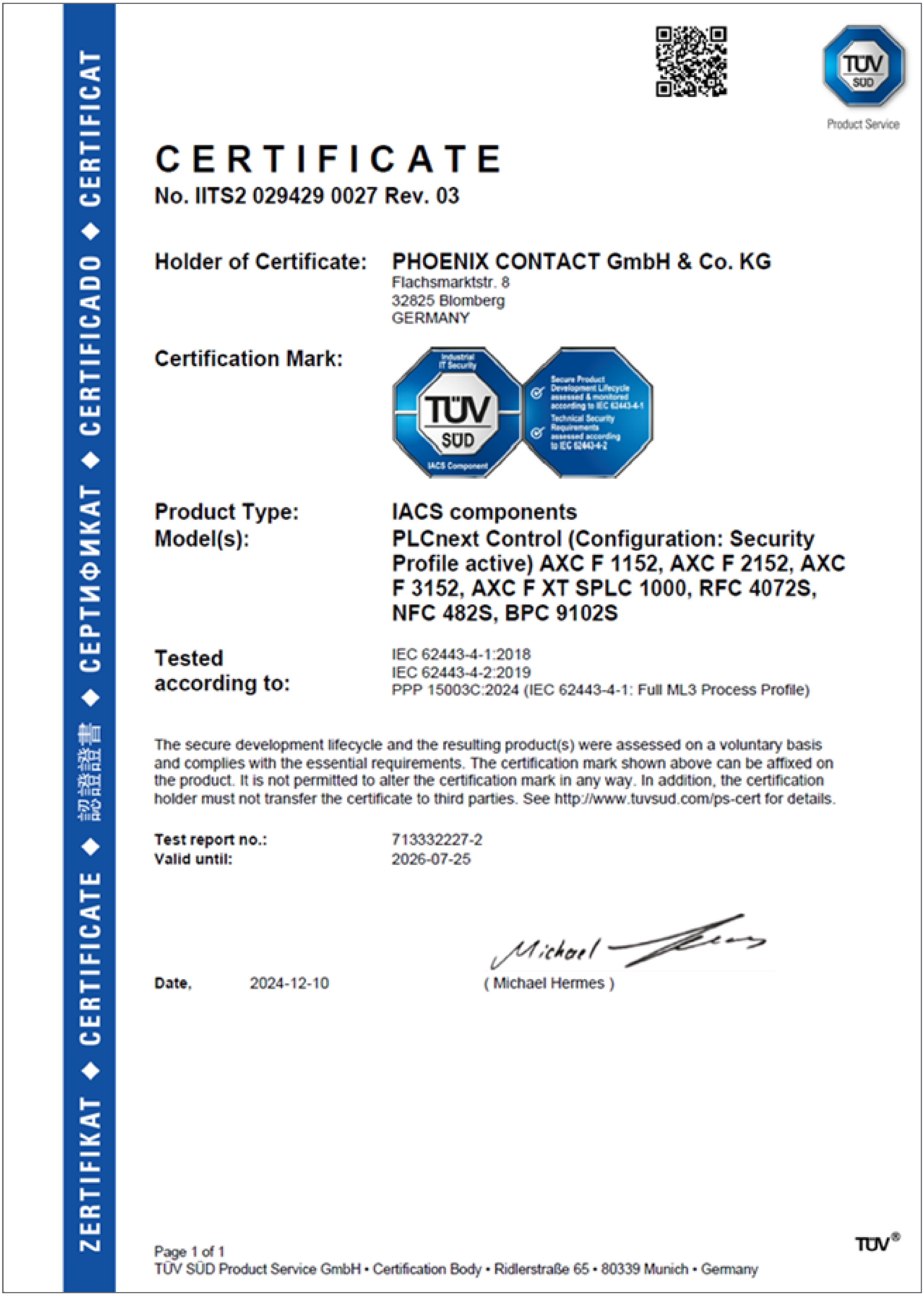
In the following you find the IEC 62443 certificates and the functional safety certificates as well as the IEC 62443-4-2 compliance list.

Certified secure development lifecycle

In December 2024, Phoenix Contact passed the certification process for a secure development lifecycle according to IEC 62443-4-1 and IEC 62443-4-2 for devices of the PLCnext Control series.

The development process audit according to IEC 62443-4-1 ML3 has been proceeded in December 2024.

...certificates see next two pages...



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. IITS2 029429 0027 Rev. 03

Holder of Certificate: **PHOENIX CONTACT GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Industrial IT Security
TÜV SÜD
IACS Component
Secure Product Development Lifecycle assessed & monitored according to IEC 62443-4-1
Technical Security Requirements assessed according to IEC 62443-4-2

Product Type: **IACS components**

Model(s): **PLCnext Control (Configuration: Security Profile active) AXC F 1152, AXC F 2152, AXC F 3152, AXC F XT SPLC 1000, RFC 4072S, NFC 482S, BPC 9102S**

Tested according to:
IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003C:2024 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

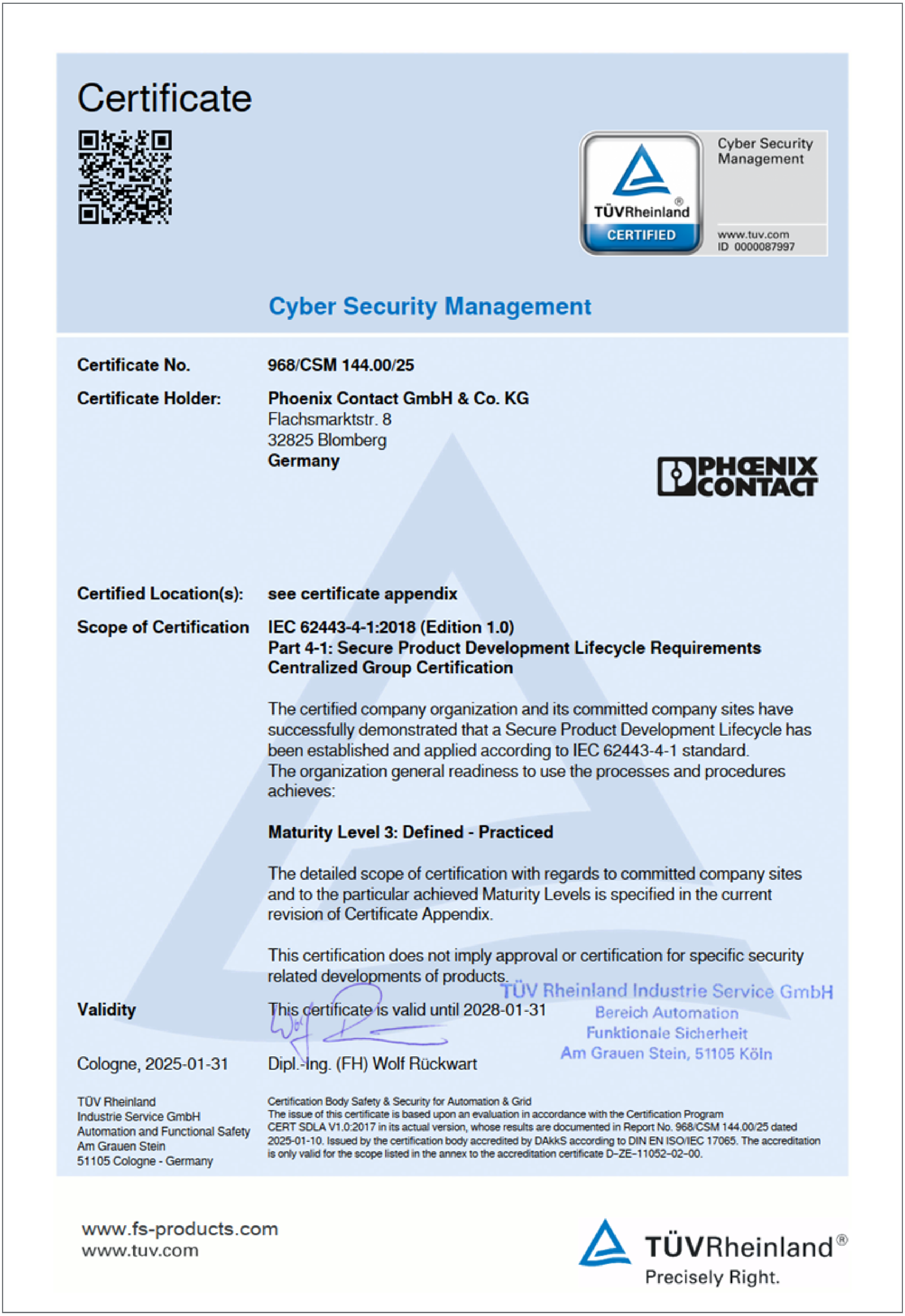
Test report no.:	713332227-2
Valid until:	2026-07-25

Date, 2024-12-10

Michael
(Michael Hermes)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®



Certificate

TÜVRheinland®
CERTIFIED

Cyber Security
Management

www.tuv.com
ID 0000087997

Cyber Security Management

Certificate No. **968/CSM 144.00/25**

Certificate Holder: **Phoenix Contact GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
Germany

PHOENIX CONTACT

Certified Location(s): **see certificate appendix**

Scope of Certification **IEC 62443-4-1:2018 (Edition 1.0)**
Part 4-1: Secure Product Development Lifecycle Requirements
Centralized Group Certification

The certified company organization and its committed company sites have successfully demonstrated that a Secure Product Development Lifecycle has been established and applied according to IEC 62443-4-1 standard.
The organization general readiness to use the processes and procedures achieves:

Maturity Level 3: Defined - Practiced

The detailed scope of certification with regards to committed company sites and to the particular achieved Maturity Levels is specified in the current revision of Certificate Appendix.

This certification does not imply approval or certification for specific security related developments of products.

Validity This certificate is valid until 2028-01-31

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

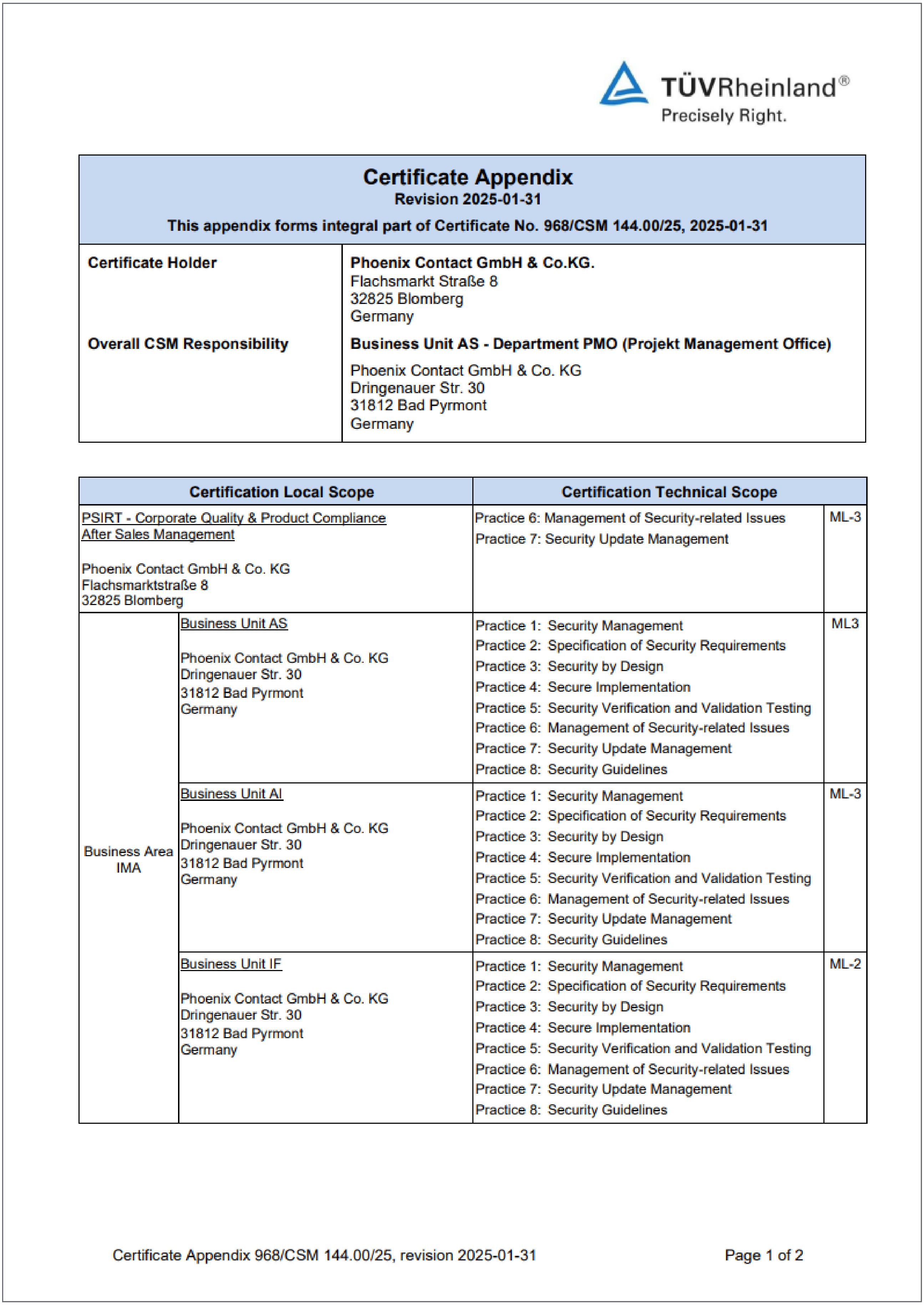
Cologne, 2025-01-31 Dipl.-Ing. (FH) Wolf Rückwart

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT SDLA V1.0:2017 in its actual version, whose results are documented in Report No. 968/CSM 144.00/25 dated 2025-01-10. Issued by the certification body accredited by DAkkS according to DIN EN ISO/IEC 17065. The accreditation is only valid for the scope listed in the annex to the accreditation certificate D-ZE-11052-02-00.

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.



TÜVRheinland®
Precisely Right.

Certificate Appendix

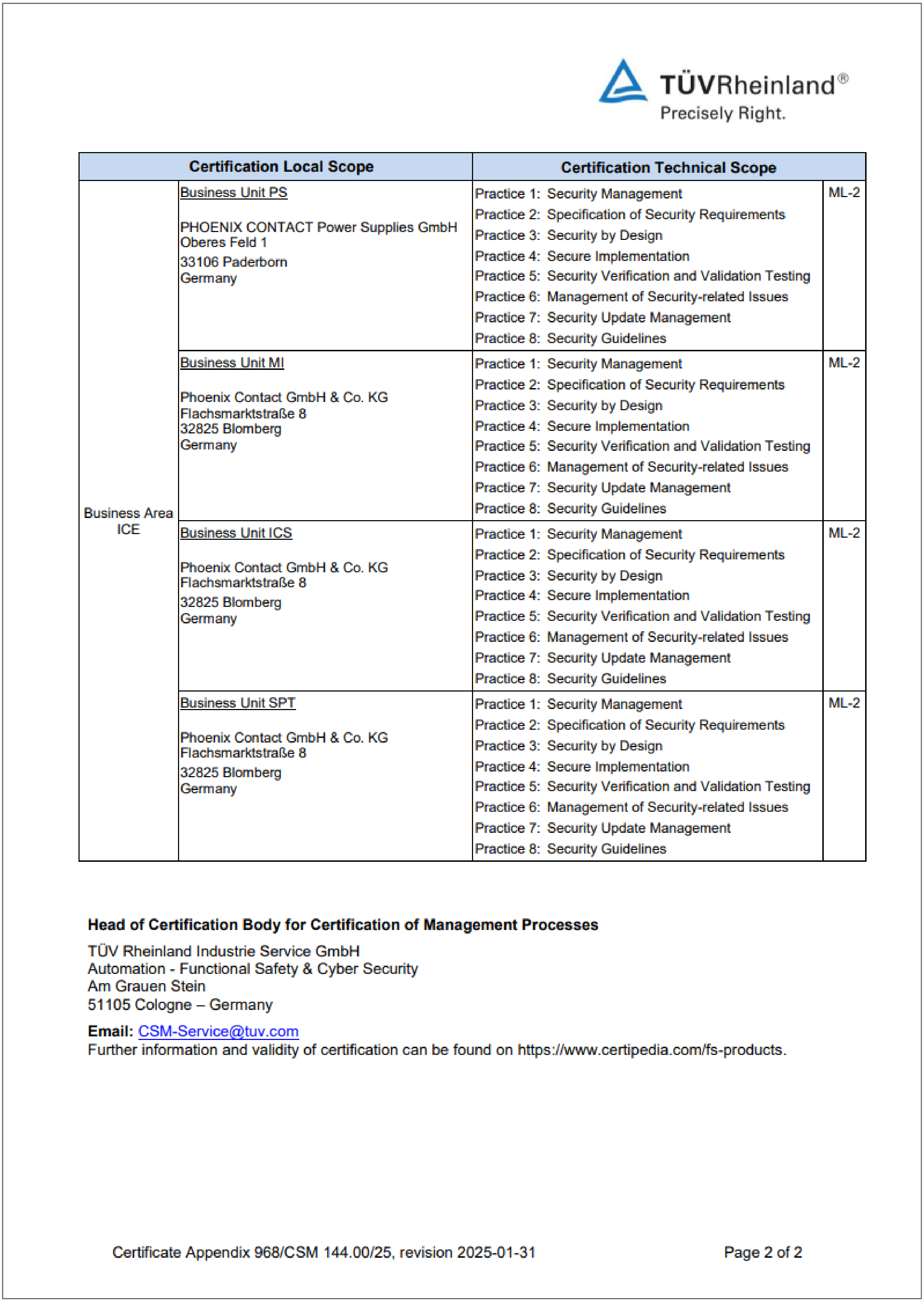
Revision 2025-01-31

This appendix forms integral part of Certificate No. 968/CSM 144.00/25, 2025-01-31

Certificate Holder	**Phoenix Contact GmbH & Co.KG.** Flachsmarkt Straße 8 32825 Blomberg Germany
Overall CSM Responsibility	**Business Unit AS - Department PMO (Projekt Management Office)** Phoenix Contact GmbH & Co. KG Dringenauer Str. 30 31812 Bad Pyrmont Germany

Certification Local Scope		**Certification Technical Scope**	
PSIRT - Corporate Quality & Product Compliance After Sales Management Phoenix Contact GmbH & Co. KG Flachsmarktstraße 8 32825 Blomberg		Practice 6: Management of Security-related Issues Practice 7: Security Update Management	ML-3
Business Area IMA	Business Unit AS Phoenix Contact GmbH & Co. KG Dringenauer Str. 30 31812 Bad Pyrmont Germany	Practice 1: Security Management Practice 2: Specification of Security Requirements Practice 3: Security by Design Practice 4: Secure Implementation Practice 5: Security Verification and Validation Testing Practice 6: Management of Security-related Issues Practice 7: Security Update Management Practice 8: Security Guidelines	ML3
	Business Unit AI Phoenix Contact GmbH & Co. KG Dringenauer Str. 30 31812 Bad Pyrmont Germany	Practice 1: Security Management Practice 2: Specification of Security Requirements Practice 3: Security by Design Practice 4: Secure Implementation Practice 5: Security Verification and Validation Testing Practice 6: Management of Security-related Issues Practice 7: Security Update Management Practice 8: Security Guidelines	ML-3
	Business Unit IF Phoenix Contact GmbH & Co. KG Dringenauer Str. 30 31812 Bad Pyrmont Germany	Practice 1: Security Management Practice 2: Specification of Security Requirements Practice 3: Security by Design Practice 4: Secure Implementation Practice 5: Security Verification and Validation Testing Practice 6: Management of Security-related Issues Practice 7: Security Update Management Practice 8: Security Guidelines	ML-2

Certificate Appendix 968/CSM 144.00/25, revision 2025-01-31 Page 1 of 2



Certification Local Scope		Certification Technical Scope	
Business Area ICE	Business Unit PS PHOENIX CONTACT Power Supplies GmbH Oberes Feld 1 33106 Paderborn Germany	Practice 1: Security Management Practice 2: Specification of Security Requirements Practice 3: Security by Design Practice 4: Secure Implementation Practice 5: Security Verification and Validation Testing Practice 6: Management of Security-related Issues Practice 7: Security Update Management Practice 8: Security Guidelines	ML-2
	Business Unit MI Phoenix Contact GmbH & Co. KG Flachsmarktstraße 8 32825 Blomberg Germany	Practice 1: Security Management Practice 2: Specification of Security Requirements Practice 3: Security by Design Practice 4: Secure Implementation Practice 5: Security Verification and Validation Testing Practice 6: Management of Security-related Issues Practice 7: Security Update Management Practice 8: Security Guidelines	ML-2
	Business Unit ICS Phoenix Contact GmbH & Co. KG Flachsmarktstraße 8 32825 Blomberg Germany	Practice 1: Security Management Practice 2: Specification of Security Requirements Practice 3: Security by Design Practice 4: Secure Implementation Practice 5: Security Verification and Validation Testing Practice 6: Management of Security-related Issues Practice 7: Security Update Management Practice 8: Security Guidelines	ML-2
	Business Unit SPT Phoenix Contact GmbH & Co. KG Flachsmarktstraße 8 32825 Blomberg Germany	Practice 1: Security Management Practice 2: Specification of Security Requirements Practice 3: Security by Design Practice 4: Secure Implementation Practice 5: Security Verification and Validation Testing Practice 6: Management of Security-related Issues Practice 7: Security Update Management Practice 8: Security Guidelines	ML-2

Head of Certification Body for Certification of Management Processes

TÜV Rheinland Industrie Service GmbH
Automation - Functional Safety & Cyber Security
Am Grauen Stein
51105 Cologne – Germany

Email: CSM-Service@tuv.com
Further information and validity of certification can be found on https://www.certipedia.com/fs-products.

Certificate Appendix 968/CSM 144.00/25, revision 2025-01-31

Page 2 of 2

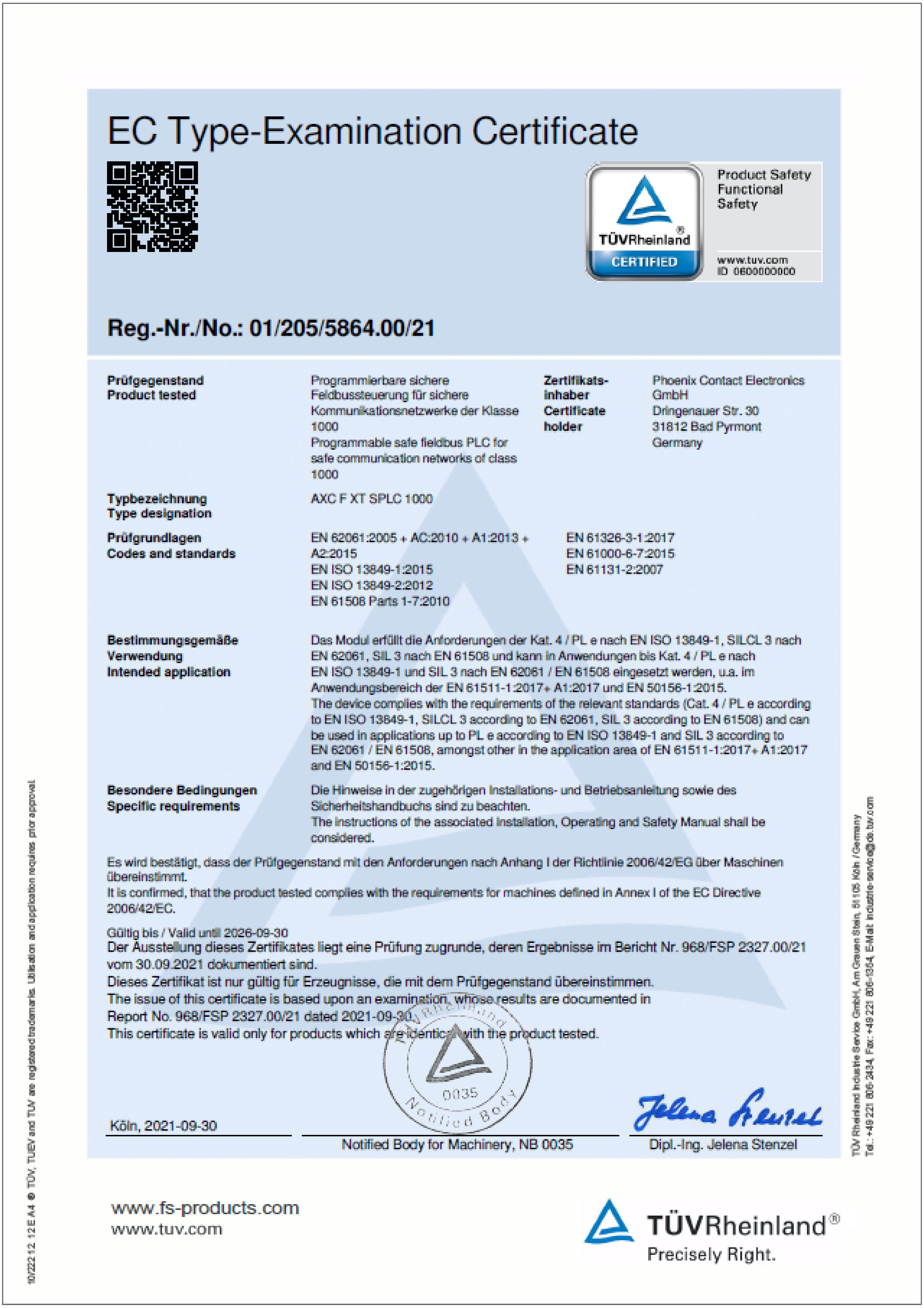
Functional Safety certificates

AXC F XT SPLC 1000

The certificate is valid for the following safety related component:

- AXC F XT SPLC 1000

...certificate see next page...



EC Type-Examination Certificate

Product Safety
Functional
Safety

TÜVRheinland®
CERTIFIED

www.tuv.com
ID 0600000000

Reg.-Nr./No.: 01/205/5864.00/21

Prüfgegenstand
Product tested

Programmierbare sichere Feldbussteuerung für sichere Kommunikationsnetzwerke der Klasse 1000
Programmable safe fieldbus PLC for safe communication networks of class 1000

Zertifikats-inhaber
Certificate holder

Phoenix Contact Electronics GmbH
Dringenauer Str. 30
31812 Bad Pyrmont
Germany

Typbezeichnung
Type designation

AXC F XT SPLC 1000

Prüfgrundlagen
Codes and standards

EN 62061:2005 + AC:2010 + A1:2013 + A2:2015
EN ISO 13849-1:2015
EN ISO 13849-2:2012
EN 61508 Parts 1-7:2010
EN 61326-3-1:2017
EN 61000-6-7:2015
EN 61131-2:2007

Bestimmungsgemäße Verwendung
Intended application

Das Modul erfüllt die Anforderungen der Kat. 4 / PL e nach EN ISO 13849-1, SILCL 3 nach EN 62061, SIL 3 nach EN 61508 und kann in Anwendungen bis Kat. 4 / PL e nach EN ISO 13849-1 und SIL 3 nach EN 62061 / EN 61508 eingesetzt werden, u.a. im Anwendungsbereich der EN 61511-1:2017+ A1:2017 und EN 50156-1:2015.
The device complies with the requirements of the relevant standards (Cat. 4 / PL e according to EN ISO 13849-1, SILCL 3 according to EN 62061, SIL 3 according to EN 61508) and can be used in applications up to PL e according to EN ISO 13849-1 and SIL 3 according to EN 62061 / EN 61508, amongst other in the application area of EN 61511-1:2017+ A1:2017 and EN 50156-1:2015.

Besondere Bedingungen
Specific requirements

Die Hinweise in der zugehörigen Installations- und Betriebsanleitung sowie des Sicherheitshandbuchs sind zu beachten.
The instructions of the associated Installation, Operating and Safety Manual shall be considered.

Es wird bestätigt, dass der Prüfgegenstand mit den Anforderungen nach Anhang I der Richtlinie 2006/42/EG über Maschinen übereinstimmt.
It is confirmed, that the product tested complies with the requirements for machines defined in Annex I of the EC Directive 2006/42/EC.

Gültig bis / Valid until 2026-09-30
Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/FSP 2327.00/21 vom 30.09.2021 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 2327.00/21 dated 2021-09-30.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland
0035
Notified Body

Köln, 2021-09-30

Notified Body for Machinery, NB 0035

Jelena Stenzel
Dipl.-Ing. Jelena Stenzel

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

10/222 12 12 E A4 ® TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

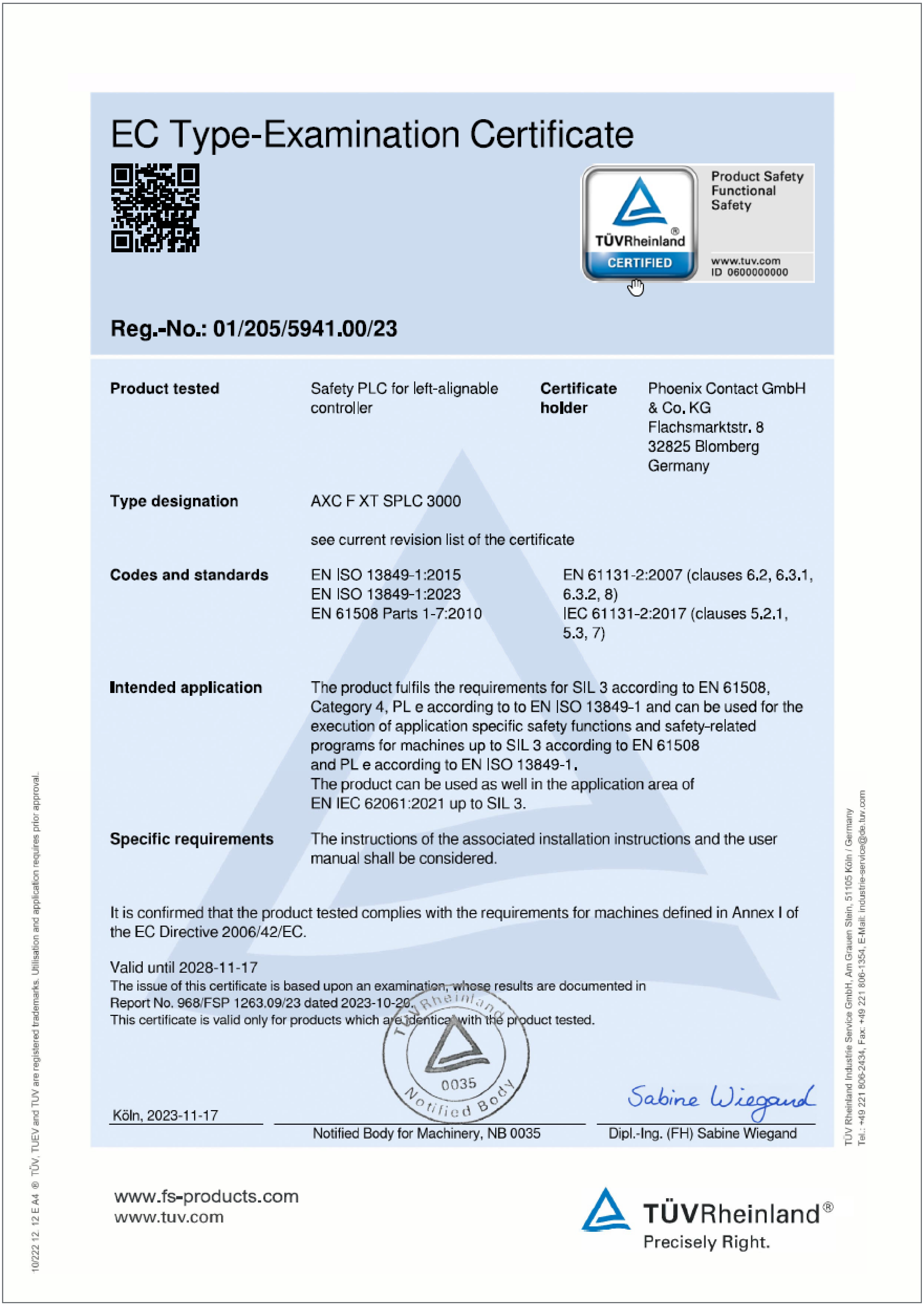
TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-3434, Fax: +49 221 806-1354, E-Mail: industrie-service@de.tuv.com

AXC F XT SPLC 3000

The certificate is valid for the following safety related component:

- AXC F XT SPLC 3000

...certificate see next page...



EC Type-Examination Certificate

Product Safety
Functional
Safety

TÜVRheinland®
CERTIFIED

www.tuv.com
ID 0600000000

Reg.-No.: 01/205/5941.00/23

Product tested	Safety PLC for left-alignable controller	**Certificate holder**	Phoenix Contact GmbH & Co. KG Flachsmarktstr. 8 32825 Blomberg Germany

Type designation AXC F XT SPLC 3000

see current revision list of the certificate

Codes and standards

EN ISO 13849-1:2015
EN ISO 13849-1:2023
EN 61508 Parts 1-7:2010
EN 61131-2:2007 (clauses 6.2, 6.3.1, 6.3.2, 8)
IEC 61131-2:2017 (clauses 5.2.1, 5.3, 7)

Intended application The product fulfils the requirements for SIL 3 according to EN 61508, Category 4, PL e according to to EN ISO 13849-1 and can be used for the execution of application specific safety functions and safety-related programs for machines up to SIL 3 according to EN 61508 and PL e according to EN ISO 13849-1.
The product can be used as well in the application area of EN IEC 62061:2021 up to SIL 3.

Specific requirements The instructions of the associated installation instructions and the user manual shall be considered.

It is confirmed that the product tested complies with the requirements for machines defined in Annex I of the EC Directive 2006/42/EC.

Valid until 2028-11-17
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1263.09/23 dated 2023-10-20.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland
0035
Notified Body

Köln, 2023-11-17

Notified Body for Machinery, NB 0035

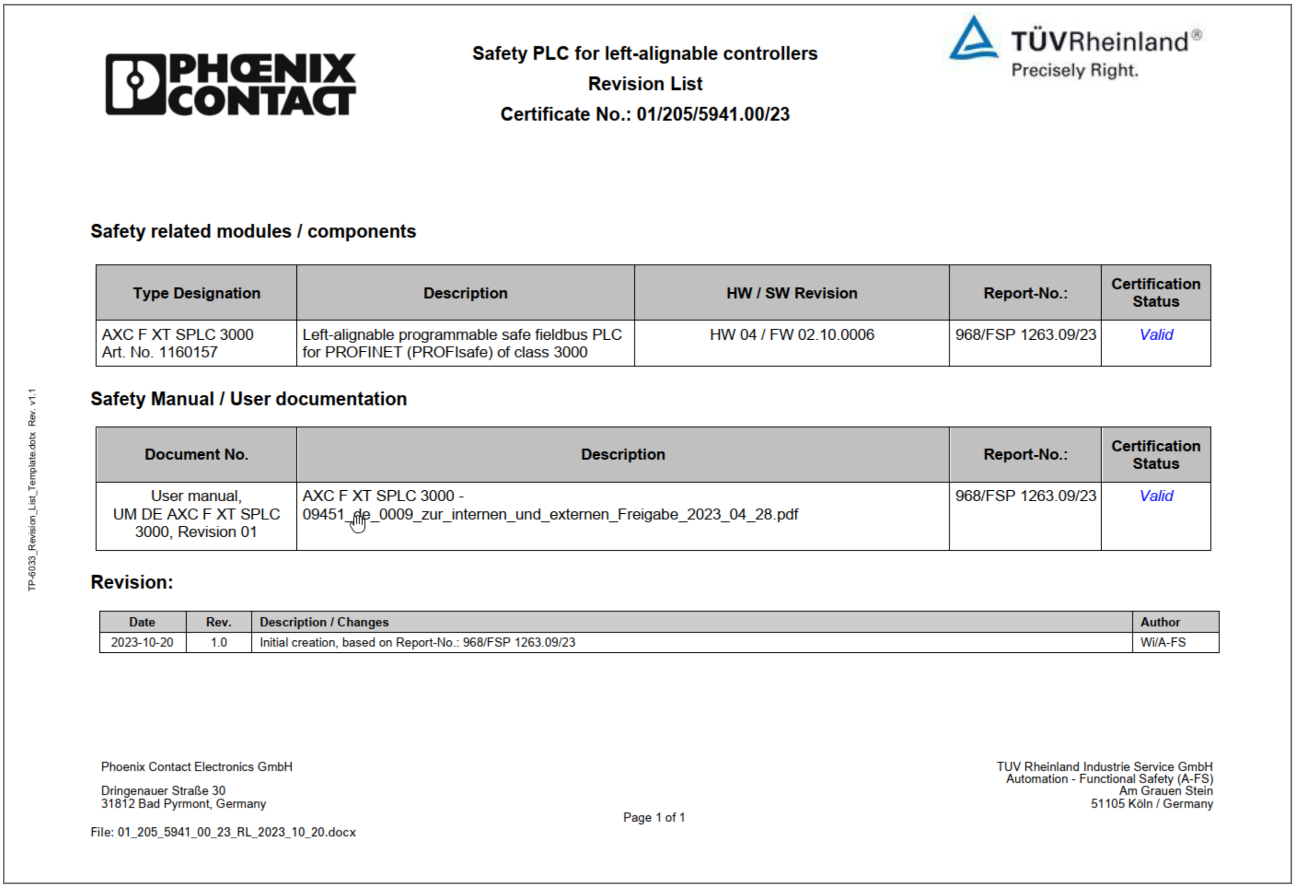
Sabine Wiegand
Dipl.-Ing. (FH) Sabine Wiegand

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

10/222 12 12 E A4 ® TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-2434, Fax: +49 221 806-1354, E-Mail: industrie-service@de.tuv.com



Safety PLC for left-alignable controllers
Revision List
Certificate No.: 01/205/5941.00/23

TÜVRheinland®
Precisely Right.

TP-6033_Revision_List_Template.dotx Rev. v1.1

Safety related modules / components

Type Designation	Description	HW / SW Revision	Report-No.:	Certification Status
AXC F XT SPLC 3000 Art. No. 1160157	Left-alignable programmable safe fieldbus PLC for PROFINET (PROFIsafe) of class 3000	HW 04 / FW 02.10.0006	968/FSP 1263.09/23	*Valid*

Safety Manual / User documentation

Document No.	Description	Report-No.:	Certification Status
User manual, UM DE AXC F XT SPLC 3000, Revision 01	AXC F XT SPLC 3000 - 09451_de_0009_zur_internen_und_externen_Freigabe_2023_04_28.pdf	968/FSP 1263.09/23	*Valid*

Revision:

Date	Rev.	Description / Changes	Author
2023-10-20	1.0	Initial creation, based on Report-No.: 968/FSP 1263.09/23	Wi/A-FS

Phoenix Contact Electronics GmbH

Dringenauer Straße 30
31812 Bad Pyrmont, Germany

TUV Rheinland Industrie Service GmbH
Automation - Functional Safety (A-FS)
Am Grauen Stein
51105 Köln / Germany

Page 1 of 1

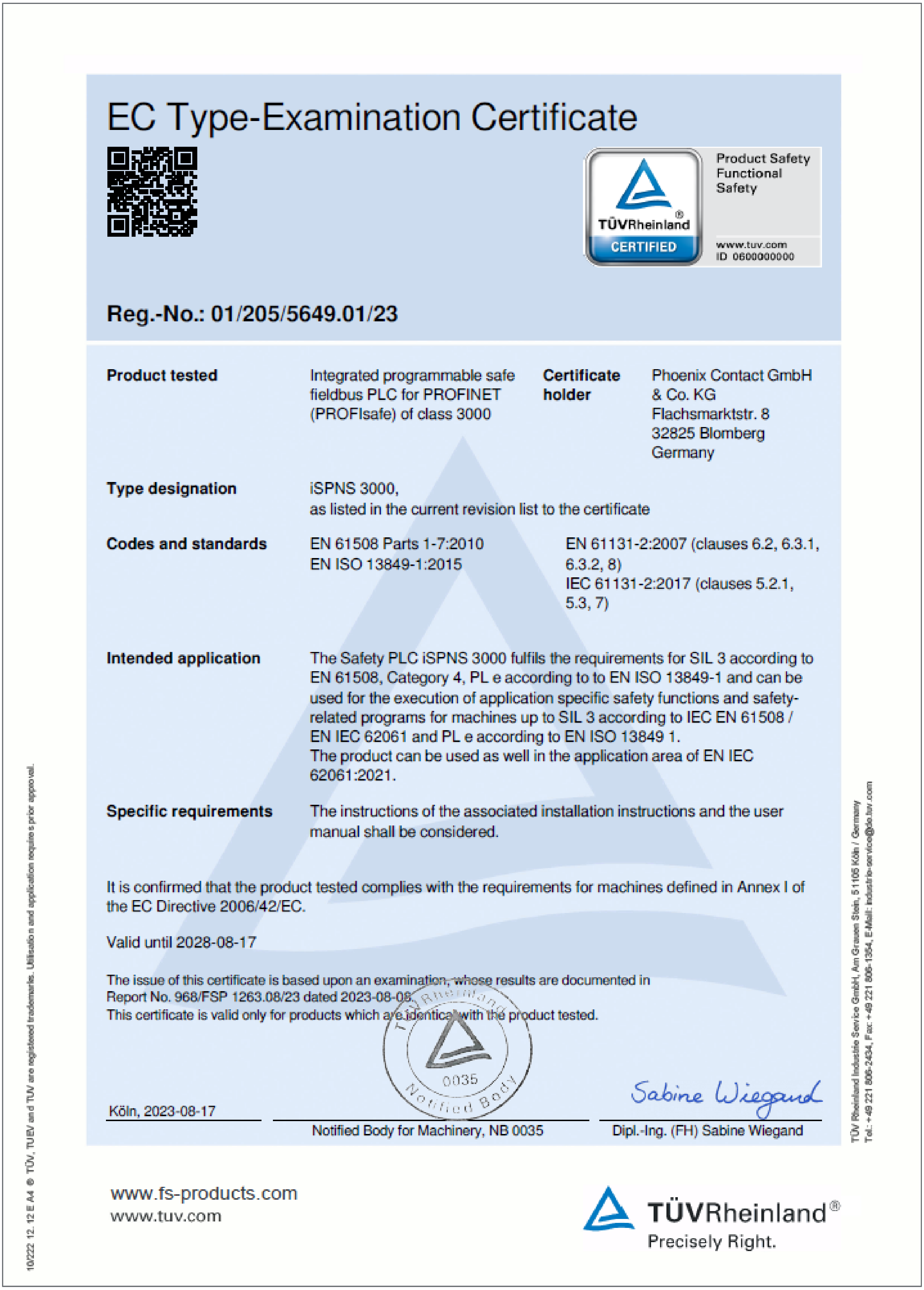
File: 01_205_5941_00_23_RL_2023_10_20.docx

iSPNS 3000

The certificate is valid for the following safety-related components:

- RFC 4072S

...certificate see next page...



EC Type-Examination Certificate

Product Safety
Functional
Safety

TÜVRheinland®
CERTIFIED

www.tuv.com
ID 0600000000

Reg.-No.: 01/205/5649.01/23

Product tested
Integrated programmable safe fieldbus PLC for PROFINET (PROFIsafe) of class 3000

Certificate holder
Phoenix Contact GmbH
& Co. KG
Flachsmarktstr. 8
32825 Blomberg
Germany

Type designation
iSPNS 3000,
as listed in the current revision list to the certificate

Codes and standards
EN 61508 Parts 1-7:2010
EN ISO 13849-1:2015
EN 61131-2:2007 (clauses 6.2, 6.3.1, 6.3.2, 8)
IEC 61131-2:2017 (clauses 5.2.1, 5.3, 7)

Intended application
The Safety PLC iSPNS 3000 fulfils the requirements for SIL 3 according to EN 61508, Category 4, PL e according to to EN ISO 13849-1 and can be used for the execution of application specific safety functions and safety-related programs for machines up to SIL 3 according to IEC EN 61508 / EN IEC 62061 and PL e according to EN ISO 13849 1.
The product can be used as well in the application area of EN IEC 62061:2021.

Specific requirements
The instructions of the associated installation instructions and the user manual shall be considered.

It is confirmed that the product tested complies with the requirements for machines defined in Annex I of the EC Directive 2006/42/EC.

Valid until 2028-08-17

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1263.08/23 dated 2023-08-08.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland
0035
Notified Body

Köln, 2023-08-17

Notified Body for Machinery, NB 0035

Sabine Wiegand
Dipl.-Ing. (FH) Sabine Wiegand

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

10/222 12. 12 E A4 © TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel: +49 221 806-2434, Fax: +49 221 806-1354, E-Mail: industrie-service@de.tuv.com

IEC 62443-4-2 compliance list

Introduction

PLCnext Control AXC F 1152, AXC F 2152 and AXC F 3152 from firmware version 2024.0.x LTS, the SPLC 1000 from firmware version 01.01.0000, the RFC 4072S from firmware version 2024.0 LTS and the BPC 9102S from firmware version 2024.0.4 LTS are certified according to IEC 62443-4-1 and IEC 62443-4-2 Full ML3 Process Profile.

Note: The AXC F XT SPLC 3000 (SPLC 3000, item no. 1160157) is developed in compliance with the IEC 62443-4-1 process and meets the requirements of IEC 62443-4-2, as detailed in the security and safety hardening guidelines.

Officially, the SPLC 3000 will be included in the forthcoming IACS Components PLCnext Control certificate for firmware 2025.0 LTS.

You can find the Functional Safety Certificate here: Functional Safety certificates

Note: If you are using older firmware versions with security certification, you must update to firmware version 2024.0.x LTS.
An update to the current LTS version is also essential, as many security vulnerabilities (CVEs) in Linux components are fixed in every LTS version.

For more information on the certified controller, refer to the topics AXC F 1152, AXC F 2152, AXC F 3152, SPLC 1000, RFC 4072S and BPC 9102S.

They support an IEC 62443-4-2 SL2 feature set like described below. In addition a subset of SL3 features is already supported.

...continuation see next page...

FR1 – Identification and authentication control (IAC)

No.	Description	Security Level	Fulfillment	Links
CR 1.1	Human user identification and authentication	SL1	PLCnext Technology provides that each user can be identified and authenticated by the PLCnext Technology User Manager in the WBM.	– Creating users in the PLCnext Technology - Security Info Center – User authentication in the main PLCnext Technology - Info Center
CR 1.1 RE1	Unique identification and authentication	SL2	PLCnext Technology provides that each user can be uniquely identified and authenticated by the PLCnext Technology User Manager in the WBM.	– Creating users in the PLCnext Technology - Security Info Center – User authentication in the main PLCnext Technology - Info Center
CR 1.2	Software process and device identification and authentication	SL2	PLCnext Technology provides that each non human user access can be identified and authenticated by the PLCnext Technology User Manager in the WBM.	– Certificate authentication in the main PLCnext Technology - Info Center
CR 1.2 RE1	Unique identification and authentication	SL3	PLCnext Technology provides that each non human user access can be uniquely identified and authenticated by the PLCnext Technology User Manager in the WBM. Via the Trust Store unique identification and authentication can be configured.	– Certificate authentication in the main PLCnext Technology - Info Center
CR 1.3	Account management	SL1	PLCnext Technology provides that users can be managed via the User Manager in the WBM, via LDAP.	– LDAP Configurationin the main PLCnext Technology - Info Center
CR 1.4	Identifier management	SL1	PLCnext Technology provides that users can be managed via the User Manager in the WBM, via LDAP, or via the Linux Configuration files.	– Creating users in the PLCnext Technology - Security Info Center – User authentication in the main PLCnext Technology - Info Center – LDAP Configurationin the main PLCnext Technology - Info Center
CR 1.5	Authenticator management	SL1	PLCnext Technology provides that the initial authenticator content is defined by the PLCnext Technology User Manager in the WBM.	– Creating users in the PLCnext Technology - Security Info Center – User authentication in the main PLCnext Technology - Info Center – Configuring authentication errors and sessions in the PLCnext Technology - Security Info Center – LDAP Configurationin the main PLCnext Technology - Info Center

No.	Description	Security Level	Fulfillment	Links
CR 1.7	Strength of password-based authentication	SL1	PLCnext Technology provides that each user is assigned to configurable password complexity rulesets. The rulesets can be configured according to password guidelines.	– Password complexity rules in the PLCnext Technology - Security Info Center – Creating users in the PLCnext Technology - Security Info Center
CR 1.7 RE1	Password generation and lifetime restrictions for human users	SL3	PLCnext Technology provides that each user is assigned to configurable password complexity rulesets. The rulesets can be configured according to password guidelines including expiration rules.	– Password complexity rules in the PLCnext Technology - Security Info Center
CR 1.8	Public key infrastructure certificates	SL2	PLCnext Technology provides an Identity Store and a Trust Store in the WBM.	– Certificate authentication in the main PLCnext Technology - Info Center
CR 1.9	Strength of public key authentication	SL2	PLCnext Technology provides an Identity Store and a Trust Store in the WBM.	– Certificate authentication in the main PLCnext Technology - Info Center
CR 1.9 RE1	Hardware security for public key-based authentication	SL3	The device identity is protected via TPM. Other identities are stored on the internal SD card and need to be protected by the system environment.	– Certificate authentication in the main PLCnext Technology - Info Center
CR 1.10	Authenticator feedback	SL1	Each component of the PLCnext Technology Runtime with authentication function provides the possibility to hide the feedback of authenticator information during the authentication process.	– WBM access and first steps in the main PLCnext Technology - Info Center
CR 1.11	Unsuccessful login attempts	SL1	PLCnext Technology defines rules how to handle authentication errors including unsuccessful login attempts.	– Authentication failure handling in the main PLCnext Technology - Info Center – Configuring authentication errors and sessionsin the PLCnext Technology - Security Info Center
CR 1.12	System use notification	SL1	PLCnext Technology provides that a system usage message is displayed before authentication. The message is configurable by authorized personnel in the user authentication.	– Activating PLCnext Engineer HMI in the PLCnext Technology - Security Info Center – Creating users in the PLCnext Technology - Security Info Center – User Authentication in the main PLCnext Technology - Info Center
CR 1.14	Strength of symmetric key authentication	SL2	Symmetric keys are used only internally for TLS and OPC UA® secure communication.	

FR2 – Use control (UC)

No.	Description	Security Level	Fulfillment	Links
CR 2.1	Authorization enforcement	SL1	PLCnext Technology provides that users can be managed via the User Manager in the WBM, via LDAP, or via the Linux Configuration files.	– Creating users in the PLCnext Technology - Security Info Center – User authentication in the main PLCnext Technology - Info Center – LDAP Configurationin the main PLCnext Technology - Info Center
CR 2.1 RE1	Authorization enforcement for all users (humans, software processes and devices)	SL2	PLCnext Technology provides that users can be managed via the User Manager in the WBM, via LDAP, or via the Linux Configuration files. User are assigned to roles which have a predefined set of permissions.	– Creating users in the PLCnext Technology - Security Info Center – User authentication in the main PLCnext Technology - Info Center – LDAP Configurationin the main PLCnext Technology - Info Center
CR 2.1 RE2	Permission mapping to roles	SL2	PLCnext Technology provides that users can be managed via the User Manager in the WBM, via LDAP, or via the Linux Configuration files. User are assigned to roles which have a predefined set of permissions. User Manager assigns roles and permissions to the session representing the user.	– Creating users in the PLCnext Technology - Security Info Center – User authentication in the main PLCnext Technology - Info Center – LDAP Configurationin the main PLCnext Technology - Info Center
CR 2.5	Session lock	SL1	PLCnext Technology provides that there is an implemented time limit of 20 minutes.	– Configuring authentication errors and sessions in the PLCnext Technology - Security Info Center – Authentication failure handling in the main PLCnext Technology - Info Center
CR 2.6	Remote session termination	SL2	PLCnext Technology provides that there is an implemented default timeout of 20 minutes. The duration can be set in the WBM.	– Configuring authentication errors and sessions in the PLCnext Technology - Security Info Center – Authentication failure handling in the main PLCnext Technology - Info Center
CR 2.7	Concurrent session control	SL3	PLCnext Technology provides that the User Manager provides configurable total number of sessions.	– Configuring authentication errors and sessions in the PLCnext Technology - Security Info Center
CR 2.8	Auditable events	SL1	PLCnext Technology provides a security logging to log all auditable events.	– Security logging in the PLCnext Technology - Security Info Center

No.	Description	Security Level	Fulfillment	Links
CR 2.9	Audit storage capacity	SL1	PLCnext Technology provides a security logging ensuring the audit storage capacity.	– Security logging in the PLCnext Technology - Security Info Center
CR 2.10	Response to audit processing failures	SL1	PLCnext Technology provides that there is an external logging system for checking and reporting local errors.	– Security logging in the PLCnext Technology - Security Info Center
CR 2.11	Timestamps	SL1	PLCnext Technology provides that Timestamp is available and can be set via PLCnext Engineer.	– Security logging in the PLCnext Technology - Security Info Center – System time in the main PLCnext Technology - Info Center
CR 2.11 RE1	Time synchronization	SL2	PLCnext Technology provides that you can set the system time using the PLCnext Engineer software.	– Configuring the system time in the PLCnext Technology - Security Info Center – System time in the main PLCnext Technology - Info Center
CR 2.12	Non-repudiation	SL1	PLCnext Technology provides a security logging to log all auditable actions and events.	– Security logging in the PLCnext Security Info Center – Configuring central logging in the PLCnext Technology - Security Info Center

FR3 – System integrity (SI)

No.	Description	Security Level	Fulfillment	Links
CR 3.1	Communication integrity	SL1	PLCnext Technology uses TLS for the communication channels (HTTPS, OPC UA, ...). TLS ensures the integrity and authenticity of the communication.	– Generating self-signed HTTPS certificates in the WBM in the PLCnext Technology - Security Info Center – Uploading the certificate in the browser in the PLCnext Technology - Security Info Center
CR 3.1 RE1	Communication authentication	SL2	PLCnext Technology uses TLS for the communication channels (HTTPS, OPC UA, ...). TLS ensures the integrity and authenticity of the communication.	– Generating self-signed HTTPS certificates in the WBM in the PLCnext Technology - Security Info Center – Uploading the certificate in the browser in the PLCnext Technology - Security Info Center
CR 3.3	Security functionality verification	SL1	PLCnext Technology provides various security measures and different verification interfaces that can be used to check the security settings by the system integrator or asset owner during production according to the needs of the system design. Security logging and central security logging are major interfaces that can be enhanced by additional checks.	– Periodic security maintenance activities in the PLCnext Technology - Security Info Center
CR 3.4	Software and information integrity	SL1	PLCnext Technology provides integrity of data in transition by using TLS. The User Management controls the access permission to the data in rest. Physical access to the controller must be protected by a lockable cabinet. External SD card must be disabled or encrypted.	– User authentication in the main PLCnext Technology - Info Center – PLCnext security hardening in the PLCnext Technology - Security Info Center – External SD card encryption is mandatory (see the PLCnext Technology - Security Info Center)

No.	Description	Security Level	Fulfillment	Links
CR 3.4 RE1	Authenticity of software and information	SL2	PLCnext Technology provides a User Management which grants authenticity for data access. Physical access is protect by the cabinet. External SD card must be disabled or encrypted. Only Users with valid credentials and permissions can access the device and change data. User actions are logged and wrong access attempts to the device are logged also.	– Creating users in the PLCnext Technology - Security Info Center – Security logging in the PLCnext Technology - Security Info Center – PLCnext security hardening in the PLCnext Technology - Security Info Center – External SD card encryptionis mandatory (see the PLCnext Technology - Security Info Center)
CR 3.5	Input validation	SL1	PLCnext Technology provides input validation on interfaces.	– PLCnext security hardening in the PLCnext Technology - Security Info Center
CR 3.6	Deterministic output	SL1	Deterministic outputs are configured in PLCnext Engineer using the so-called (substitution) behavior, which defines the default value for each output module in case of failure.	– Configuring PLCnext Engineer in the PLCnext Technology - Security Info Center
CR 3.7	Error handling	SL1	PLCnext Technology does not provide any information that could be exploited by adversaries to attack the device. Special permissions are required to read error messages. Unauthenticated users do not receive critical information.	– Creating usersin the PLCnext Technology - Security Info Center – Security loggingin the PLCnext Technology - Security Info Center
CR 3.8	Session integrity	SL2	PLCnext Technology authorization is performed by the User Manager, which creates secure sessions.	– Creating usersin the PLCnext Technology - Security Info Center – Security loggingin the PLCnext Technology - Security Info Center
CR 3.9	Protection of audit information	SL2	Only the PLCnext Technology roles SecurityAdmin and SecurityAuditor have the permission to read security loggings.	– Security logging in the PLCnext Technology - Security Info Center – Configuring central logging in the PLCnext Technology - Security Info Center

FR4 – Data confidentiality (DC)

No.	Description	Security Level	Fulfillment	Links
CR 4.1	Information confidentiality	SL1	PLCnext Technology provides integrity of data in transition by using TLS. The User Management controls the access permission to the data in rest. Physical access to the controller must be protected by a lockable cabinet. External SD card must be disabled or encrypted.	– PLCnext security hardening in the PLCnext Technology - Security Info Center – External SD card encryption is mandatory (see topic in the PLCnext Technology - Security Info Center)
CR 4.2	Information persistence	SL2	Reset 1 and reset 2 set back the device to factory defaults securely.	– Secure disposal in the PLCnext Technology - Security Info Center
CR 4.3	Use of cryptography	SL1	PLCnext Technology provides TLS for the communication channels (HTTPS, OPC UA, ...). The cryptography is based on openssl and offers state-of-the-art security mechanisms.	– PLCnext security hardening in the PLCnext Technology - Security Info Center

FR5 – Restricted data flow (RDF)

No.	Description	Security Level	Fulfillment	Links
CR 5.1	Network segmentation	SL1	PLCnext Technology provides separate Ethernet interfaces. Each controller may require different configuration options for network segmentation.	– AXC F 2152 in the PLCnext Technology - Security Info Center – AXC F 3152 in the PLCnext Technology - Security Info Center

FR6 – Timely response to events (TRE)

No.	Description	Security Level	Fulfillment	Links
CR 6.1	Audit log accessibility	SL1	PLCnext Technology provides a security logging to log all auditable actions and events.	– Security logging in the PLCnext Technology - Security Info Center
CR 6.1 RE1	Programmatic access to audit logs	SL3	PLCnext Technology provides a security logging to log all auditable actions and events and provides it to central logging server via syslog-ng.	– Security logging in the PLCnext Technology - Security Info Center – Configuring central logging in the PLCnext Technology - Security Info Center
CR 6.2	Continuous monitoring	SL2	PLCnext Technology provides a security logging to log all auditable actions and events and provides it to central logging server via syslog-ng.	– Security logging in the PLCnext Technology - Security Info Center – Configuring central logging in the PLCnext Technology - Security Info Center

FR7 – Resource availability (RA)

No.	Description	Security Level	Fulfillment	Links
CR 7.1	Denial of service protection	SL1	PLCnext Technology provides netload limiter, firewall (nf-tables) to control the communication load.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center – Netload Limiter in the main PLCnext Technology - Info Center
CR 7.1 RE1	Manage communication load from component	SL2	PLCnext Technology provides netload limiter, firewall (nf-tables) to control the communication load. The task management is designed to manage and recover from high communication load.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center – Netload Limiter in the main PLCnext Technology - Info Center
CR 7.2	Resource management	SL1	PLCnext Technology provides netload limiter, firewall (nf-tables) to control the communication load and resource management. In addition, the task management controls execution and resource load.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center – Netload Limiter in the main PLCnext Technology - Info Center
CR 7.3	Control system backup	SL1	PLCnext Technology provides an app to start a backup during normal operations. It generates a backup file which is managed by the Device and Update Management.	– Data Backup and Restore in the PLCnext Technology - Security Info Center – Perform backup and restore in the PLCnext Technology - Security Info Center – Backups via Device and Update Management in the main PLCnext Technology - Info Center
CR 7.3 RE1	Backup integrity verification	SL2	PLCnext Technology 's backup data is integrity protected. Before starting a restore the data integrity is validated.	– Data Backup and Restore in the PLCnext Technology - Security Info Center – Perform backup and restore in the PLCnext Technology - Security Info Center

No.	Description	Security Level	Fulfillment	Links
CR 7.4	Control system recovery and reconstitution	SL1	PLCnext Technology provides recovery after a disruption or failure. To recover a device based on the backup data, it must be set to delivery status by reset 1, configured according to the system configuration and Security Profile must be activated. The restore data is managed by the Device and Update Management.	– Data Backup and Restore in the PLCnext Technology - Security Info Center – Perform backup and restore in the PLCnext Technology - Security Info Center – Backups via Device and Update Management in the main PLCnext Technology - Info Center
CR 7.6	Network and security configuration settings	SL1	PLCnext Technology provides that the network and security configuration can be set via the WBM.	– Network configuration in the main PLCnext Technology - Info Center – Handling the Security Profile in the PLCnext Technology - Security Info Center
CR 7.7	Least functionality	SL1	PLCnext Technology provides that the Security Profile follows the principle of least functionality: only components that have been considered in the threat analysis may run. This specifies exactly what is permissible. This specifies exactly what is permissible.	– Handling the Security Profile in the PLCnext Technology - Security Info Center
CR 7.8	Control system component inventory	SL2	PLCnext Technology provides via OPC UA (device info) the component inventory information.	– Activating OPC UA Server in the PLCnext Technology - Security Info Center – Assets (see areas and functions, Device and Update Management in the main PLCnext Technology - Info Center)

Embedded device requirement (EDR)

No.	Description	Security Level	Fulfillment	Links
EDR 2.4	Mobile code	SL1	PLCnext Technology provides integrity of data in transition by using TLS. The User Management controls the access permission to the mobile code in rest. Physical access to the controller must be protected by a lockable cabinet. External SD card must be disabled or encrypted.	– PLCnext security hardening in the PLCnext Technology - Security Info Center – External SD card encryption is mandatory (see topic in the PLCnext Technology - Security Info Center)
EDR 2.4 RE1	Mobile code authenticity check	SL2	PLCnext Technology provides integrity of data in transition by using TLS. The User Management controls the access permission to the mobile code in rest. Physical access to the controller must be protected by a lockable cabinet. External SD card must be disabled or encrypted.	– PLCnext security hardening in the PLCnext Technology - Security Info Center – External SD card encryption is mandatory (see topic in the PLCnext Technology - Security Info Center)
EDR 2.13	Use of physical diagnostic and test interfaces	SL2	PLCnext Technology protects access to physical test and diagnostic interfaces through the housing. Interfaces cannot be accessed through the housing with testbed adapters. The device must be protected in a lockable cabinet. The device and SD card must be shipped in a secure manner.	– Protection against physical access in the PLCnext Technology - Security Info Center
EDR 3.2	Protection from malicious code	SL1	PLCnext Technology provides protection from malicious code by using TLS for data in transition. The User Management controls the access permission to the data in rest.	– PLCnext security hardening in the PLCnext Technology - Security Info Center
EDR 3.10	Support for updates	SL1	PLCnext Technology provides a WBM page to install updates. OPC UA Software Update is supported to integrate PLCnext Technology into the Device and Update Management Service.	– Firmware Updates in the main PLCnext Technology - Info Center – Activating Software Updates in the PLCnext Security Info Center – Update plans (Device and Update Management) in the main PLCnext Technology - Info Center – Update packages (Device and Update Management) in the main PLCnext Technology - Info Center

No.	Description	Security Level	Fulfillment	Links
EDR 3.10 RE1	Update authenticity and integrity	SL2	PLCnext Technology provides RAUC update containers signed with an X509.3 certificate from a product vendor. Before installation, the authenticity and integrity of the update is verified. All update files provided via the download center are verifiable with a SHA 256.	– Activating Software Updates in the PLCnext Technology - Security Info Center
EDR 3.11	Physical tamper resistance and detection	SL2	PLCnext Technology provides that the cabinet must be locked; application must supervise cabinet accesses.	– PLCnext security hardening in the PLCnext Technology - Security Info Center – Protection against physical access in the PLCnext Technology - Security Info Center
EDR 3.12	Provisioning product supplier roots of trust	SL2	PLCnext Technology provides a device identifier called IdevID. This device identity is installed during production and protected by the TPM. The boot integrity check validates the further trust roots such as firmware update.	– Certificate Authentication in the main PLCnext Technology - Info Center (Identity Store)
EDR 3.13	Provisioning asset owner roots of trust	SL2	PLCnext Technology provides the Certificate Authentication web page to install Asset Owner Roots of Trust via the Trust Store mechanism. Devices (SD cards) containing installed Asset Owner Roots of Trust must be specially protected in the field by locked cabinets in the field and must not be sent to other sites without special protection from physical access.	– Certificate Authentication in the main PLCnext Technology - Info Center (Trust Store) – SD card encryption in the PLCnext Technology - Security Info Center
EDR 3.14 [1]	Integrity of the boot process	SL1	PLCnext Technology provides a partial boot integrity check for the OS and FW prior starting the PLC function. The result is shown in the WBM and a notification in the security logging is generated.	– Checking the integrity state in the PLCnext Technology - Security Info Center
EDR 3.14 RE1 [1]	Authenticity of the boot process	SL2	PLCnext Technology provides a partial boot integrity check for the OS and FW based on the root of trust of the device.	– Checking the integrity state in the PLCnext Technology - Security Info Center

[1] *Check with the respective controllers how the feature is implemented.*

Network device requirement (NDR)

No.	Description	Security Level	Fulfillment	Links
NDR 1.13	Access via untrusted networks	SL1	PLCnext Technology provides separate Ethernet interfaces. Each controller may require different configuration options for network segmentation. By using the firewall, access via untrusted networks is managed.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center
NDR 1.13 RE1	Explicit access request approval	SL3	PLCnext Technology provides separate Ethernet interfaces. Each controller may require different configuration options for network segmentation. By using the firewall, access via untrusted networks is managed. The firewall is configured to reject output and input communication requests by default. Only explicitly configured communication requests are allowed.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center
NDR 5.2	Zone boundary protection	SL1	PLCnext Technology provides separate Ethernet interfaces. Each controller may require different configuration options for network segmentation. By using the netload limiter and firewall, zone boundary protection can be established.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center – AXC F 2152 in the PLCnext Technology - Security Info Center – AXC F 3152 in the PLCnext Technology - Security Info Center
NDR 5.2 RE1	Deny all, permit by exception	SL2	PLCnext Technology provides separate Ethernet interfaces. Each controller may require different configuration options for network segmentation. By using the firewall, access via untrusted networks is managed. The firewall is configured to reject output and input communication requests by default. Only explicitly configured communication requests are allowed.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center

No.	Description	Security Level	Fulfillment	Links
NDR 5.2 RE2	Island mode	SL3	PLCnext Technology provides separate Ethernet interfaces. Each controller may require different configuration options for network segmentation. By using the Netload Limiter and firewall, zone boundary protection can be established. The firewall can be configured for each Ethernet interface.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center
NDR 5.3	General purpose, person-to-person communication restrictions	SL1	PLCnext Technology provides firewall configurations to reject output and input communication requests by default. Only explicitly configured communication requests including dedicated ports as well as IP addresses are allowed.	– Configuring basic firewall settings in the PLCnext Technology - Security Info Center – Configuring extended firewall settings in the PLCnext Technology - Security Info Center – PLCnext security hardening in the PLCnext Technology - Security Info Center – Security measures in the PLCnext Technology - Security Info Center

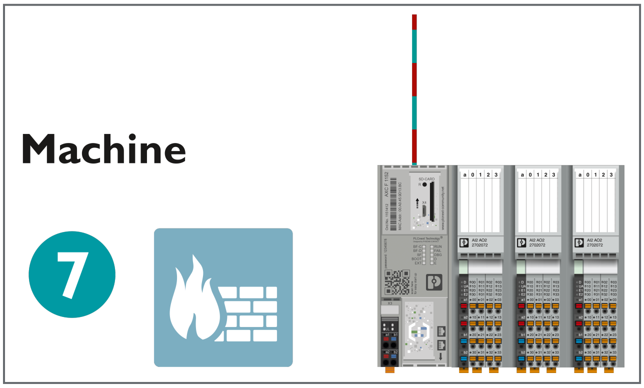
AXC F 1152

Note: For further information about the hardware, refer to the product documentation of this controller (item no. 1151412):

- User manual
- Product page

The AXC F 1152 is approved for certified security based on a limited scope. The AXC F 1152 does not support left-alignable modules and therefore network segmentation is not possible.

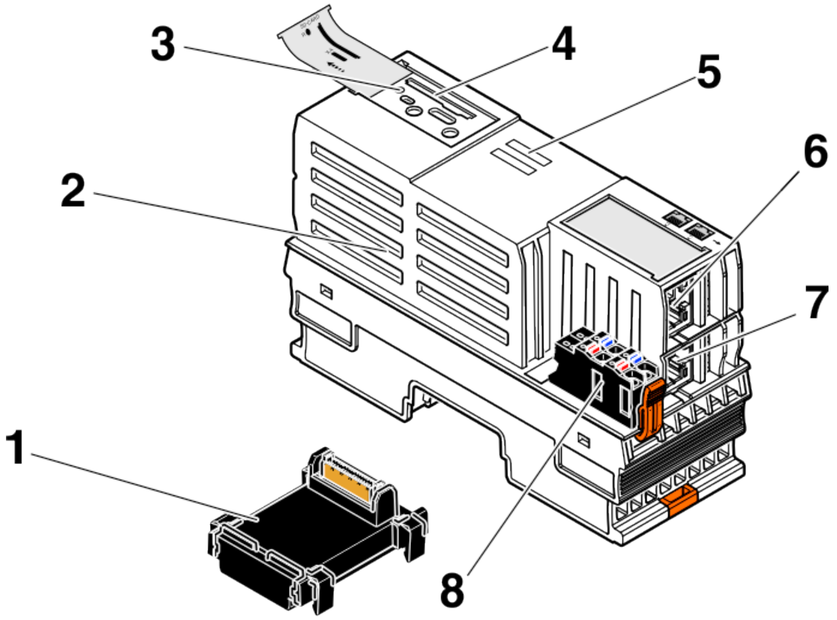
Since no network segmentation is possible, you can only use the AXC F 1152 as a stand-alone controller without subordinate networks.



For information on the security context, refer to the topic Generic Security Concept.

...continuation see next page...

Connecting and operating elements of the controller



The controller consists of the following components:

1	Bus base module
2	Electronics module
3	Reset button
4	SD card holder
5	Diagnostic and status indicators
6	Ethernet interface X2
7	Ethernet interface X1
8	Supply connector (connector for connecting the supply voltage (communications voltage U_L))

SD card

- Only use encrypted SD cards!

Information on this can be found in the topic SD card encryption.

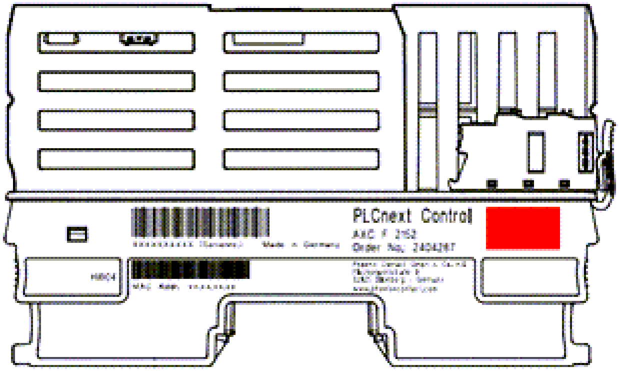
Security seals

In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the controller.

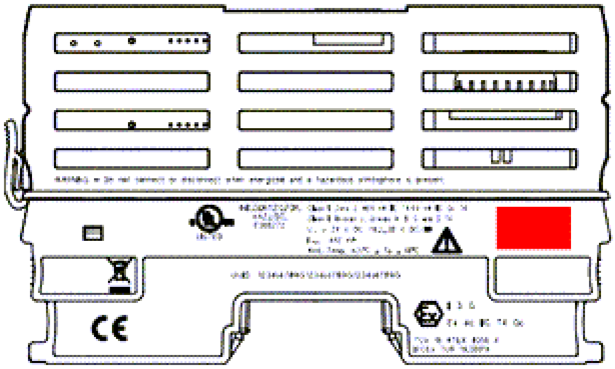
From production dates Q2/2022 and later, the housing of PLCnext Control AXC F 1152 is protected by a security seal on both sides like shown below.

These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the PLCnext Control can no longer be ensured.

- Check the delivery for transport damage. Damaged packaging is an indicator of potential damage to the device that may have occurred during transport. This could result in a malfunction.
- Do not open the housing. If the housing is opened, the function of the device can no longer be ensured.
- Check at regular intervals that none of the seals are damaged. If any of the seals are damaged or missing, it may be that the device has been tampered. In this case, contact Phoenix Contact without delay before using the device.



Example: AXC F 2152 viewed from the left side



Example: AXC F 2152 viewed from the right side

Assignment of the Ethernet interfaces

The following is an overview of how the Ethernet interfaces are assigned on the various pages in the WBM:

Ethernet interface hardware	Ethernet interface WBM - Network page	Ethernet interfaces WBM - Firewall page
X2	**TCP/IP (LAN1) - Switched Mode** (see Assigning IP addresses)	**eth0** (see Configuring extended firewall settings)
X1	**TCP/IP (LAN1) - Switched Mode** (see Assigning IP addresses)	**eth0** (see Configuring extended firewall settings)

How to reset the controller

Reset 1

Resetting the controller to default setting type 1 deletes all settings that you have configured. These include, for example:

- The PLCnext Engineer project, including all applications that have been programmed in accordance with IEC 61131-3
- All applications that were programmed using high-level languages
- The configured bus configuration
- The network configuration of the controller
- Changes and extensions that you have made to the operating system or to the firmware

To reset the controller to default setting type 1, proceed as follows:

- Switch off the supply voltage of the controller.
- After the LEDs have gone out, press the reset button.
- Hold the reset button down and switch the supply voltage on.
  The RUN and FAIL LEDs light up.
- Release the reset button.

The controller is reset to default setting type 1.

Reset 2

Resetting to default setting type 2 resets the controller to the delivery state. This deletes all settings that you have configured.

To reset the controller to default setting type 2, proceed as follows:

- Switch off the supply voltage of the controller.
- After the LEDs have gone out, press the reset button.
- Hold the reset button down and switch the supply voltage on.
  The RUN and FAIL LEDs light up.
- Press and hold the Reset button down (approx. 30 s) until all LEDs (except the E and D LEDs) light up.
- Release the reset button.

The controller is reset to default setting type 2.

Netload Limiter configuration

You configure the Netload Limiter on the **Netload Limiter** page in the WBM (**Configuration** → **Network** , **Netload Limiter** tab).

Fur further information, refer to the topic Configuring Netload Limiter.

Controller-specific information on the 62443-4-2 compliance list

Note: Please note the additional controller-specific information on the 62443-4-2 compliance list.

AXC F 2152

Note: For further information about the controller (item no. 2404267), refer to the respective product documentation:

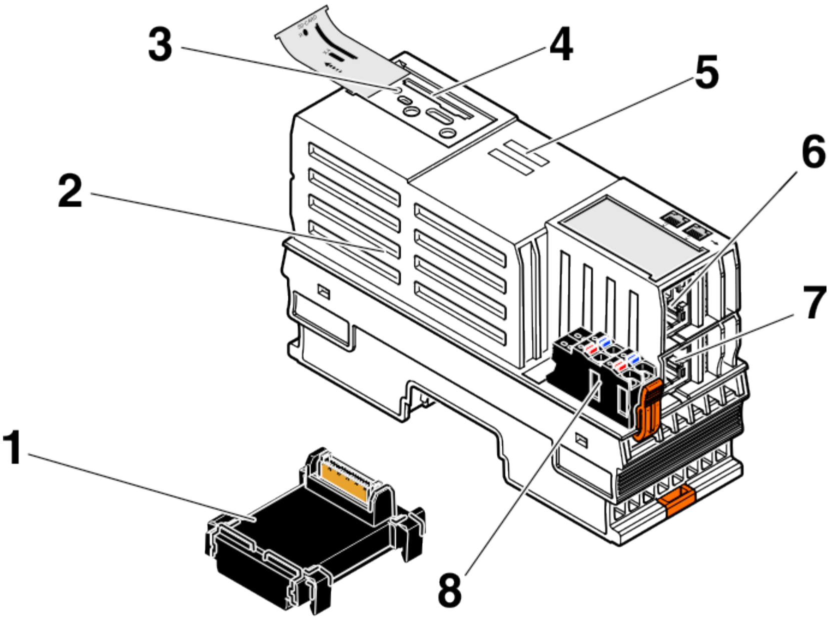
- User manual
- Product page AXC F 2152

For further information about the left-alignable Ethernet module (item no. 2403115), refer to the respective product documentation:

- Data sheet
- Product page AXC F XT ETH 1TX

The Security Profile must be activated, the left-alignable Ethernet module must be installed and the corresponding bus base module must be used.

Connecting and operating elements of the controller



The controller consists of the following components:

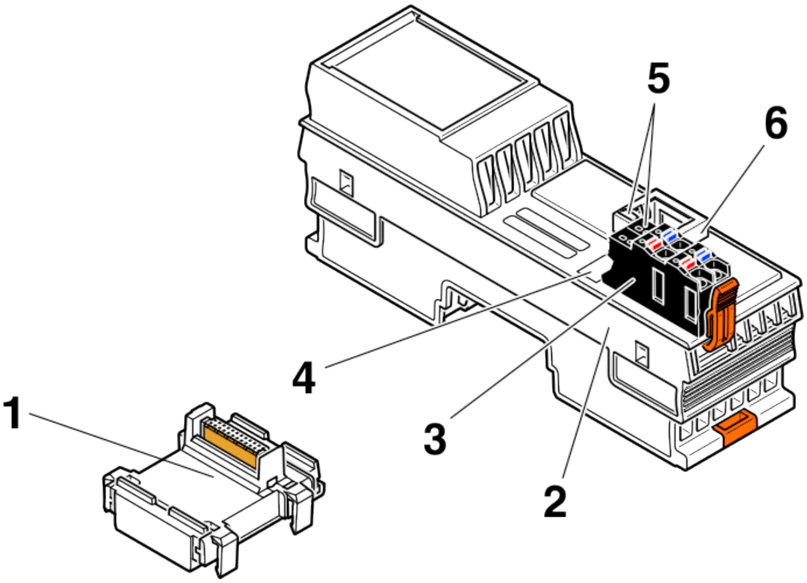
1 Bus base module
Note: To be able to use the AXC F 2152 with the extension module AXC F XT ETH 1TX, you need the bus base module AXC BS L 2, item no. 1064312.
2 Electronics module
3 Reset button
4 SD card holder
5 Diagnostic and status indicators
6 Ethernet interface X2
7 Ethernet interface X1
8 Supply connector (connector for connecting the supply voltage (communications voltage U_L))

SD card

- Only use encrypted SD cards!

Information on this can be found in the topic SD card encryption.

Components of the left-alignable Ethernet module



The left-alignable Ethernet module consists of the following components:

1	Bus base module
2	Electronics module
3	Supply connector
4	Function identification
5	Diagnostic and status indicators
6	Ethernet interface

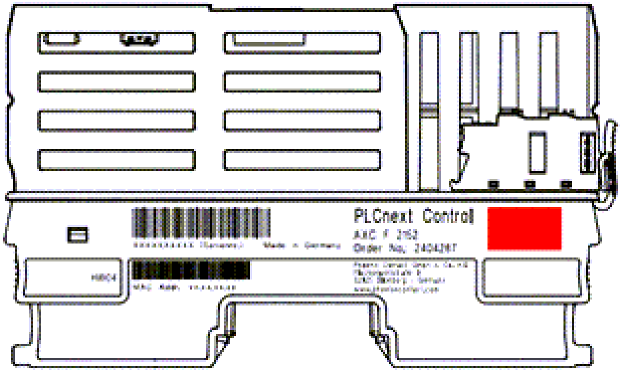
Security seals

In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the controller.

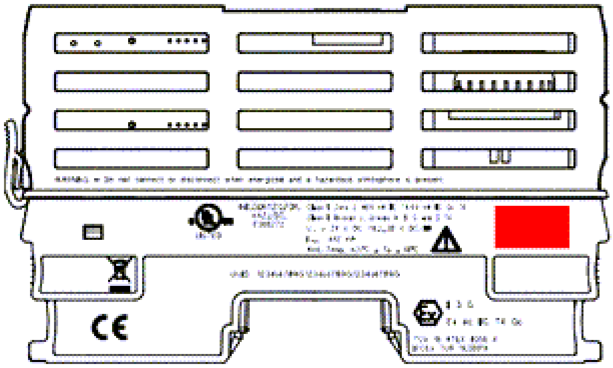
From production dates Q2/2022 and later, the housing of PLCnext Control AXC F 2152 is protected by a security seal on both sides like shown below.

These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the PLCnext Control can no longer be ensured.

- Check the delivery for transport damage. Damaged packaging is an indicator of potential damage to the device that may have occurred during transport. This could result in a malfunction.
- Do not open the housing. If the housing is opened, the function of the device can no longer be ensured.
- Check at regular intervals that none of the seals are damaged. If any of the seals are damaged or missing, it may be that the device has been tampered. In this case, contact Phoenix Contact without delay before using the device.



Example: AXC F 2152 viewed from the left side



AXC F 2152 viewed from the right side

Assignment of the Ethernet interfaces

The following is an overview of how the Ethernet interfaces are assigned on the various pages in the WBM:

Ethernet interface hardware	Ethernet interface WBM - Network page	Ethernet interfaces WBM - Firewall page
AXC F 2152: X2	**TCP/IP (LAN1) - Switched Mode** (see Assigning IP addresses)	**eth0** (see Configuring extended firewall settings)
AXC F 2152: X1	**TCP/IP (LAN1) - Switched Mode** (see Assigning IP addresses)	**eth0** (see Configuring extended firewall settings)
AXC F XT ETH 1TX (left-alignable Ethernet module)	**TCP/IP (EXT LAN 1)** (see Assigning IP addresses)	**enp1s0** (see Configuring extended firewall settings)

Activating PROFINET

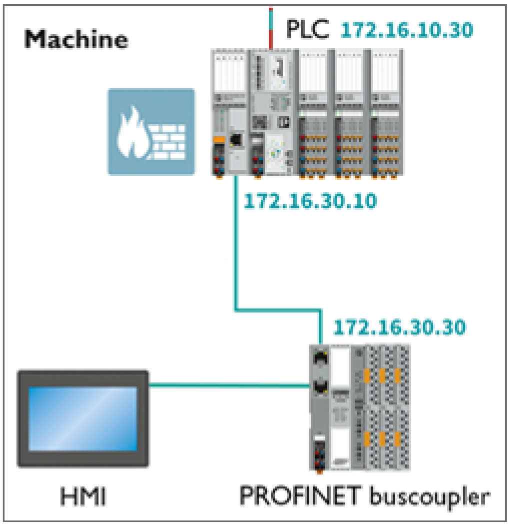
After you have performed a threat analysis and implemented appropriate protective measures from the security context, you can activate PROFINET.

ℹ For information on how to activate PROFINET, refer to the topic Activating PROFINET in this PLCnext Technology - Security Info Center.

ℹ For further information on PROFINET in the WBM, refer to the PROFINET diagnostics topic in the main PLCnext Technology - Info Center.

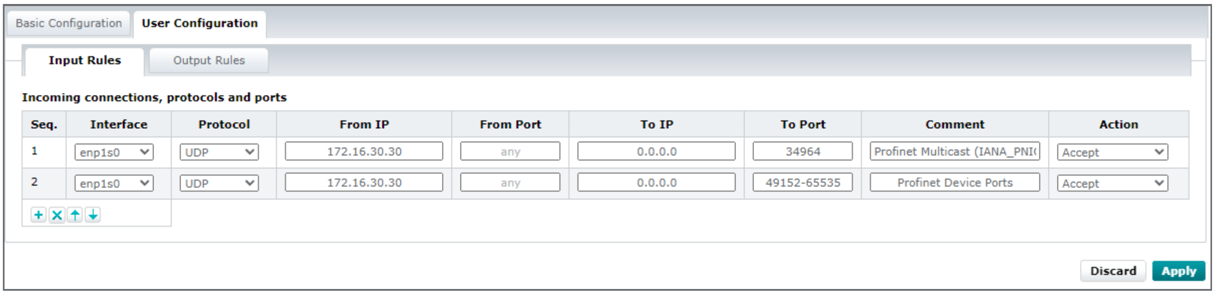
Using PROFINET

PROFINET is always operated on the extension module, while PLCnext Control is responsible for network segmentation. This results in the following architecture:



Accordingly, you need to adjust the firewall configurations (for more information, refer to the firewall basic configurations):

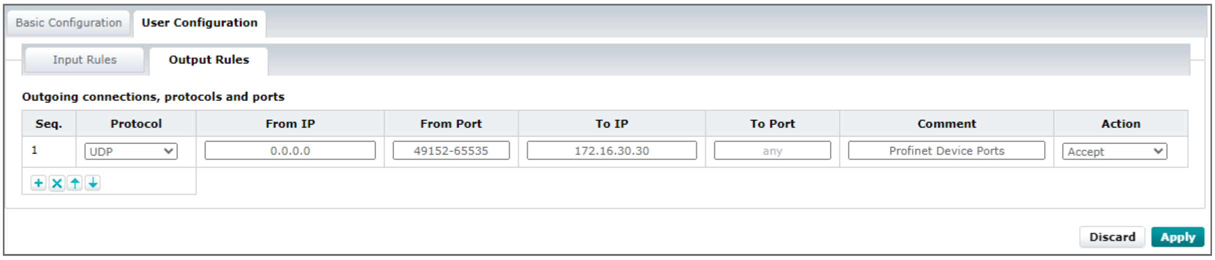
Input rules:



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	enp1s0	UDP	172.16.30.30	any	0.0.0.0	34964	Profinet Multicast (IANA_PNI(	Accept
2	enp1s0	UDP	172.16.30.30	any	0.0.0.0	49152-65535	Profinet Device Ports	Accept

Output rules:



Outgoing connections, protocols and ports

Seq.	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	UDP	0.0.0.0	49152-65535	172.16.30.30	any	Profinet Device Ports	Accept

How to reset the controller

Reset 1

Resetting the controller to default setting type 1 deletes all settings that you have configured. These include, for example:

– The PLCnext Engineer project, including all applications that have been programmed in accordance with IEC 61131-3
– All applications that were programmed using high-level languages
– The configured bus configuration
– The network configuration of the controller
– Changes and extensions that you have made to the operating system or to the firmware

To reset the controller to default setting type 1, proceed as follows:

- Switch off the supply voltage of the controller.
- After the LEDs have gone out, press the reset button.
- Hold the reset button down and switch the supply voltage on.
  The RUN and FAIL LEDs light up.
- Release the reset button.

The controller is reset to default setting type 1.

Reset 2

Resetting to default setting type 2 resets the controller to the delivery state. This deletes all settings that you have configured.

To reset the controller to default setting type 2, proceed as follows:

- Switch off the supply voltage of the controller.
- After the LEDs have gone out, press the reset button.
- Hold the reset button down and switch the supply voltage on.
  The RUN and FAIL LEDs light up.
- Press and hold the Reset button down (approx. 30 s) until all LEDs (except the E and D LEDs) light up.
- Release the reset button.

The controller is reset to default setting type 2.

Netload Limiter configuration

You configure the Netload Limiter on the **Netload Limiter** page in the WBM (**Configuration** → **Network**, **Netload Limiter** tab).

The Netload Limiter must be configured on the interface of the left-alignable Ethernet module (**TCP/IP (EXT LAN 1)**).

For further information, refer to the topic Configuring Netload Limiter.

Controller-specific information on the 62443-4-2 compliance list

Note: Please note the additional controller-specific information on the 62443-4-2 compliance list.

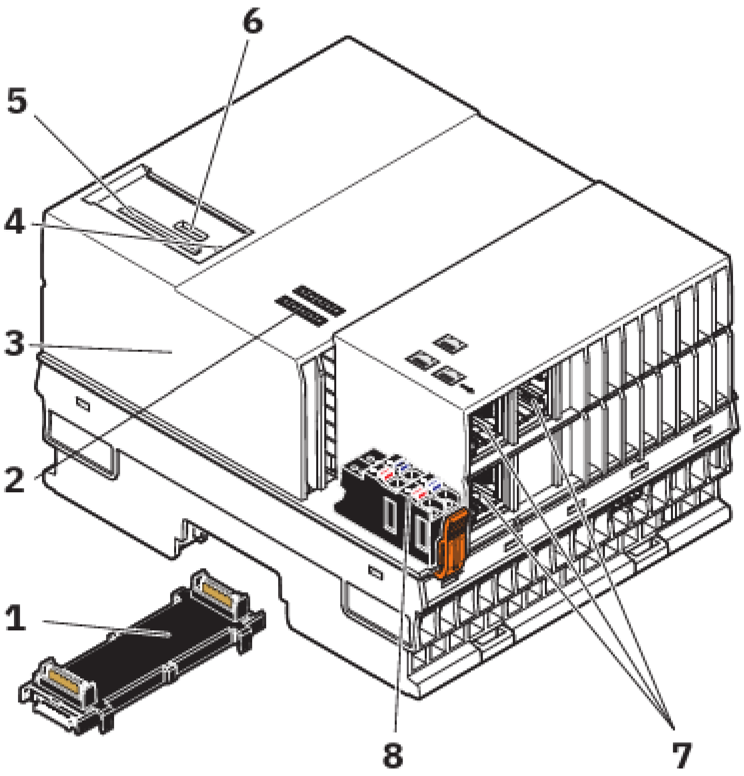
AXC F 3152

Note: For further information about the hardware, refer to the product documentation of this controller (item no. 1069208):

- User manual
- Product page

There are different Ethernet and firewall configurations due to three Ethernet interfaces.

Connecting and operating elements



The controller consists of the following components:

1 Bus base module
2 Diagnostic and status indicators
3 Electronics module
4 Reset button
5 SD card holder
6 Service interface (X4)
7 Ethernet interfaces (X1, X2, X3)
8 Supply connector (connector for connecting the supply voltage (communications voltage U_L))

SD card

- Only use encrypted SD cards!

Information on this can be found in the topic SD card encryption.

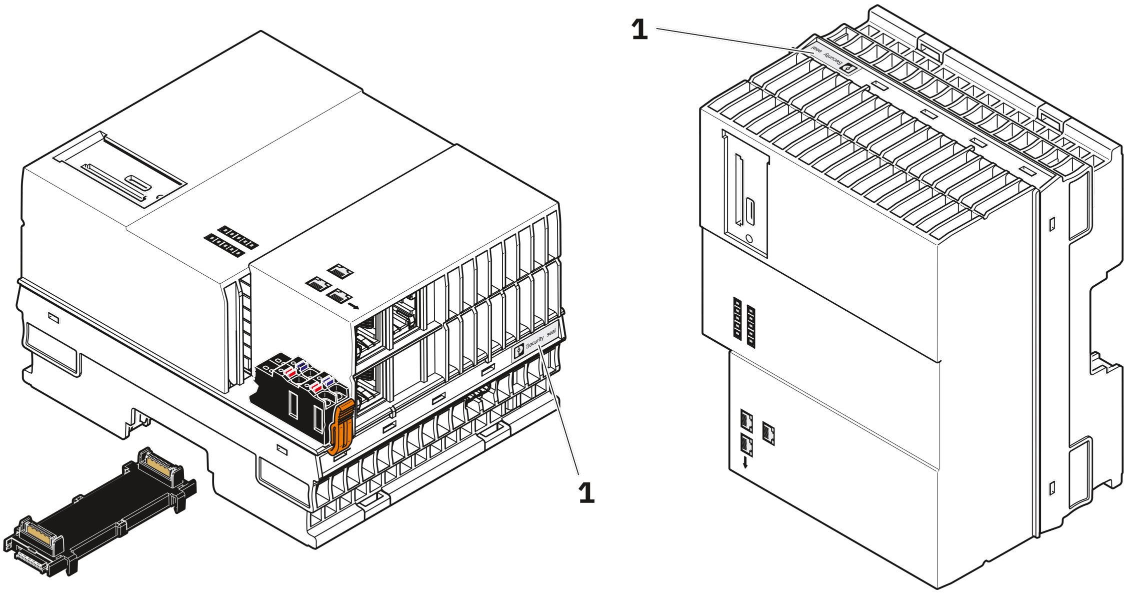
Security seals

In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the controller.

From hardware revision 04, the housing of PLCnext Control AXC F 3152 is protected by security seals like shown below.

These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the PLCnext Control can no longer be ensured.

- Check the delivery for transport damage. Damaged packaging is an indicator of potential damage to the device that may have occurred during transport. This could result in a malfunction.
- Do not open the housing. If the housing is opened, the function of the device can no longer be ensured.
- Check at regular intervals that none of the seals are damaged. If any of the seals are damaged or missing, it may be that the device has been tampered. In this case, contact Phoenix Contact without delay before using the device.



1 Security seals

Checking the device identity

PLCnext Control uses Trusted Platform Modules (TPM) to ensure the device identity. During production, a unique Device Certificate (IDevID) is installed on each device and stored in the TPM. To check the device identity, please check the device certificate and follow the certificate chain to the Phoenix Contact root certificate. Depending on the controller model or hardware revisions, PLCnext Control devices use different types of TPMs.

Latest AXC F 3152 hardware revisions are containing the Infineon Trusted Platform Module 2.0 SLB 9673 (firmware 26.13). The compliance with FIPS 140-2 physical level 3 is confirmed by NIST CMVP certificate #4467.

Activating PROFINET

After you have performed a threat analysis and implemented appropriate protective measures from the security context, you can activate PROFINET.

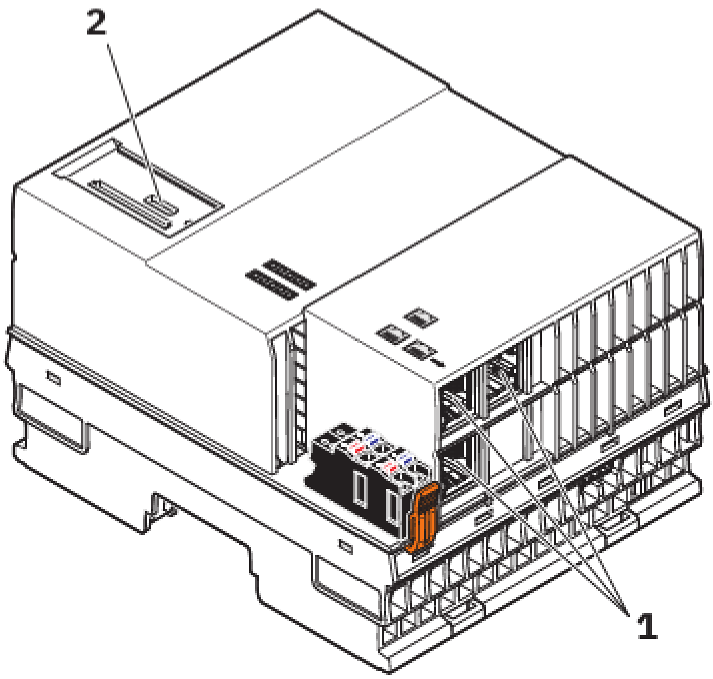
ℹ For information on how to activate PROFINET, refer to the topic Activating PROFINET in this PLCnext Technology - Security Info Center.

ℹ For further information on PROFINET in the WBM, refer to the PROFINET diagnostics topic in the main PLCnext Technology - Info Center.

Using PROFINET

Communication paths

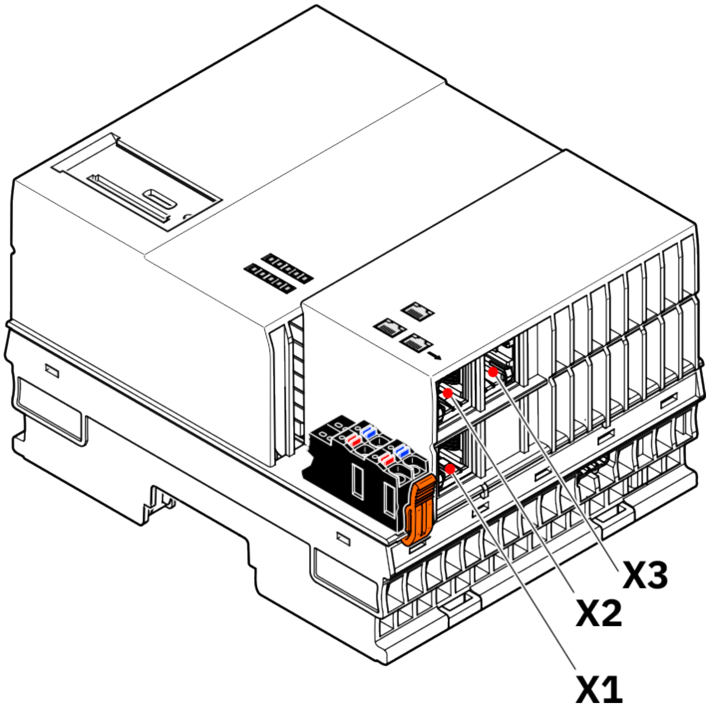
The controller consists of these communication paths:



1	3 x Ethernet	X1/X2/X3: 10/100/1000 BASE-T(X) X2: PROFINET controller interface X3: PROFINET device interface
2	Service interface	For service purposes, you can connect a PC to the service interface (USB-C interface). In this case, the service interface is used as an Ethernet interface (default IP address: 128.0.0.1/30). Use as a USB host interface is not possible. **Note:** The service interface is deactivated by default. Perform a threat analysis before activating the service interface! The procedure for commissioning the service interface can be found in the topic Starting up the service interface of the AXC F 3152 in the main PLCnext Technology - Info Center. Only operate the service interface within the protected network! The service interface must be secured via the firewall (as described below)!

Ethernet interfaces

The Ethernet interfaces are assigned as follows:



Assignment of the Ethernet interfaces

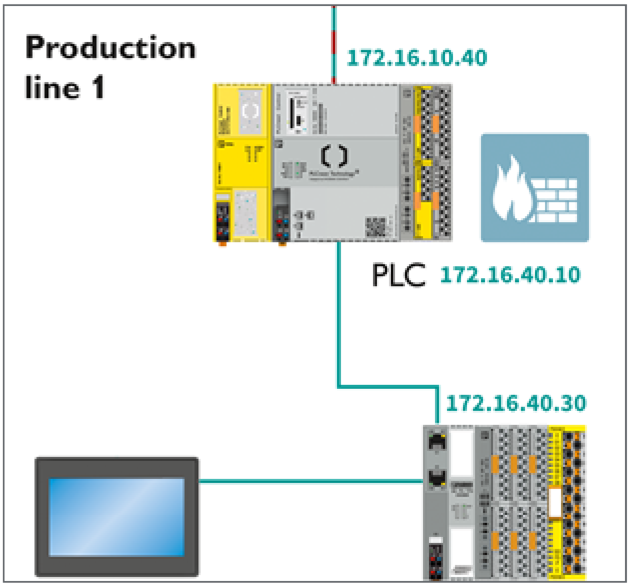
The following is an overview of how the Ethernet interfaces are assigned on the various pages in the WBM:

Ethernet interface hardware	Ethernet interface WBM - Network page	Ethernet interfaces WBM - Firewall page
X1	TCP/IP (LAN1)	LAN1
X2	TCP/IP (LAN2)	LAN2
X3	TCP/IP (LAN3)	LAN3

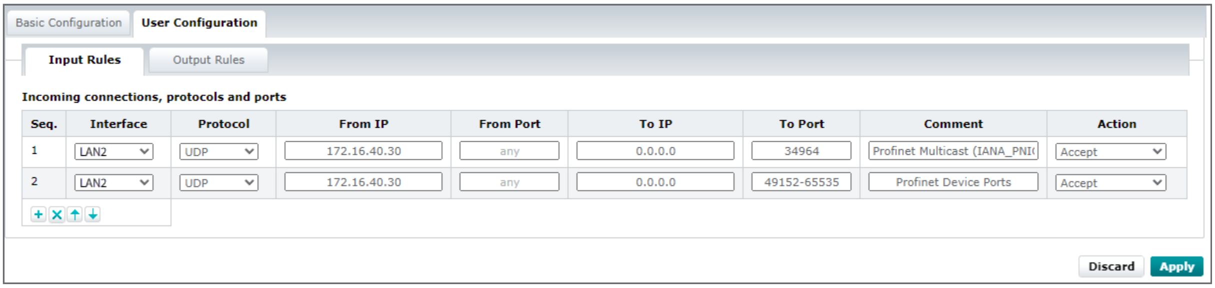
...continuation see next page...

Firewall configurations

You need to adjust the firewall configurations (for more information, refer to the firewall basic configurations):



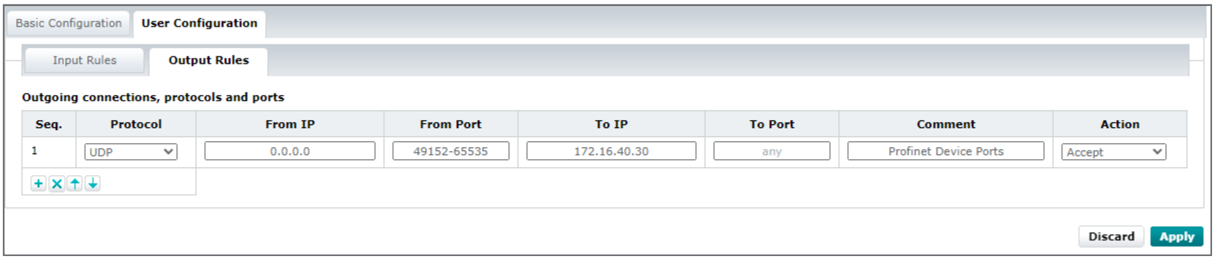
Input rules:



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	LAN2	UDP	172.16.40.30	any	0.0.0.0	34964	Profinet Multicast (IANA_PNI(	Accept
2	LAN2	UDP	172.16.40.30	any	0.0.0.0	49152-65535	Profinet Device Ports	Accept

Output rules:



Outgoing connections, protocols and ports

Seq.	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	UDP	0.0.0.0	49152-65535	172.16.40.30	any	Profinet Device Ports	Accept

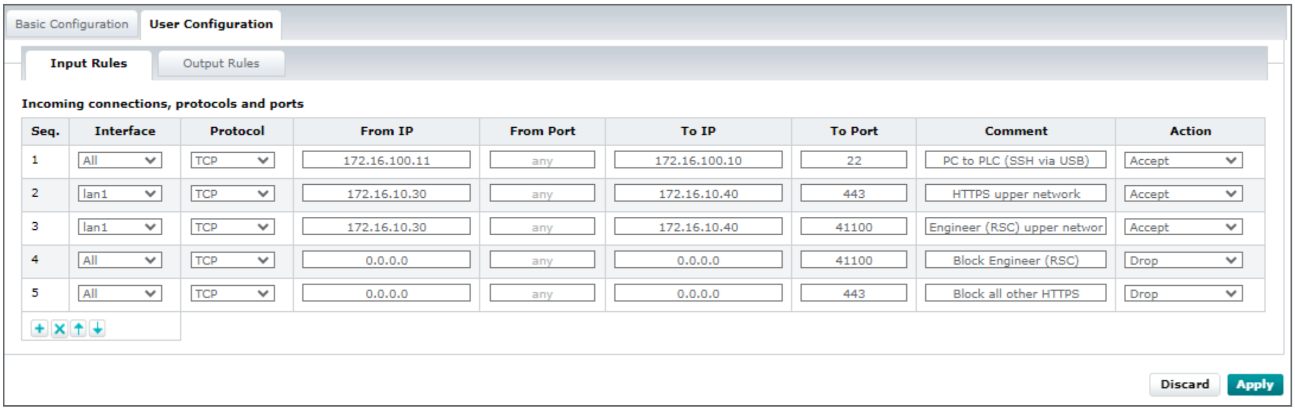
Using the service interface (USB)

- Perform a threat analysis before activating the service interface.

You should only use an SSH connection during commissioning, not during operation of a system.

> **Note:** You must always explicitly deactivate the service interface. It is not deactivated by a reset 1/reset 2 or activating the Security Profile. Once activated, the service interface will otherwise always remain on.

Here is an example of the firewall settings you need to make when using the service interface (see comments in the following screenshot):



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	All	TCP	172.16.100.11	any	172.16.100.10	22	PC to PLC (SSH via USB)	Accept
2	lan1	TCP	172.16.10.30	any	172.16.10.40	443	HTTPS upper network	Accept
3	lan1	TCP	172.16.10.30	any	172.16.10.40	41100	Engineer (RSC) upper networ	Accept
4	All	TCP	0.0.0.0	any	0.0.0.0	41100	Block Engineer (RSC)	Drop
5	All	TCP	0.0.0.0	any	0.0.0.0	443	Block all other HTTPS	Drop

...continuation see next page...

How to reset the controller

Reset 1

Resetting the controller to default setting type 1 deletes all settings that you have configured. These include, for example:

- The PLCnext Engineer project, including all applications that have been programmed in accordance with IEC 61131-3
- All applications that were programmed using high-level languages
- The configured bus configuration
- The network configuration of the controller
- Changes and extensions that you have made to the operating system or to the firmware

To reset the controller to default setting type 1, proceed as follows:

- Switch off the supply voltage of the controller.
- After the LEDs have gone out, press the reset button.
- Hold the reset button down and switch the supply voltage on.
  The RUN and FAIL LEDs light up.
- Release the reset button.

The controller is reset to default setting type 1.

Reset 2

Resetting to default setting type 2 resets the controller to the delivery state. This deletes all settings that you have configured.

To reset the controller to default setting type 2, proceed as follows:

- Switch off the supply voltage of the controller.
- After the LEDs have gone out, press the reset button.
- Hold the reset button down and switch the supply voltage on.
  The RUN and FAIL LEDs light up.
- Press and hold the Reset button down (approx. 30 s) until all LEDs (except the E and D LEDs) light up.
- Release the reset button.

The controller is reset to default setting type 2.

Netload Limiter configuration

You configure the Netload Limiter on the **Netload Limiter** page in the WBM (**Configuration** → **Network** , **Netload Limiter** tab).

The Netload Limiter must be activated on the interface x1 (LAN 1).

For further information, refer to the topic Configuring Netload Limiter.

Controller-specific information on the 62443-4-2 compliance list

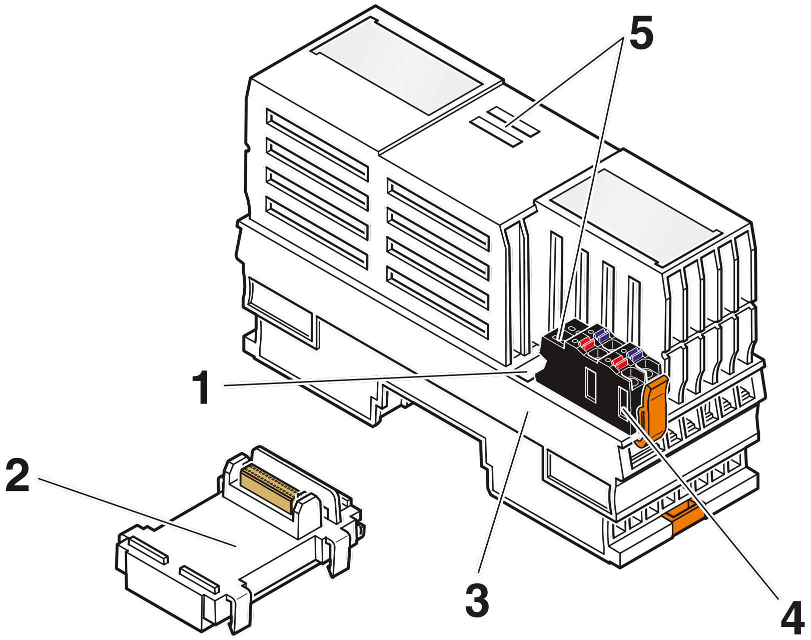
Note: Please note the additional controller-specific information on the 62443-4-2 compliance list.

AXC F XT SPLC 1000 (SPLC 1000)

Note: For further information about the hardware, refer to the product documentation of this controller (item no. 1159811):

- User manual
- Product page

Connecting and operating elements



The controller consists of the following components:

1 Function identification

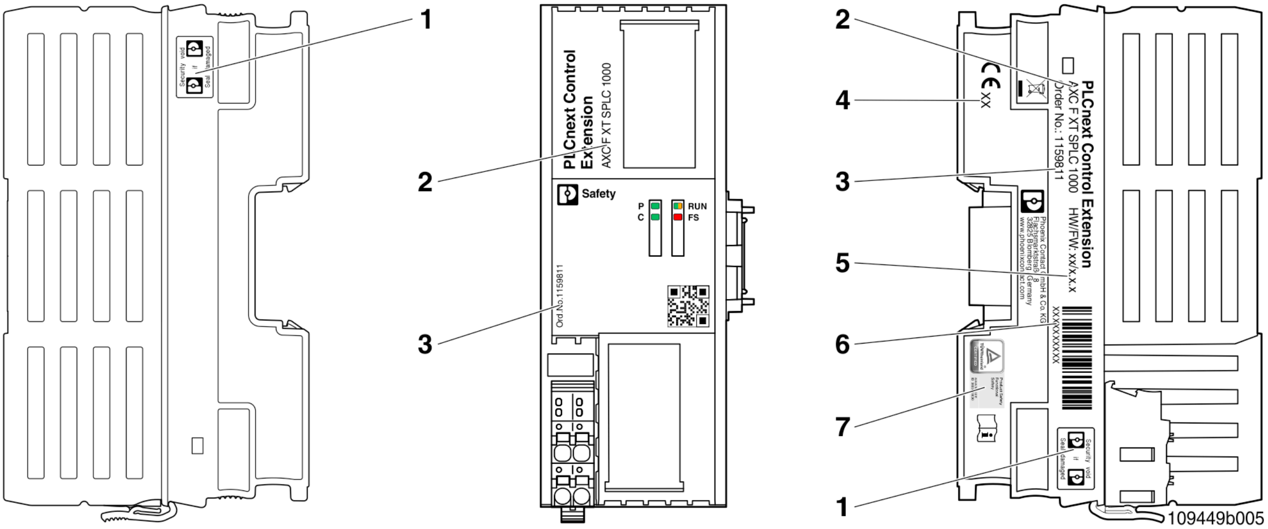
2 Bus base module

3 Electronics module

4 Supply connector (connector for connecting the supply voltage (communications voltage UL, 24 V DC))

5 Diagnostics and status indicators

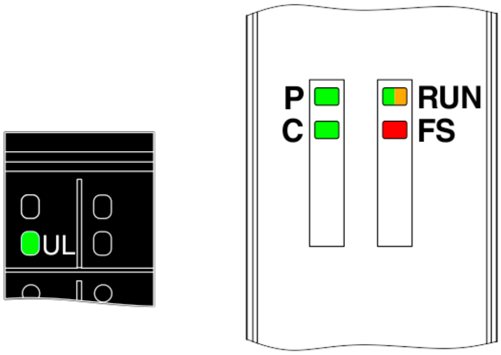
Printing and test mark


1
2
3
PLCnext Control Extension
AXC F XT SPLC 1000
Safety
P
C
RUN
FS
Ord.No.1159811
Security void if seal damaged
2
4
3
5
6
7
1
PLCnext Control Extension
AXC F XT SPLC 1000 HW/FW: xx/x.x.x
Order No.: 1159811
CE xx
Phoenix Contact GmbH & Co. KG
32825 Blomberg Germany
www.phoenixcontact.com
XXXXXXXXXX
109449b005

SPLC 1000 printing, including test mark:

1 Security seals
2 Item designation
3 Item number
4 Year of manufacture
5 Revision versions (HW/FW)
6 Serial number
7 Test mark

Diagnostics and status indicators



LED	Color	Meaning	Status	Description
FS	-	Failure State: Safe state of the SPLC 1000	Off	– Error-free operating state of the SPLC 1000 with supply voltage present. – A Failure State is not present.
	Red		Flashing (1 Hz)	– The SPLC 1000 is in the Failure State due to a configuration error in the PLCnext Engineer software. – The SPLC 1000 has switched to the safe state (Failure State). – The SPLC 1000 can be accessed from PLCnext Engineer online. **Remedy:** ● Remedy the configuration error in PLCnext Engineer. ● Download the standard project to the standard controller used. ● Download the safety project to the SPLC 1000.
			On	– A critical error in the SPLC 1000 hardware has occurred and been detected. – The SPLC 1000 has switched to the safe state (Failure State). **Remedy:** Perform a voltage reset: ● Switch off the supply voltage of the SPLC 1000 and the standard controller for at least 30 seconds and then switch it back on again (Power UP). Or restart the standard controller in the PLCnext Engineer software: ● Click the "Reboot the controller" button in the PLCnext Control "Cockpit" editor.

SD card

- Only use encrypted SD cards!

Information on this can be found in the topic SD card encryption.

Controller-specific information on the 62443-4-2 compliance list

Note: Please note the additional controller-specific information on the 62443-4-2 compliance list.

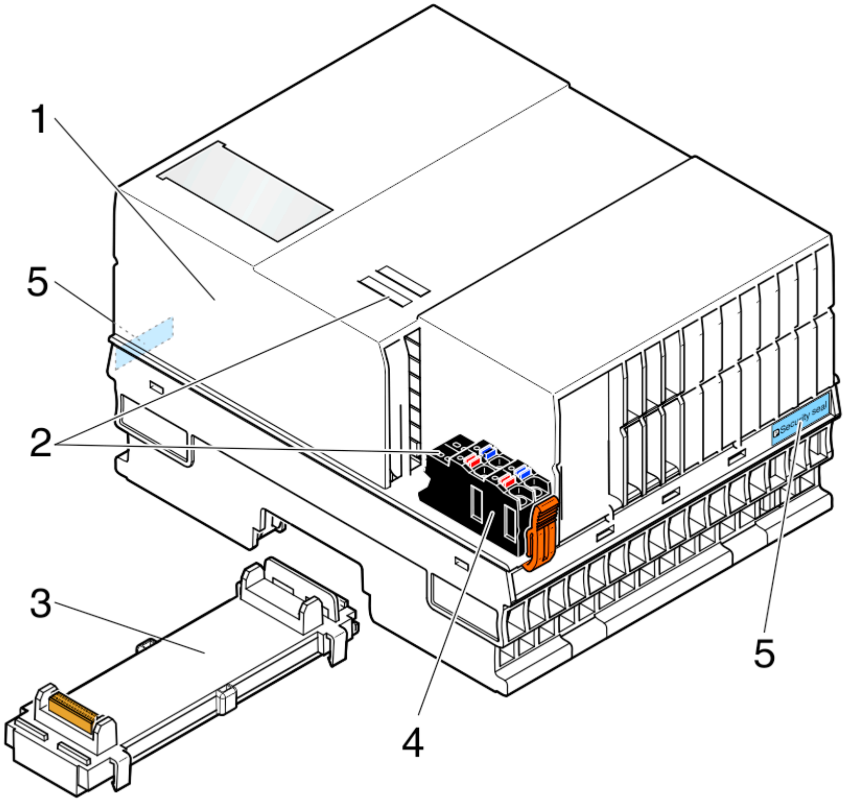
AXC F XT SPLC 3000 (SPLC 3000)

Note: The AXC F XT SPLC 3000 (SPLC 3000, item no. 1160157) is developed in compliance with the IEC 62443-4-1 process and meets the requirements of IEC 62443-4-2, as detailed in the security and safety hardening guidelines.

Officially, the SPLC 3000 will be included in the forthcoming IACS Components PLCnext Control certificate for firmware 2025.0 LTS.

You can find the Functional Safety Certificate here: Functional Safety certificates

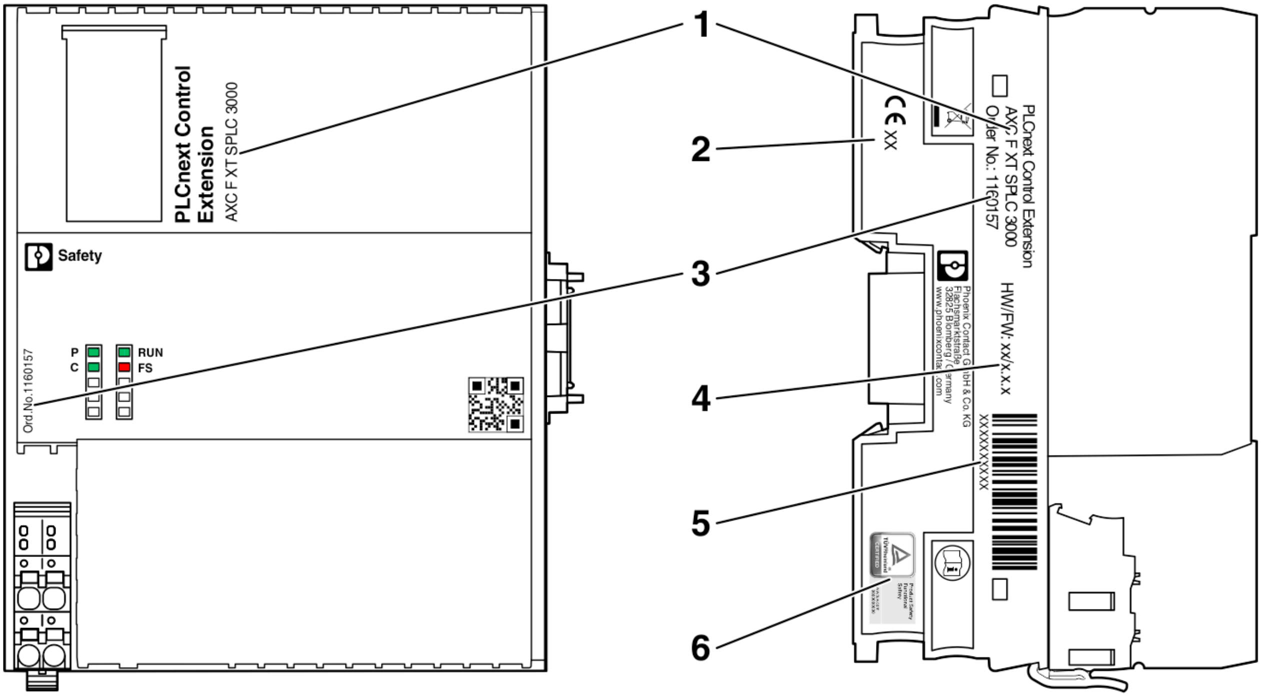
Connecting and operating elements



The controller consists of the following components:

1 Electronics module
2 Diagnostics and status indicators
3 Bus base module
4 Supply connector (connector for connecting the supply voltage (communications voltage UL, 24 V DC))
5 Security seals

Printing and test mark



SPLC 3000 printing, including test mark:

1 Item designation
2 Year of manufacture
3 Item number
4 Revision versions (HW/FW)
5 Serial number
6 Test mark

> **Note:** For further information about the hardware, refer to the product documentation of this controller (item no. 1160157):
>
> – User manual
> – Product page

SD card

- Only use encrypted SD cards!

Information on this can be found in the topic SD card encryption.

Controller-specific information on the 62443-4-2 compliance list

> **Note:** Please note the additional controller-specific information on the 62443-4-2 compliance list.

RFC 4072S

Note: For further information about the hardware, refer to the product documentation of this controller (item no. 1051328):

- User manual
- Product page

NOTICE

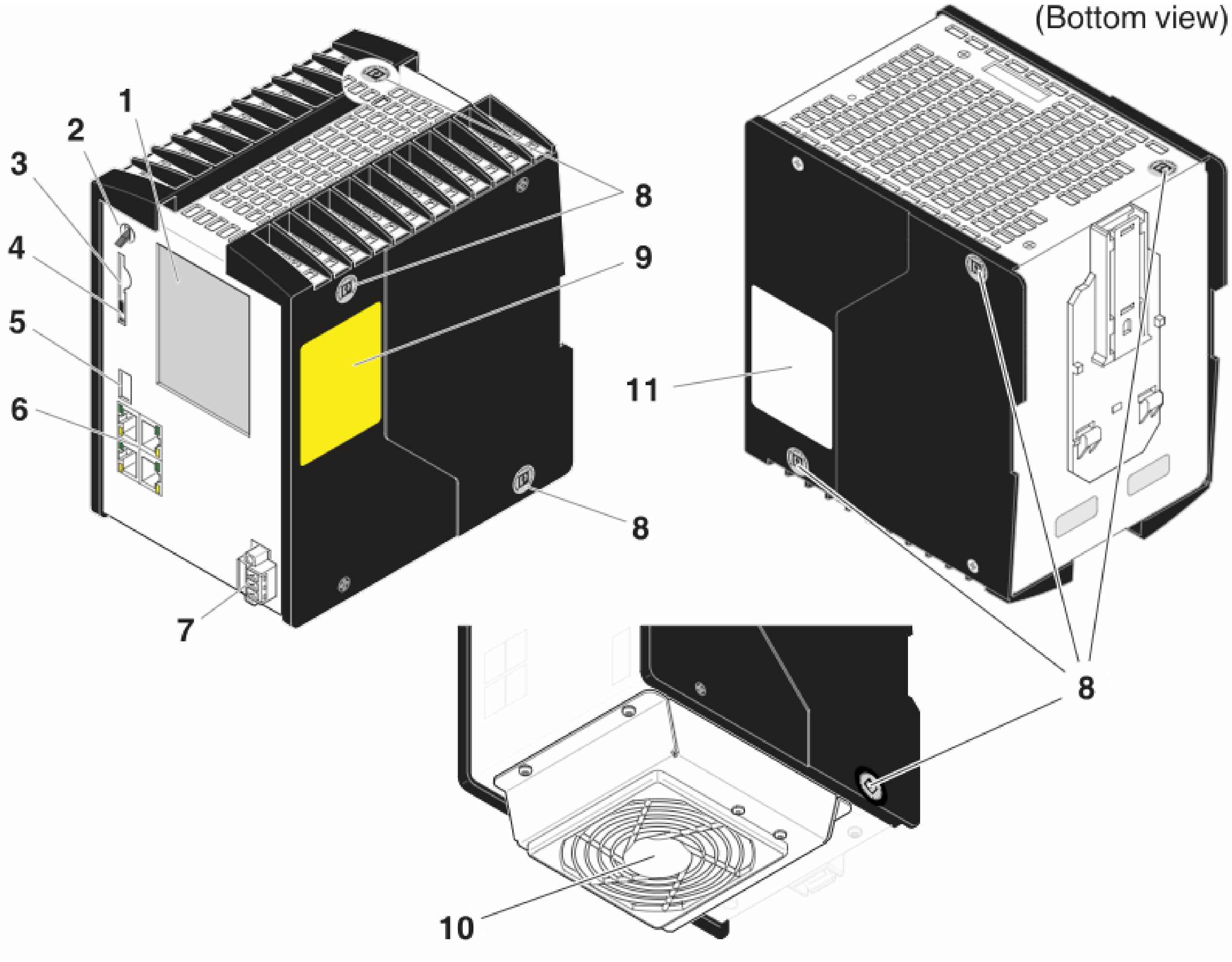
Risk of unauthorized access to devices

The safety controller RFC 4072S has a touch screen display and is used with an external SD card. This makes unencrypted information available. To prevent damage, data corruption, loss of data, or misuse of data due to authorized access, make sure that only authorized access is possible.

- Protect the interfaces by installing the devices in a control cabinet.
- Secure the control cabinet with a lock.
- Make sure that only authorized persons have access to the control cabinet key.
- Run cables in such a way that they are protected against unauthorized access.

There are different Ethernet and firewall configurations due to three Ethernet interfaces.

Connecting and operating elements



The controller consists of the following components:

1 Touch screen display
2 Mode selector switch
3 Slot for the parameterization memory/card holder (SD card)
4 Ejector for the parameterization memory
5 USB interface (type A USB 3.0 socket;
currently not supported)
6 Ethernet interfaces (RJ45 sockets)
7 Connection for external supply voltage (24 V DC)
8 Security seals
9 Test marks and revision status (hardware/firmware of iSPNS 3000)
10 Fan module (optional)
11 Label showing:
- Revision status (hardware/firmware) of the standard controller
- MAC addresses
- Serial number of the device
- Default password for `admin` user authentication

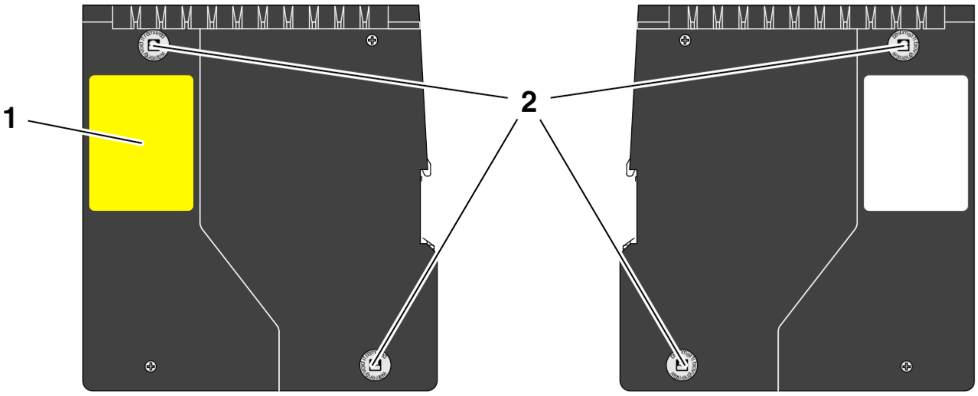
Security seals

In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the controller.

The housing of safety controller RFC 4072S is protected by security seals on both sides like shown below.

These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the PLCnext Control can no longer be ensured.

- Check the delivery for transport damage. Damaged packaging is an indicator of potential damage to the device that may have occurred during transport. This could result in a malfunction.
- Do not open the housing. If the housing is opened, the function of the device can no longer be ensured.
- Check at regular intervals that none of the seals are damaged. If any of the seals are damaged or missing, it may be that the device has been tampered. In this case, contact Phoenix Contact without delay before using the device.



1 Test marks and revision status (hardware/firmware) of the integrated safety-related PROFINET controller iSPNS 3000

2 Security seals

SD card

The use of the SD card is mandatory. You may only use encrypted SD cards (refer to the topic SD card encryption).

Phoenix Contact recommends the use of the following SD cards:

– SD FLASH 8GB PLCNEXT MEMORY **LIC** (item no. 1151112)
– SD FLASH 32GB PLCNEXT MEMORY **LIC** (item no. 1151111)
– SD FLASH PLCNEXT MEMORY **LIC CFG** (item no. 1308064)

From firmware 2024.0 LTS, these special SD cards provide data protection, and therefore can be used together with the Security Profile.

Sensitive data is stored on the SD card. This data can even be restored after reformatting the SD card.

- To protect the data, make sure that the cover of the slot for the SD card is always screwed tight.

Touch screen display

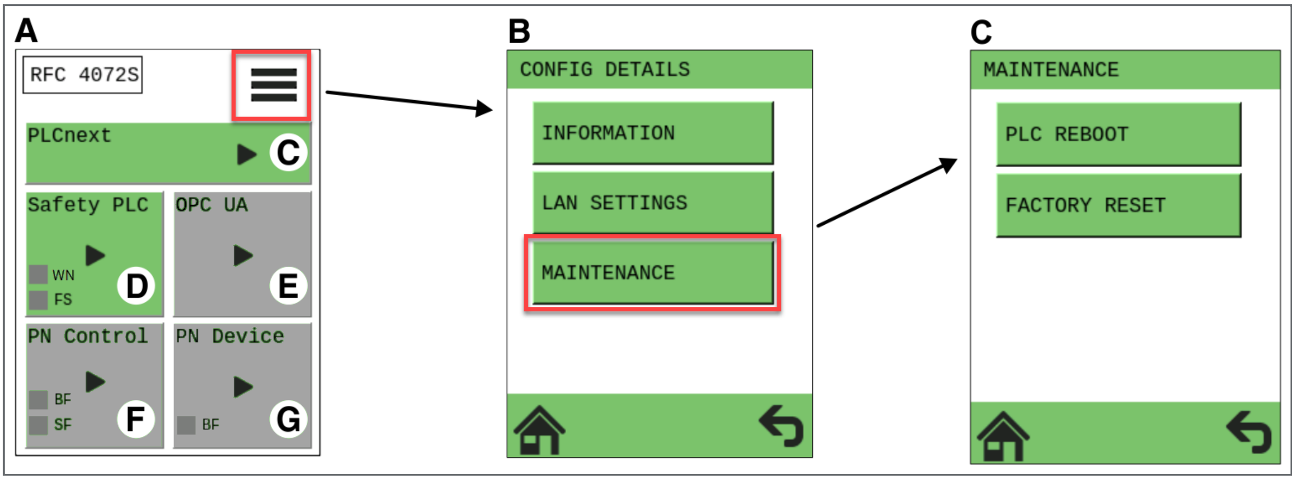
The RFC 4072S has a touch screen display (also referred to as “display” in the following). This display shows tiles containing various information on the device and the connected network. The display allows you to retrieve information about the iSPNS 3000 and OPC UA connections, for example. The depth of information shown varies by tapping the individual tiles. The display allows menu-guided operation of the device. Among other things, you can reset the device to the factory default.

How to reset the controller

> **Note:** Resetting to the default settings deactivates the Security Profile.

The menu **MAINTENANCE** allows for the following maintenance settings:

- **PLC REBOOT**:
  Restarts the RFC 4072S
- **FACTORY RESET**:
  Resets the RFC 4072S to the factory defaults (Reset type 1)



A Home menu
B CONFIG DETAILS menu
C MAINTENANCE menu

Status information

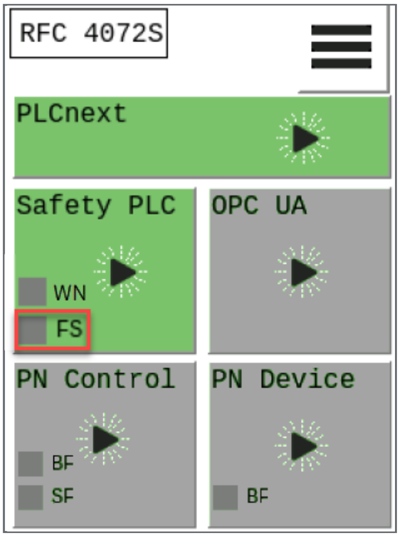
There are status information on the touch screen display. The status information of the individual tiles of the display is only shown in the home menu. The background color on the individual tiles varies depending on the state.

Status information of the safety PLC (iSPNS 3000):

Indicator	Color	Meaning
■	Gray	The function of the iSPNS 3000 is deactivated. No safety-related program is loaded.
⏸	Blue	Initial state in which the iSPNS 3000 passes through various phases until it is ready for operation (e.g., self-test, synchronization with the standard controller). The iSPNS 3000 is ready for operation once it has passed through these phases. FS (Failure State) is off.
▶	Green	Cyclical processing of the safety-related application program has started. FS (Failure State) is off.
▶	Orange	The iSPNS 3000 is in the "Debug Run" state. This state was invoked from the PLCnext Engineer software with an active online connection. FS (Failure State) is off.
■	Orange	The iSPNS 3000 is in the "Debug Stop" state. This state was invoked from the PLCnext Engineer software with an active online connection. The iSPNS 3000 is ready. Cyclical processing of the safety-related application program has stopped. The iSPNS 3000 must be started manually via the PLCnext Engineer software. FS (Failure State) is off.
■	Red	The iSPNS 3000 is in the safe state (failure state). FS (Failure State) is red.

Diagnostic indicators

The diagnostic indicators of all the tiles are displayed in the home menu using virtual LEDs.
Below you can see the meaning of the FS (Failure State) LED (at the Safety PLC tile):



LED	Color		Meaning
FS	Red	On	A critical error has occurred and been detected. The iSPNS 3000 has switched to the "safe state".
		Flashing 1 Hz	– Initialization phase is running (firmware boot process with power-on self-test, loading the parameterization and configuration data from the parameterization memory, booting the safe application program) *or* – Initialization phase has been aborted with an error *or* – Error-free DEBUG state of the iSPNS 3000
	Gray	Off	Error-free operating state of the iSPNS 3000 (if supply voltage is present)

...continuation see next page...

Booting the device

During boot, the USB interface is intentionally accessible via a connected keyboard.
You can choose between:

- Linux A
- Linux B
- Recovery
- Installing a new firmware via USB device

After the firmware has booted, the USB interface is disabled.

NOTICE

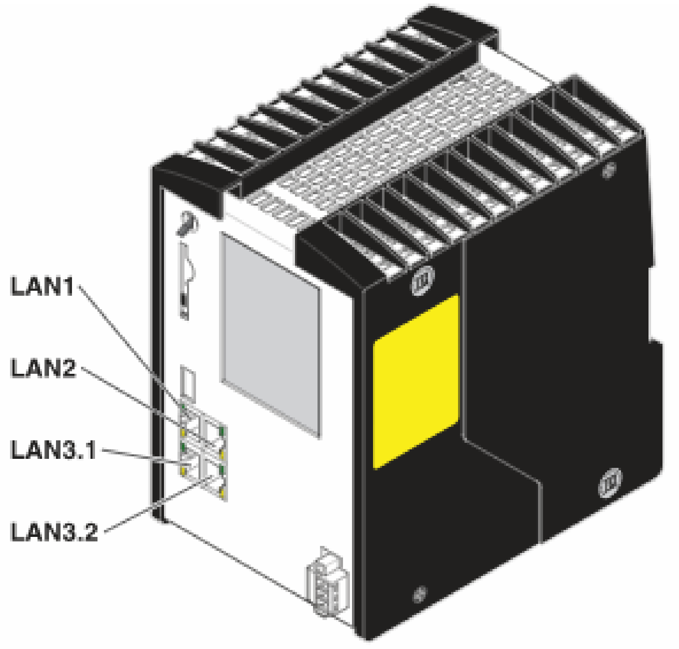
Risk of unauthorized access to the firmware of the device

Attackers can boot the device with a different firmware than intended if they have physical access to the device.

To prevent damage, data corruption, loss of data, or misuse of data due to authorized access, make sure that only authorized access is possible:

- Protect the interfaces by installing the device in a control cabinet.
- Secure the control cabinet with a lock.
- Make sure that only authorized persons have access to the control cabinet key.
- Make sure that on all possible boot partitions the intended firmware is installed before using the device for productive applications.

Assignment of the Ethernet interfaces



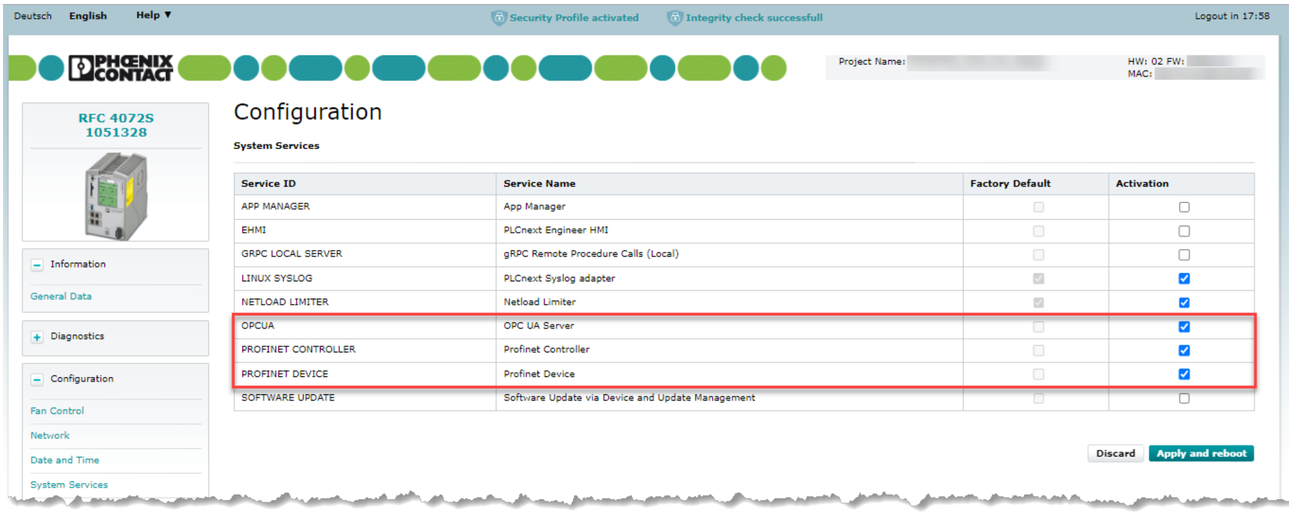
The following is an overview of how the Ethernet interfaces are assigned by default in the various pages in the WBM:

Ethernet interface hardware	Description	PROFINET function by default	Ethernet interface WBM - Network page	Ethernet interfaces WBM - Firewall page
LAN1	10/100/1000 BASE-T(X), separate MAC address	PROFINET Controller	TCP/IP (LAN1)	enp1s0
LAN2	10/100/1000 BASE-T(X), separate MAC address		TCP/IP (LAN2)	enp2s0
LAN3.1 LAN3.2	10/100/1000 BASE-T(X), common MAC address, internally switched	PROFINET Device	TCP/IP (LAN3) - Switched Mode	enp6s0

...continuation see next page...

Activating PROFINET and OPC UA®

After you have performed a threat analysis and implemented appropriate protective measures from the security context, you can activate PROFINET and OPC UA®.



Project Name: [redacted]
HW: 02 FW: [redacted]
MAC: [redacted]

Configuration

System Services

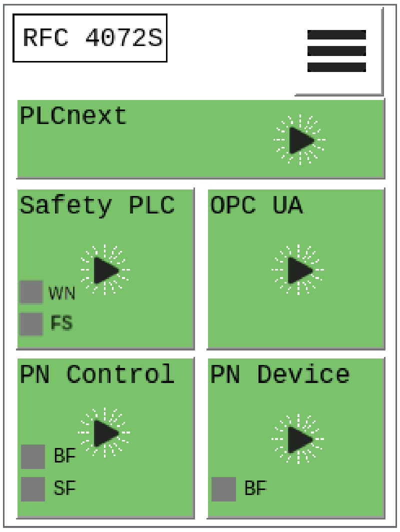
Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	□	□
EHMI	PLCnext Engineer HMI	□	□
GRPC LOCAL SERVER	gRPC Remote Procedure Calls (Local)	□	□
LINUX SYSLOG	PLCnext Syslog adapter	☑	☑
NETLOAD LIMITER	Netload Limiter	☑	☑
OPCUA	OPC UA Server	□	☑
PROFINET CONTROLLER	Profinet Controller	□	☑
PROFINET DEVICE	Profinet Device	□	☑
SOFTWARE UPDATE	Software Update via Device and Update Management	□	□

ℹ For further information on how to activate PROFINET, refer to the topic Activating PROFINET® in this PLCnext Technology - Security Info Center.

ℹ For further information on how to activate OPC UA® , refer to the topic Activating OPC UA Server in this PLCnext Technology - Security Info Center.

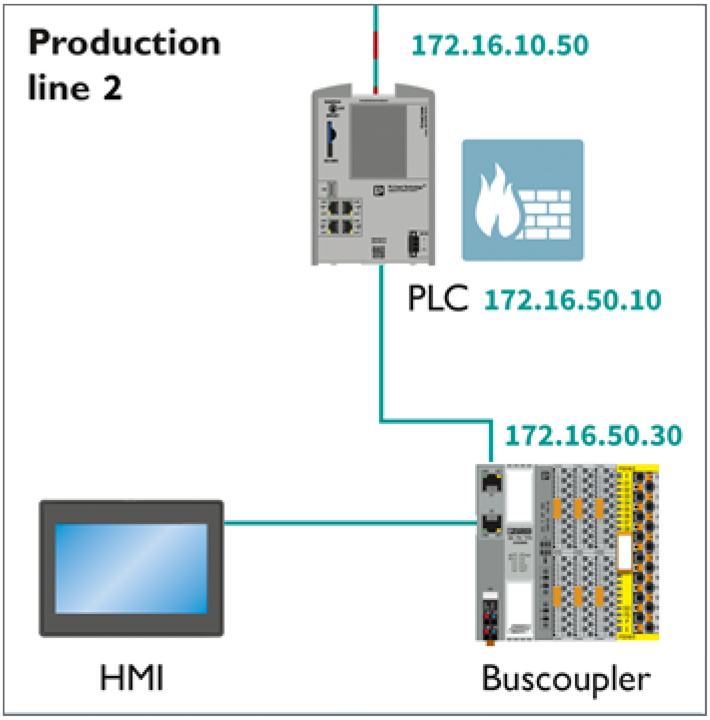
ℹ For further information on PROFINET in the WBM, refer to the PROFINET diagnostics topic in the main PLCnext Technology - Info Center.

After activation of PROFINET and OPC UA®, the home display looks like this:

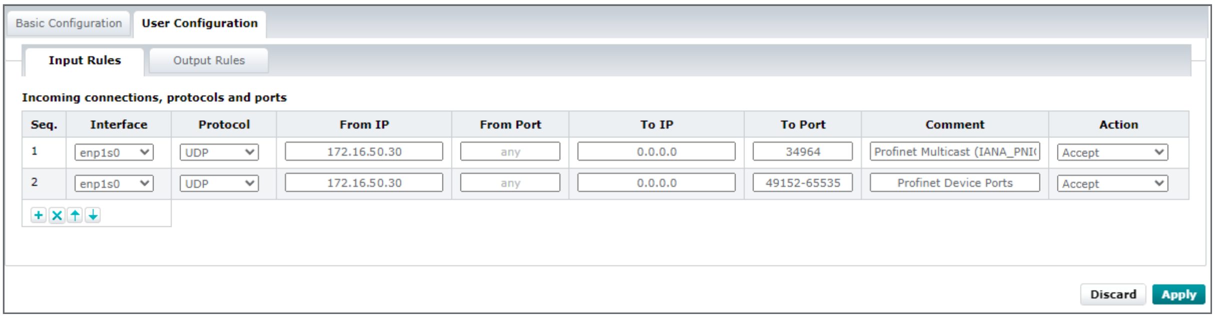


Using PROFINET

You need to adjust the firewall configurations (for more information, refer to the firewall basic configurations):



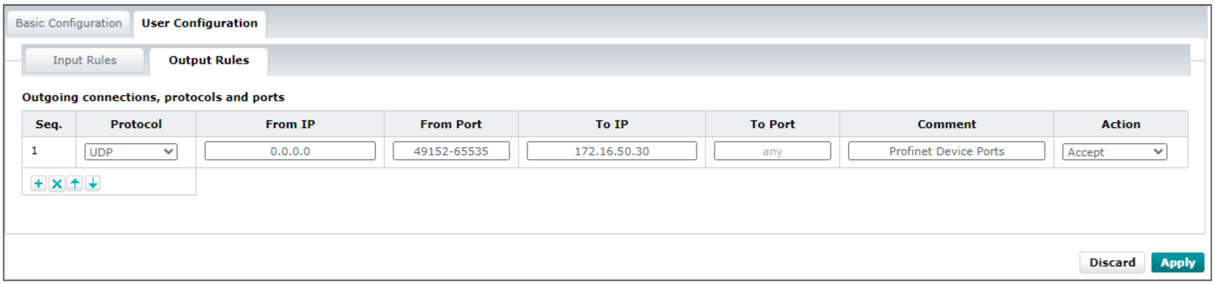
Input rules:



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	enp1s0	UDP	172.16.50.30	any	0.0.0.0	34964	Profinet Multicast (IANA_PNI(	Accept
2	enp1s0	UDP	172.16.50.30	any	0.0.0.0	49152-65535	Profinet Device Ports	Accept

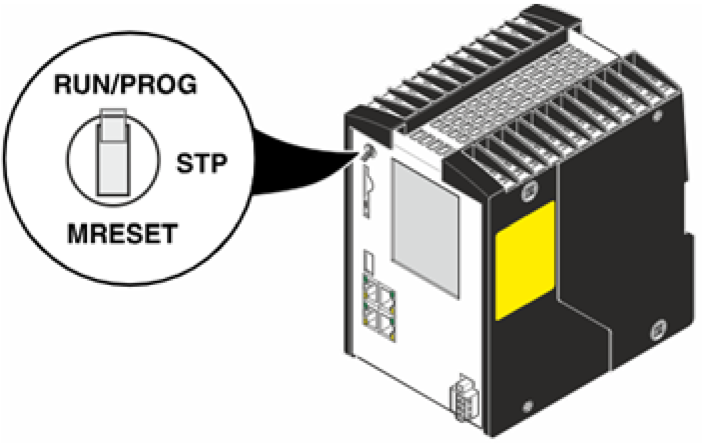
Output rules:



Outgoing connections, protocols and ports

Seq.	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	UDP	0.0.0.0	49152-65535	172.16.50.30	any	Profinet Device Ports	Accept

Mode selector switch



The mode selector switch is used to define the operating state of the standard controller only. The mode selector switch does not influence the operating state of the safety-related PROFINET controller (SPNS).

There are three operating modes: The RUN/PROG and STP (= stop) positions have a toggle-button function, and the MRESET position has a push-button function. After releasing the switch in the MRESET position, it returns to the STP position.

ℹ For further information on the mode selector switch, refer to the user manual for RFC 4072S controllers.

Netload Limiter configuration

You configure the Netload Limiter on the **Netload Limiter** page in the WBM (**Configuration** → **Network** , **Netload Limiter** tab).

For further information, refer to the topic Configuring Netload Limiter.

Controller-specific information on the 62443-4-2 compliance list

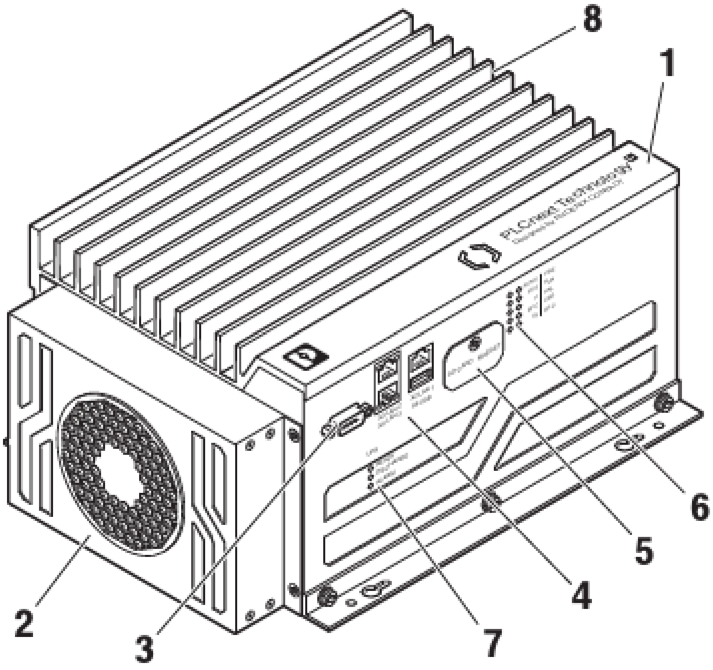
Note: Please note the additional controller-specific information on the 62443-4-2 compliance list.

BPC 9102S

Note: For further information about the hardware, refer to the product documentation of this controller (item no. 1246285):

- User manual
- Product page

Connecting and operating elements



The controller consists of the following components:

1 BPC 9102S

2 BPC 9102 FAN KIT (optional)

3 COM service interface (D-SUB 9 pin strip)

4 LAN1/LAN2/LAN3 Ethernet interfaces (RJ45 jacks; 10/100/1000 Mbps) and USB service interface (USB 3.0 type A socket)

5 Cover of the SD card holder (slot for the configuration memory) and MRESET button

6 Diagnostics and status indicators (LED)

7 Status LEDs of the device-internal UPS

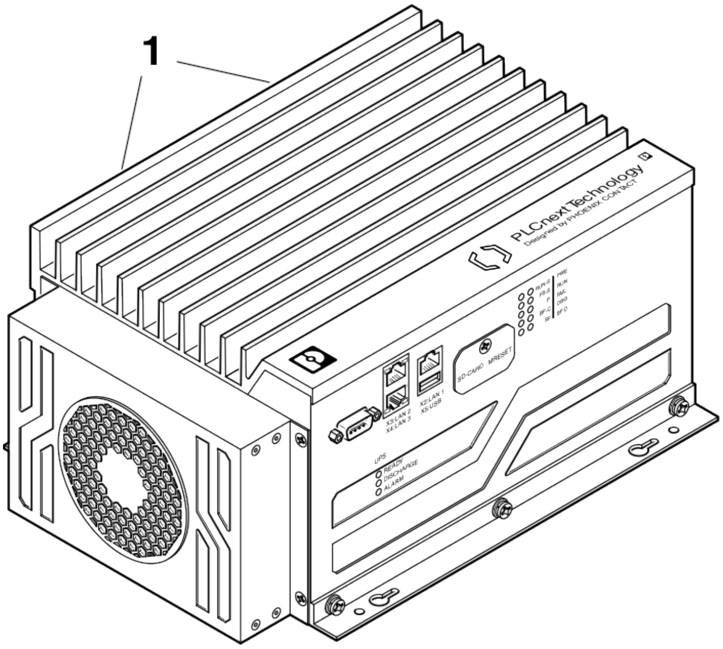
8 Connection for external supply voltage (24 V DC)

Security seals

In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the BPC 9102S.

These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the PLCnext Control can no longer be ensured.

- Check the delivery for transport damage. Damaged packaging is an indicator of potential damage to the device that may have occurred during transport. This could result in a malfunction.
- Do not open the housing. If the housing is opened, the function of the device can no longer be ensured.
- Check at regular intervals that none of the seals are damaged. If any of the seals are damaged or missing, it may be that the device has been tampered. In this case, contact Phoenix Contact without delay before using the device.



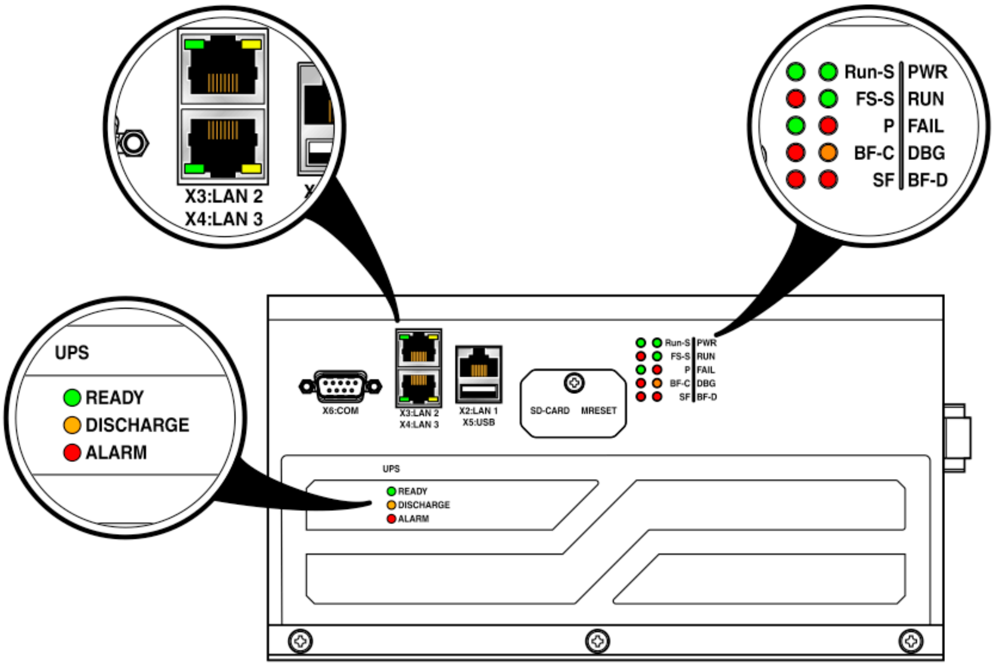
The controller consists of the following components:

1 Security seals (on the unillustrated side of the BPC 9102S)

USB and COM service interfaces

The BPC 9102S has a USB service interface (USB 3.0 type A socket) and a COM service interface (D-SUB 9 pin strip). These two interfaces are for internal service purposes only. During normal operation of the device, these interfaces cannot be used.

Diagnostics and status indicators



LED	Color	Meaning	Status	Description
Run-S	Green	Operating state of the safe application program	On	Cyclical processing of the safety-related application program has started.
			Off	Cyclical processing of the safety-related application program has stopped.
FS-S	Red	Failure state: Safe state of the SPLC 3000	On	A critical error has occurred and been detected. The SPLC 3000 has switched to the safe state (failure state).
			Flashing (1 Hz)	This can indicate: – Initialization phase is running (firmware boot process with power-on self-test; loading parameterization and configuration data from the configuration memory; booting the safe application program) – Initialization phase has been aborted with an error – Error-free BPC 9102S debug mode
			Off	Error-free operating state of the SPLC 3000 with supply voltage present

SD card

The use of the SD card is mandatory. You may only use encrypted SD cards (refer to the topic SD card encryption).

Phoenix Contact recommends the use of the following SD cards:

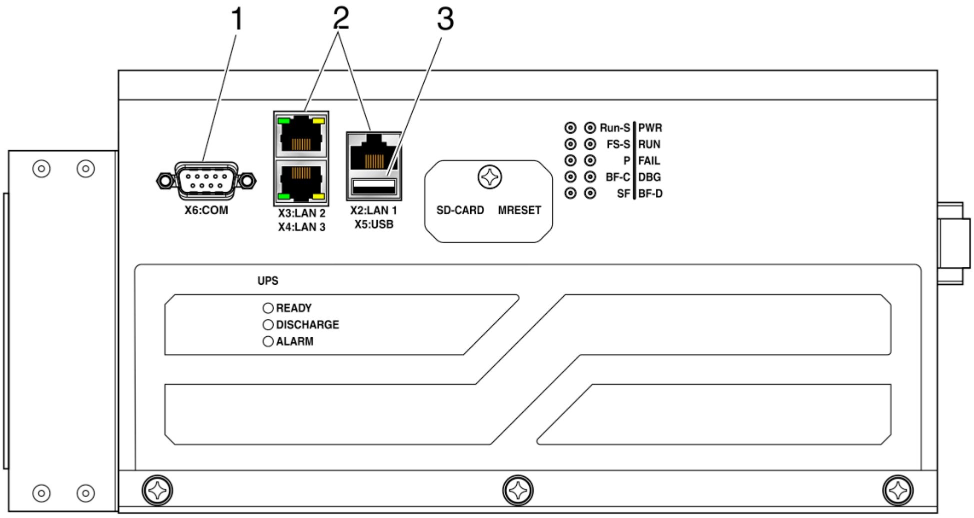
- SD FLASH 8GB PLCNEXT MEMORY **LIC** (item no. 1151112)
- SD FLASH 32GB PLCNEXT MEMORY **LIC** (item no. 1151111)
- SD FLASH PLCNEXT MEMORY **LIC CFG** (item no. 1308064)

From firmware 2024.0 LTS, these special SD cards provide data protection, and therefore can be used together with the Security Profile.

Sensitive data is stored on the SD card. This data can even be restored after reformatting the SD card.

- To protect the data, make sure that the cover of the slot for the SD card is always screwed tight.

Assignment of the Ethernet interfaces



The BPC 9102S is equipped with the following interfaces:

Pos.	Interfaces		Description
1	COM	RS-232	Service interface (reserved internally): D-SUB 9 pin strip (serial, RS-232)
2	LAN1	3 x Ethernet	Ethernet: 1 Gbps or 2.5 Gbps
	LAN2		PROFINET: Controller interfaces function (max. 1 Gbps)
	LAN3		PROFINET: Device interfaces function (max. 1 Gbps)
3	USB		Service interface (reserved internally): USB 3.0 socket (type A)

Note: The IP addresses of interfaces LAN1/LAN2/LAN3 must be in different subnets.

The following is an overview of how the Ethernet interfaces are assigned by default in the various pages in the WBM:

Ethernet interface hardware	Description	PROFINET function by default	Ethernet interface WBM - Network page	Ethernet interfaces WBM - Firewall page
X2:LAN1	10/100/1000 BASE-T(X), separate MAC address		**TCP/IP (LAN1)**	**LAN1**
X3:LAN2	10/100/1000 BASE-T(X), separate MAC address	PROFINET Controller	**TCP/IP (LAN2)**	**LAN2**
X4:LAN3	10/100/1000 BASE-T(X), common MAC address, internally switched	PROFINET Device	**TCP/IP (LAN3)**	**LAN3**

Activating PROFINET

After you have performed a threat analysis and implemented appropriate protective measures from the security context, you can activate PROFINET.

ℹ For information on how to activate PROFINET, refer to the topic Activating PROFINET in this PLCnext Technology - Security Info Center.

ℹ For further information on PROFINET in the WBM, refer to the PROFINET diagnostics topic in the main PLCnext Technology - Info Center.

Using PROFINET

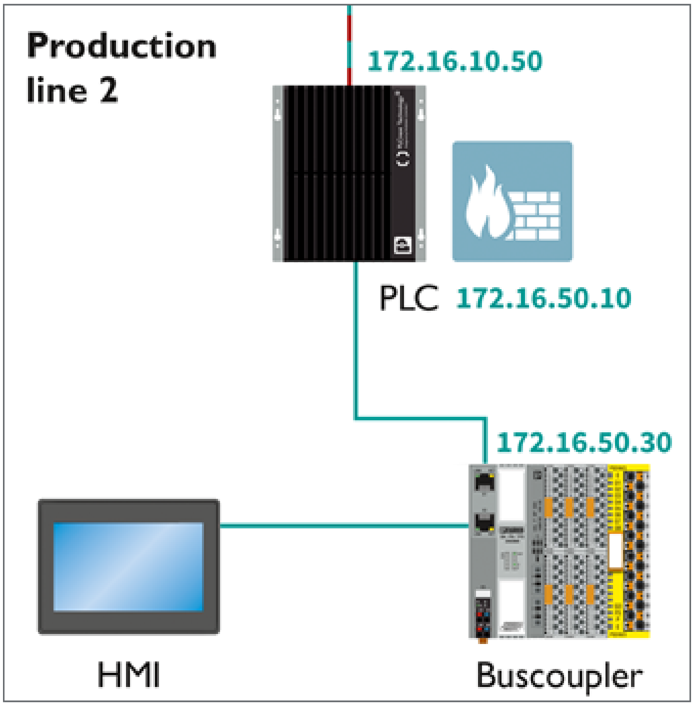
If you activate and use PROFINET , it is strongly recommended to use the PROFINET configuration described below.

Depending on the connected interface, the BPC 9102S can be accessed on the Ethernet via three different IP addresses.

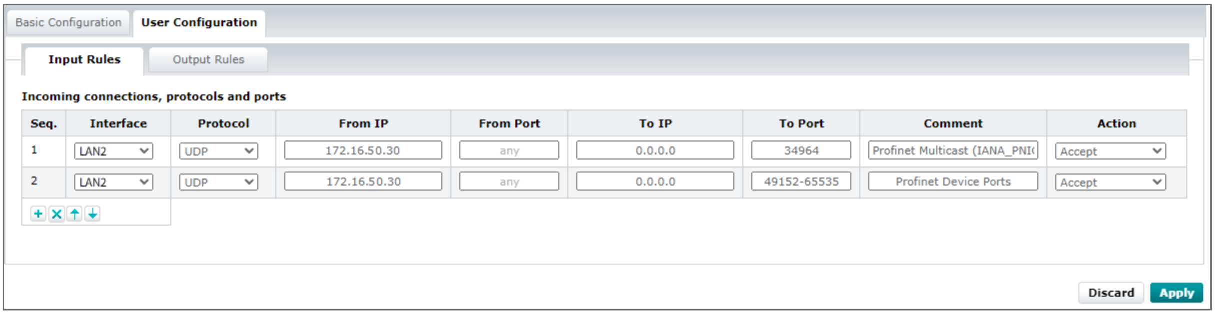
Note:

- The IP addresses of interfaces LAN1/LAN2/LAN3 must be in different subnets.
- The PROFINET controller function of the BPC 9102S is available at interface LAN2. This interface must then be assigned an IP address if the PROFINET controller function of the device is to be used in the application.
- An IP address must be assigned to the LAN3 interface if you want to use the PROFINET device function of the BPC 9102S on these interfaces.
- The LAN1 and LAN3 interfaces do not necessarily have to be assigned an IP address if, for example, communication between a PC with PLCnext Engineer and the BPC 9102S is also implemented via the LAN2 interface. We recommend that appropriate IP addresses be assigned to all interfaces.

You need to adjust the firewall configurations (for more information, refer to the firewall basic configurations):



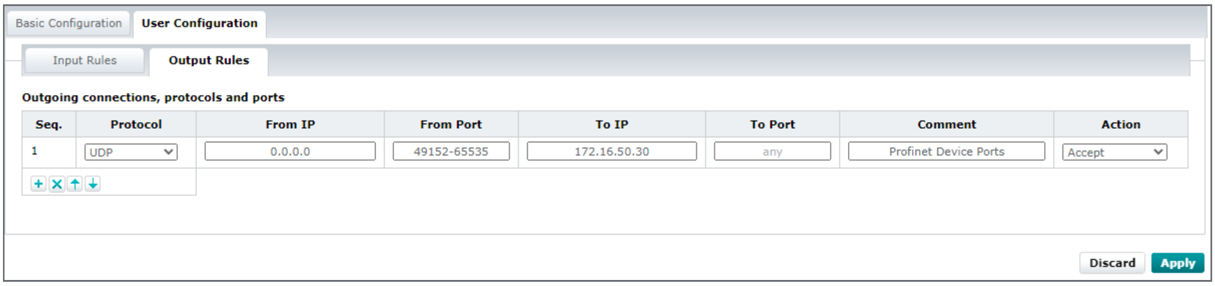
Input rules:



Incoming connections, protocols and ports

Seq.	Interface	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	LAN2	UDP	172.16.50.30	any	0.0.0.0	34964	Profinet Multicast (IANA_PNI(	Accept
2	LAN2	UDP	172.16.50.30	any	0.0.0.0	49152-65535	Profinet Device Ports	Accept

Output rules:



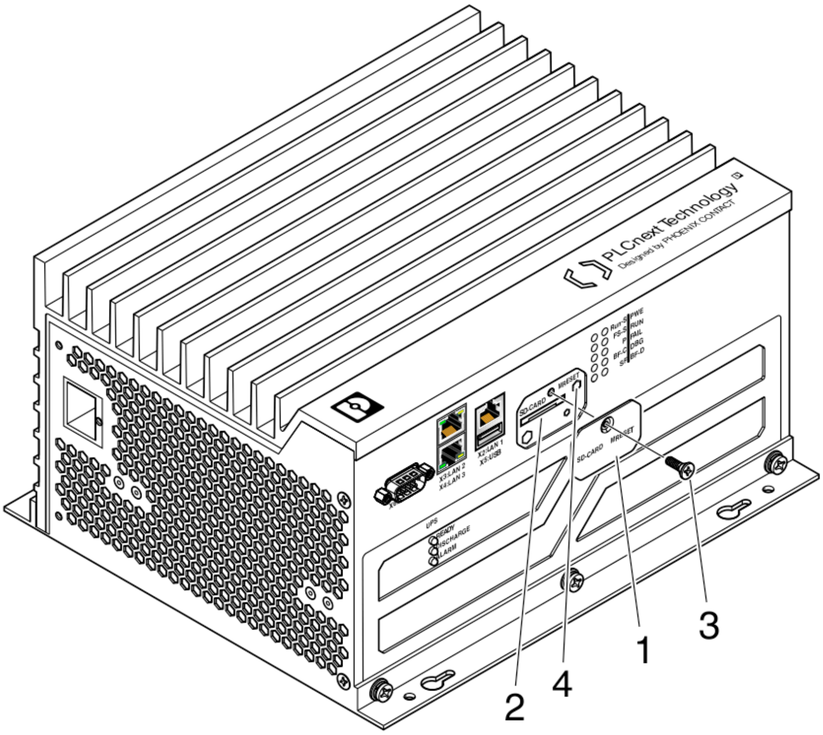
Outgoing connections, protocols and ports

Seq.	Protocol	From IP	From Port	To IP	To Port	Comment	Action
1	UDP	0.0.0.0	49152-65535	172.16.50.30	any	Profinet Device Ports	Accept

Resetting the controller

You reset the BPC 9102S by actuating the MRESET button.

The MRESET button is located under the side cover of the BPC 9102S. The button can only be pressed with a pointed object (such as a pen).
Using the MRESET button will delete the application program in the BPC 9102S main memory and the retain data.



Procedure:

- To actuate the MRESET button (**4**), remove the screw (**3**) in the cover (**1**) with a Torx® TX 10 screwdriver.
- Then swivel the cover (**1**) to the side so that you can easily access the MRESET button (**4**).
- To delete the application program and the retain data, actuate the MRESET button in the following sequence:
  - Press and hold down the button for three seconds.
  - Release the button for less than three seconds.
  - Press and hold down the button for three seconds.
- Re-affix the cover (**1**) after actuating the MRESET button by tightening the screw (**3**) to protect the MRESET button against accidental damage or actuation.

Secure disposal

Sensitive data is stored on the SD card. This data can even be restored after reformatting the SD card. To ensure that your data does not fall into unauthorized hands, you should physically destroy the SD card before disposal.

- Physically destroy the SD card, e.g., by cutting up the SD card.
- Dispose of the irreparably damaged SD card in accordance with the applicable national regulations.

The device contains an internal memory.

- To ensure that the internal memory cannot be accessed, you must ensure that the hardware is disposed of safely.

For more information on secure disposal, refer to the topic Secure disposal.

Controller-specific information on the 62443-4-2 compliance list

Note: Please note the additional controller-specific information on the 62443-4-2 compliance list.

Controller-specific information on the 62443-4-2 compliance list

EDR 3.14

The PLCnext Control supports a software-based partial integrity and authenticity protection of the boot process. Before mounting the Linux file system, a system integrity check is performed. The boot loader, the kernel and certain files are not covered by this integrity check.

You can check the result of the integrity check here: Checking the integrity state.

The software-based partial integrity and authenticity protection of the boot process has been certified in the last three audits since 2021. With new CPUs now supporting hardware secure boot from the ROM, a new state of the art security technology is established. From version 2024.0, PLCnext Control devices do not longer fully comply with the EDR 3.14 requirements.

As the threat landscape evolves, more organizational security measures must be supervised to protect the device against tampering. Existing PLCnext Control devices will not be updated to a compliant integrity and authenticity protection of the boot process, as device replacement use cases can not be supported by compliant firmware versions. New PLCnext Control devices with new CPUs supporting hardware secure boot (EDR 3.14) are under development and are planned to be released to the market in 2025 and 2026, depending on the controller type.

The prerequisite is that the Security Profile is activated. Only use PLCnext Control devices in the security context with an activated Security Profile.

Before installing a project, ensure that the project integrity settings in the toolchain and PLCnext Engineer are active to protect it (Checking project data integrity). Verify the integrity of the device's firmware and application by checking the local security logs and enabling syslog supervision by a network server to monitor access to the device: Security logging and Configuring central logging.
Follow all security advice in the PLCnext Technology - Security Info Center:

- understanding the generic security concept
- security hardening
- configuring the firewall
- protecting the device against network attacks and physical access

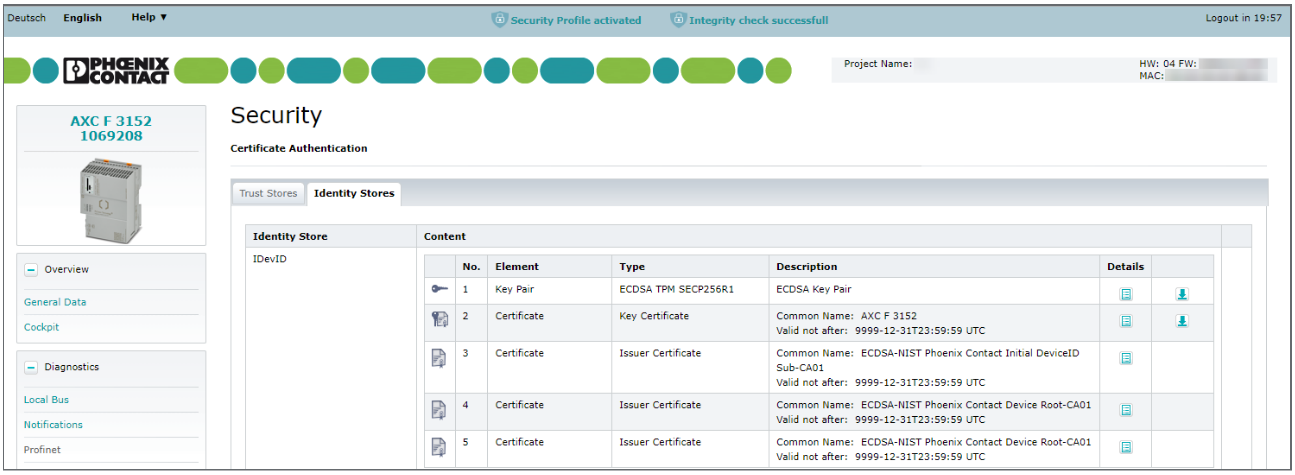
OpenSSL

The OpenSSL library has been updated to version 3.0. The PLCnext Technology firmware uses this version only. For compatibility reasons the previous OpenSSL library (version 1.1.1) still exists in the file system. As this version is outdated, it will be removed in one of the next firmware releases. For applications (including PLCnext Technology Apps) which use the OpenSSL library, an update is recommended as soon as an application version is available, which uses OpenSSL 3.0.

Device certificates

In this topic you can find out about current device certificates.

For example, there is currently a new device certificate for the PLCnext Control devices, see the following screenshot:



Identity Store	Content
IDevID	

	No.	Element	Type	Description	Details	
	1	Key Pair	ECDSA TPM SECP256R1	ECDSA Key Pair		
	2	Certificate	Key Certificate	Common Name: AXC F 3152 Valid not after: 9999-12-31T23:59:59 UTC		
	3	Certificate	Issuer Certificate	Common Name: ECDSA-NIST Phoenix Contact Initial DeviceID Sub-CA01 Valid not after: 9999-12-31T23:59:59 UTC		
	4	Certificate	Issuer Certificate	Common Name: ECDSA-NIST Phoenix Contact Device Root-CA01 Valid not after: 9999-12-31T23:59:59 UTC		
	5	Certificate	Issuer Certificate	Common Name: ECDSA-NIST Phoenix Contact Device Root-CA01 Valid not after: 9999-12-31T23:59:59 UTC		

Further information can be found on the Phoenix Contact Device PKI website.

Protection against physical access

Protection against physical access is an important requirement for OT devices (component). Attackers may access the hardware and try to manipulate the firmware, configuration, or applications.

IEC 62443 describes major attack vectors, like:

- **non-operational**
  - transferring the component from the manufacturer to the system integrator
  - transferring the component installed to the asset owner in a cabinet together with the machine
  - storing the component on stock
- **commissioning/maintenance**
  - accessing the component by the service personal
- **operational**
  - recognize physical access to the component during running

Even if PLCnext Control devices provide already several tampering protection mechanisms, the potential physical access needs to be supervised by the system integrator, the service provider, and the asset owner. This is done by using additional organizational measures defined in their Information Security Management System (ISMS). Such measures are for example described in IEC 62443-2-4 and IEC 62443-3-3, as well as in ISO IEC 27001.

NOTICE

Risk of unauthorized access to devices

The safety controller RFC 4072S has a touch screen display and is used with an external SD card. This makes unencrypted information available. To prevent damage, data corruption, loss of data, or misuse of data due to authorized access, make sure that only authorized access is possible.

- Protect the interfaces by installing the devices in a control cabinet.
- Secure the control cabinet with a lock.
- Make sure that only authorized persons have access to the control cabinet key.
- Run cables in such a way that they are protected against unauthorized access.

PLCnext Control devices provide security measures to support organizational measures by:

- Security seals (security void) to protect the housing as well as indicating opening attempts.
- **CabinetDoorState** library providing the possibility to generate security notifications based on lockable, supervised cabinets.
- Disabled communication on external interfaces, e.g. SD card slot, USB connector

Shipping packaging

Stickers are attached to the packaging to prevent tampering with the device during shipping (e.g. by installing a different firmware) and to detect unauthorized opening of the packaging.

- Make sure that the packaging has not yet been opened. To do this, check that the sticker on the box of the PLCnext Control is intact.

If the sticker on the box is damaged, you must not use the device!

- If you notice any damage to the packaging, contact Phoenix Contact immediately.

Measures for shipment

If a PLCnext Control is delivered from the system integrator to the asset owner, the following measures must be taken into account:

- There must be no customer-specific data on the internal SD card.
- Only use external, encrypted SD cards and send them in a separate package from the PLCnext Control.
- Prepare the PLCnext Control so that it can be used with the external SD card (set up the recovery password).
- Send the recovery password and the encryption password separately from the PLCnext Control and SD card.
- Preferably, PLCnext Control, SD cards and passwords should be shipped individually in sealed packaging with security seals.

Security seals

In order to prevent manipulation of the device supplied and to detect unauthorized opening of the device, security seals have been applied to the controller. These security seals are damaged in the event of unauthorized opening. In this case, correct operation of the controller can no longer be ensured.

For more information, refer to the corresponding topic of the controller (e. g. AXC F 2152).

Cabinet supervision

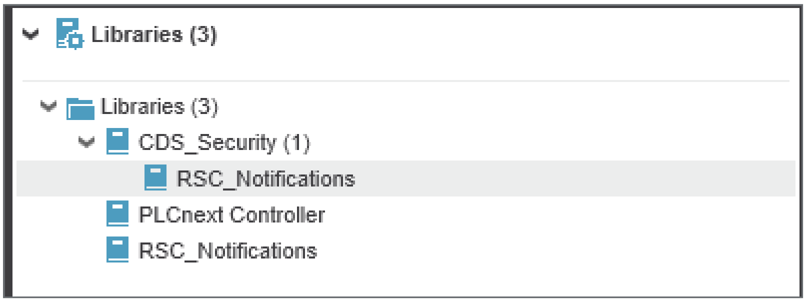
To protect the PLCnext Control during operation, commissioning, and maintenance an example application and library can be installed via the app "IEC 62443 Cabinet Supervision" in the PLCnext Store. It contains the `CDS_SendNotification` function block which can be connected to one or more cabinet supervision contacts. If the status of the cabinet door supervision contacts is changed, the function block is generating security notifications which may indicate an unauthorized access.

To supervise the control cabinet door, add the `CDS_SendNotification` function block into your program, connect it with the cabinet supervision contact, setup the notification text according to your organizational measures, and you will be notified about every action at the cabinet's door.

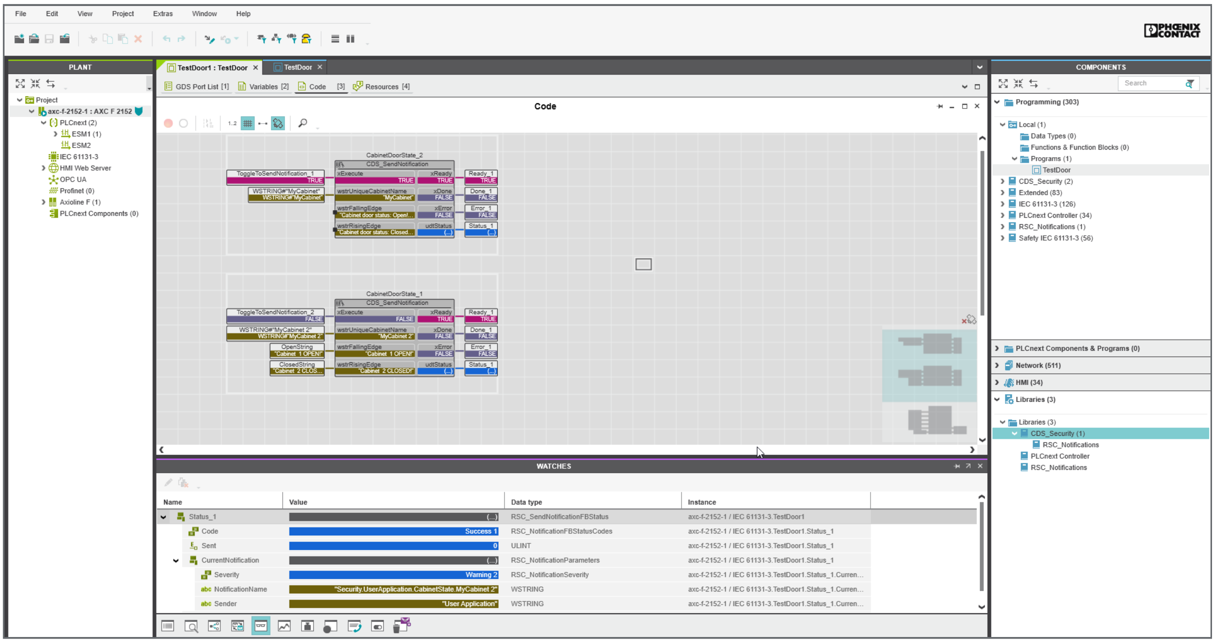
From the app "IEC 62443 Cabinet Supervision" you must install the function block libraries `CDS_Security` and `RSC_Notifications` .

To use the `CDS_SendNotification` function block, proceed as follows:

- Open your project in the PLCnext Engineer. show more
- From the **Libraries** section of the **COMPONENTS** area, insert the `RSC_Notifications` function block example into your program.

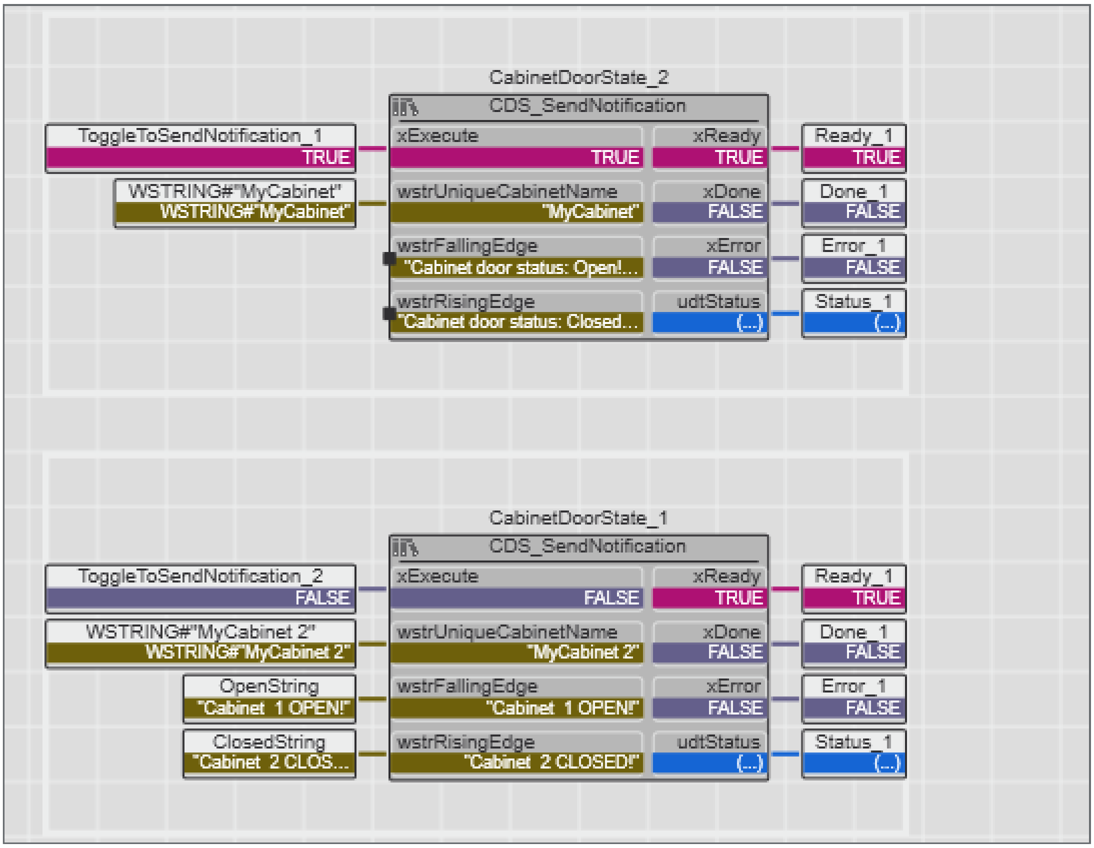


- Instantiate one function block per cabinet door to be supervised.



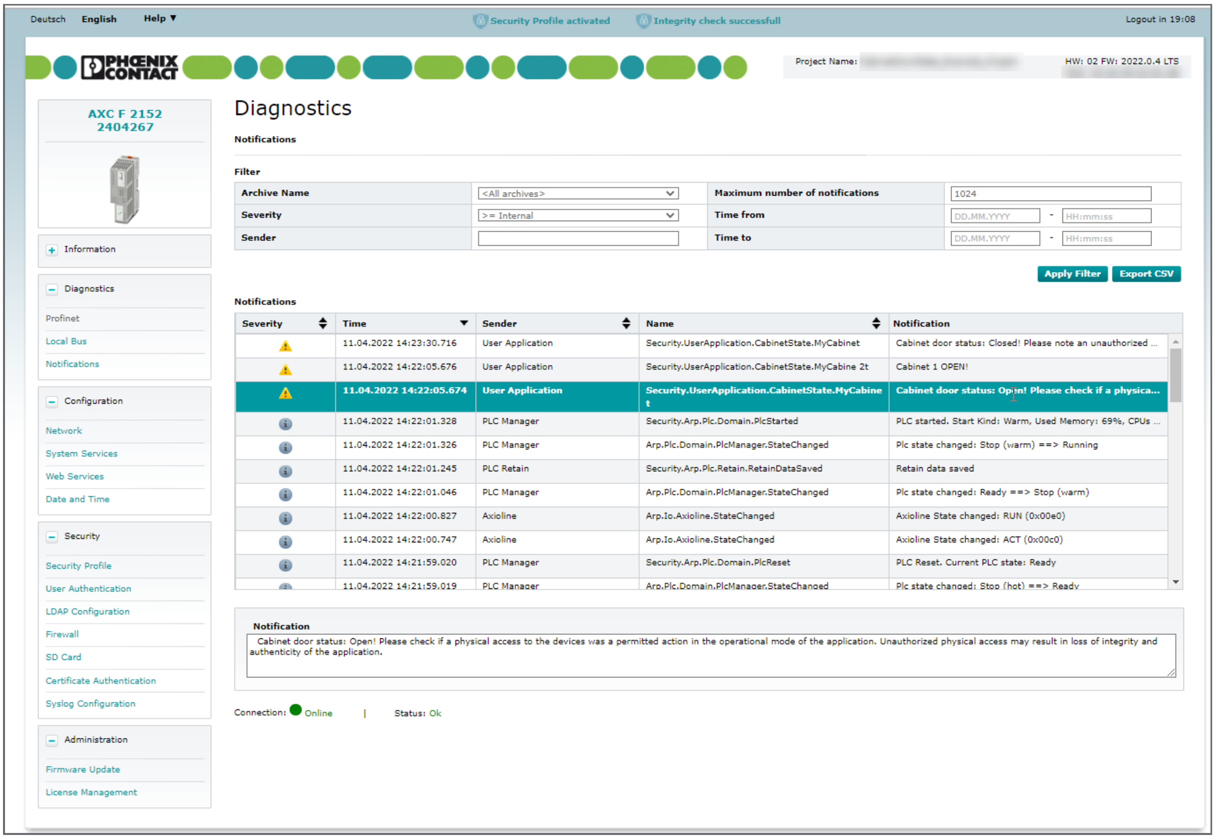
Name	Value	Data type	Instance
Status_1	(...)	RSC_SendNotificationFBStatus	axc-f-2152-1 / IEC 61131-3.TestDoor1
Code	Success 1	RSC_NotificationFBStatusCodes	axc-f-2152-1 / IEC 61131-3.TestDoor1.Status_1
Sent	0	ULINT	axc-f-2152-1 / IEC 61131-3.TestDoor1.Status_1
CurrentNotification	(...)	RSC_NotificationParameters	axc-f-2152-1 / IEC 61131-3.TestDoor1.Status_1
Severity	Warning 2	RSC_NotificationSeverity	axc-f-2152-1 / IEC 61131-3.TestDoor1.Status_1.Curren...
NotificationName	"Security.UserApplication.CabinetState.MyCabinet 2"	WSTRING	axc-f-2152-1 / IEC 61131-3.TestDoor1.Status_1.Curren...
Sender	"User Application"	WSTRING	axc-f-2152-1 / IEC 61131-3.TestDoor1.Status_1.Curren...

- Assign inputs and outputs of the function blocks.



Note: The default setting of the IN ports is NC (`normally closed`). If you use an NO contact (`normally open`), you must adjust the string accordingly.

- Save and transfer your project to the controller.
  ↪ Now you will receive messages about the status of your control cabinet via the Web-based Management (WBM) on your PLCnext Control:



Project Name: [redacted]

HW: 02 FW: 2022.0.4 LTS [redacted]

Diagnostics

Notifications

Filter

Archive Name	<All archives>	Maximum number of notifications	1024
Severity	>= Internal	Time from	DD.MM.YYYY - HH:mm:ss
Sender		Time to	DD.MM.YYYY - HH:mm:ss

Notifications

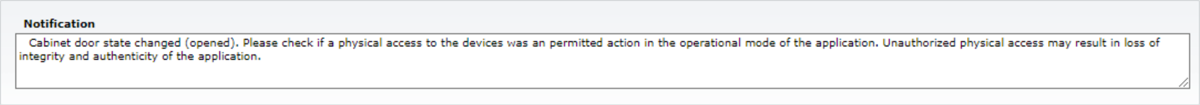
Severity	Time	Sender	Name	Notification
⚠	11.04.2022 14:23:30.716	User Application	Security.UserApplication.CabinetState.MyCabinet	Cabinet door status: Closed! Please note an unauthorized ...
⚠	11.04.2022 14:22:05.676	User Application	Security.UserApplication.CabinetState.MyCabine 2t	Cabinet 1 OPEN!
⚠	**11.04.2022 14:22:05.674**	**User Application**	**Security.UserApplication.CabinetState.MyCabine t**	**Cabinet door status: Open! Please check if a physica...**
ℹ	11.04.2022 14:22:01.328	PLC Manager	Security.Arp.Plc.Domain.PlcStarted	PLC started. Start Kind: Warm, Used Memory: 69%, CPUs ...
ℹ	11.04.2022 14:22:01.326	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Stop (warm) ==> Running
ℹ	11.04.2022 14:22:01.245	PLC Retain	Security.Arp.Plc.Retain.RetainDataSaved	Retain data saved
ℹ	11.04.2022 14:22:01.046	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Ready ==> Stop (warm)
ℹ	11.04.2022 14:22:00.827	Axioline	Arp.Io.Axioline.StateChanged	Axioline State changed: RUN (0x00e0)
ℹ	11.04.2022 14:22:00.747	Axioline	Arp.Io.Axioline.StateChanged	Axioline State changed: ACT (0x00c0)
ℹ	11.04.2022 14:21:59.020	PLC Manager	Security.Arp.Plc.Domain.PlcReset	PLC Reset. Current PLC state: Ready
ℹ	11.04.2022 14:21:59.019	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Stop (hot) ==> Ready

Notification

Cabinet door status: Open! Please check if a physical access to the devices was a permitted action in the operational mode of the application. Unauthorized physical access may result in loss of integrity and authenticity of the application.

Connection: ● Online | Status: Ok

↪ In the **Notification** area at the bottom you will see the following notification:



Notification

Cabinet door state changed (opened). Please check if a physical access to the devices was an permitted action in the operational mode of the application. Unauthorized physical access may result in loss of integrity and authenticity of the application.

For more information on how to work with function blocks in PLCnext Engineer, see the Quick Start Guide section of the main PLCnext Technology - Info Center, or refer to the respective section in the PLCnext Engineer Help which is online available.

For more information on how to use the function blocks, see the app documentation on the app's details page in the PLCnext Store.

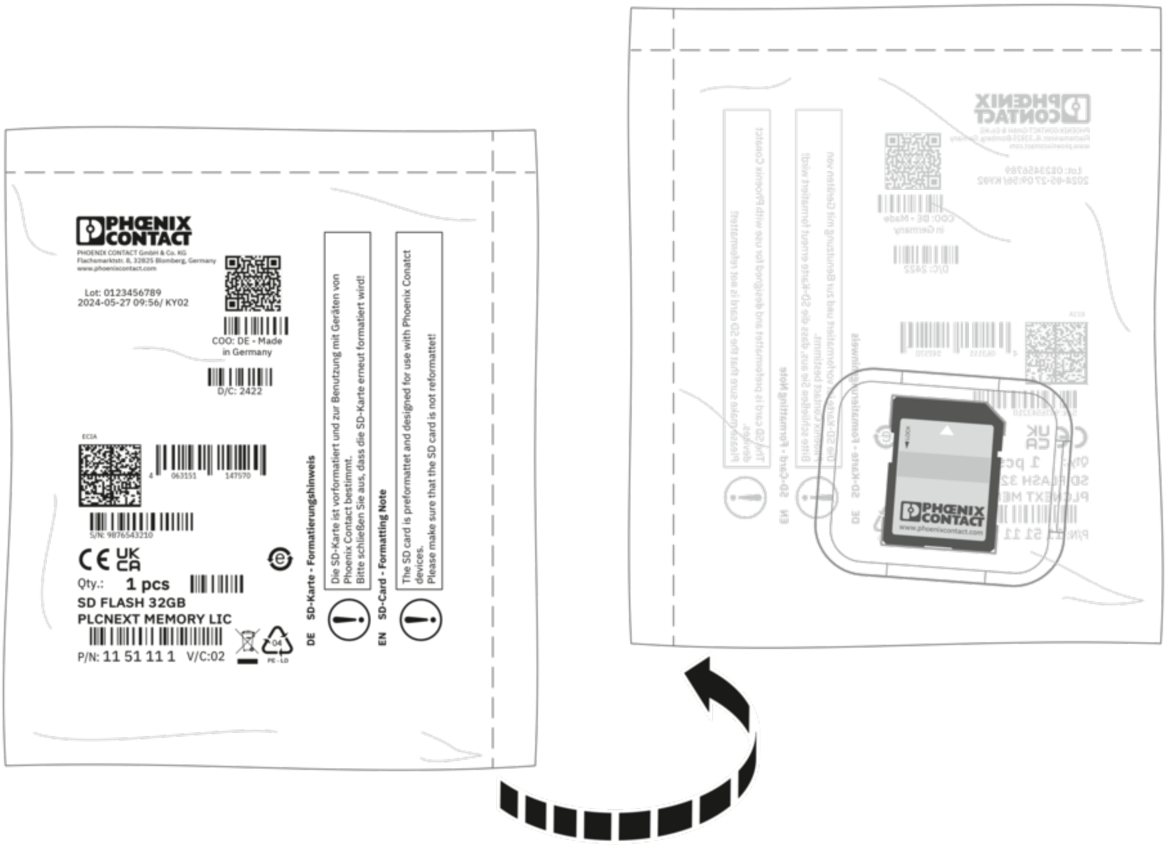
Disabled communication on external interfaces

The housing of PLCnext Control AXC F 1152, AXC F 2152, and AXC F 3152 provides two major external interfaces:

- **Mini USB port**
  The mini USB port is switched off by the firmware and cannot be accessed.
- **External SD card slot**
  The communication with the SD card slot is deactivated by the Security Profile.
  It might be enabled in the Web-based Management after risk assessment, but only using a special SD card supporting encryption (Phoenix Contact item no. 1151112 or item no. 1151111).

SD cards

- Check the delivery of the SD card for transport damage.


PHOENIX CONTACT
PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8, 32825 Blomberg, Germany
www.phoenixcontact.com
Lot: 0123456789
2024-05-27 09:56/ KY02
COO: DE - Made in Germany
D/C: 2422
ECIA
4 063151 147570
S/N: 9876543210
Qty.: 1 pcs
SD FLASH 32GB
PLCNEXT MEMORY LIC
P/N: 11 51 11 1 V/C:02
04 PE - LD
DE SD-Karte - Formatierungshinweis
Die SD-Karte ist vorformatiert und zur Benutzung mit Geräten von Phoenix Contact bestimmt.
Bitte schließen Sie aus, dass die SD-Karte erneut formatiert wird!
EN SD-Card - Formatting Note
The SD card is preformattet and designed for use with Phoenix Conatct devices.
Please make sure that the SD card is not reformattet!
PHOENIX CONTACT
www.phoenixcontact.com

If the packaging is opened or damaged, there is a security risk. The SD card could have been tampered with.

- You must not use the SD card! In this case, contact Phoenix Contact immediately.

SD card encryption

Note:

- Make sure that the Security Profile is activated before you start encrypting the SD card.

Please also note the general information on handling encrypted SD cards in the main PLCnext Technology - Info Center.

You can only use the following SD cards for encryption:

– SD FLASH 8GB PLCNEXT MEMORY **LIC** (item no. 1151112)
– SD FLASH 32GB PLCNEXT MEMORY **LIC** (item no. 1151111)
– SD FLASH PLCNEXT MEMORY **LIC CFG** (item no. 1308064)

These cards have two partitions: The first partition ("system") is reserved for license handling and a second partition for the controller data. This second partition ("overlay") is encrypted using the WBM.

For the encryption of the SD card, *dm-crypt* with the encryption mode *aes-xts-plain* is used. For secure key derivation, *argon2id* is used.
dm-crypt is a cryptography module of the device mapper in the Linux kernel. *dm-crypt* can encrypt and decrypt data using various algorithms. The encryption can be applied to any device files, in most cases to partitions (as in this case to the "overlay" partition of the SD card).

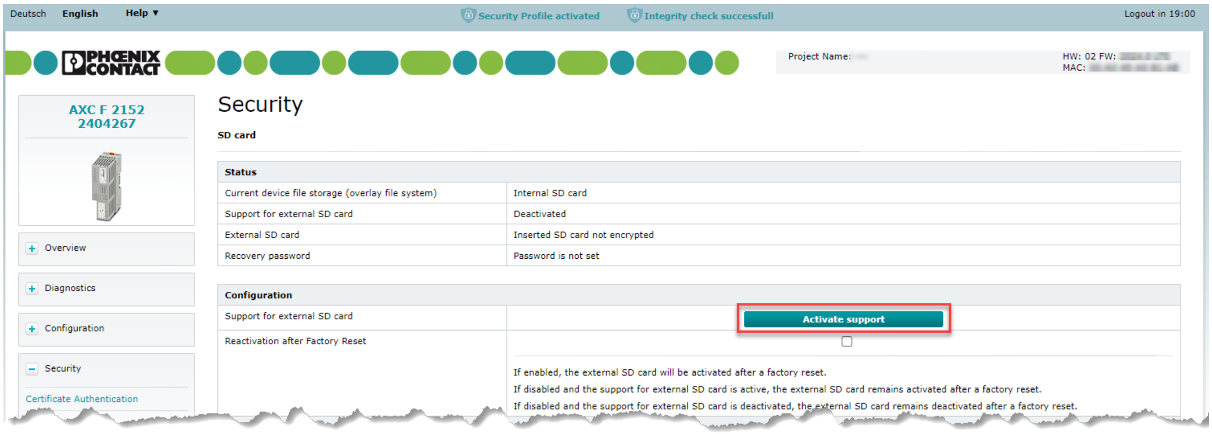
Activating SD card support

Note: Perform these steps in exactly this order as described below! The activation of the support for external SD card and encryption of the SD card must be activated at the same time. This deletes the existing overlay on the SD card and prevents unintentional changes to the currently configured users. You must adhere to this procedure. If you deviate from this procedure, configuration problems may occur.

To use an encrypted sd card, you must first activate support for the external SD card. Proceed as follows:

- Log in to the WBM.
- Open the **SD card** page (**Security** → **SD card**).

- Click the Activate support button.



Project Name: [redacted] HW: 02 FW: [redacted] MAC: [redacted]

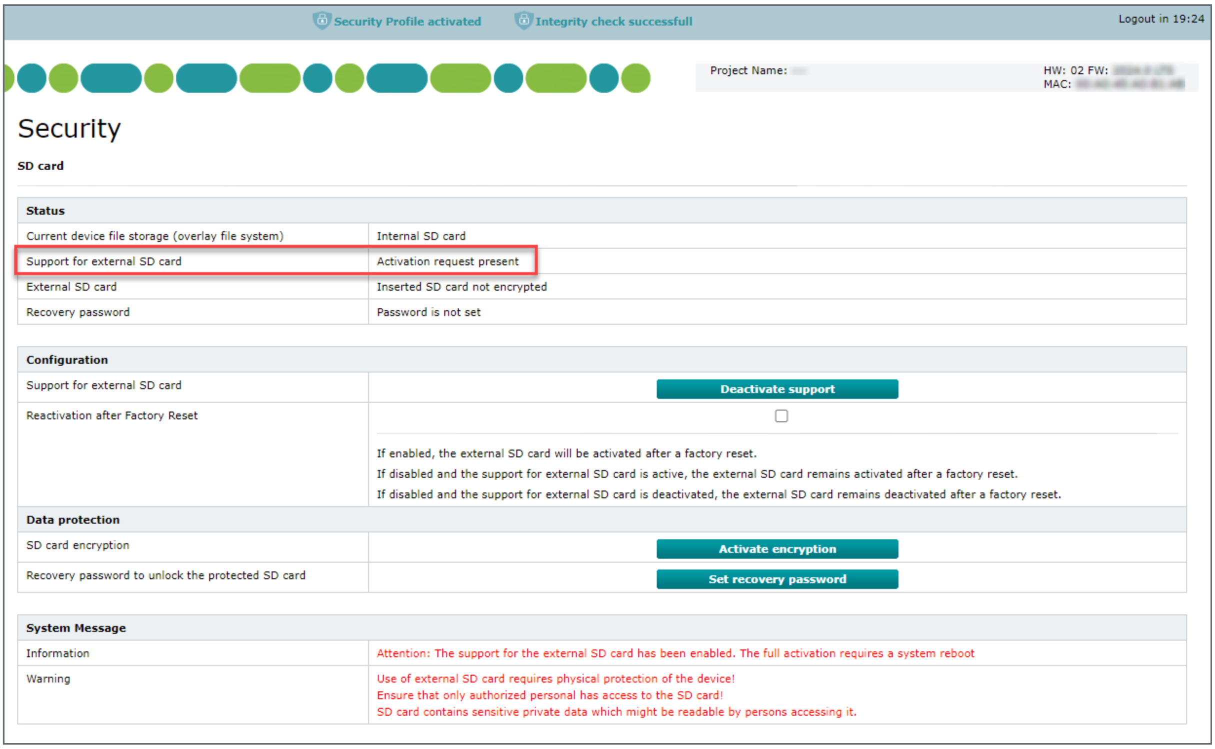
Security

SD card

Status	
Current device file storage (overlay file system)	Internal SD card
Support for external SD card	Deactivated
External SD card	Inserted SD card not encrypted
Recovery password	Password is not set

Configuration	
Support for external SD card	Activate support
Reactivation after Factory Reset	☐ If enabled, the external SD card will be activated after a factory reset. If disabled and the support for external SD card is active, the external SD card remains activated after a factory reset. If disabled and the support for external SD card is deactivated, the external SD card remains deactivated after a factory reset.

↪ You will then see the following status:



Project Name: [redacted] HW: 02 FW: [redacted] MAC: [redacted]

Security

SD card

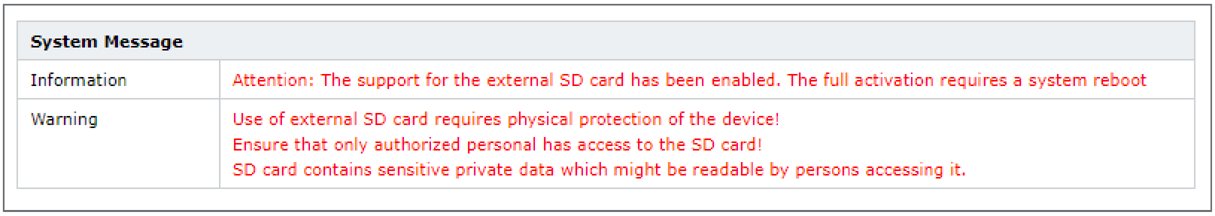
Status	
Current device file storage (overlay file system)	Internal SD card
Support for external SD card	Activation request present
External SD card	Inserted SD card not encrypted
Recovery password	Password is not set

Configuration	
Support for external SD card	Deactivate support
Reactivation after Factory Reset	☐ If enabled, the external SD card will be activated after a factory reset. If disabled and the support for external SD card is active, the external SD card remains activated after a factory reset. If disabled and the support for external SD card is deactivated, the external SD card remains deactivated after a factory reset.

Data protection	
SD card encryption	Activate encryption
Recovery password to unlock the protected SD card	Set recovery password

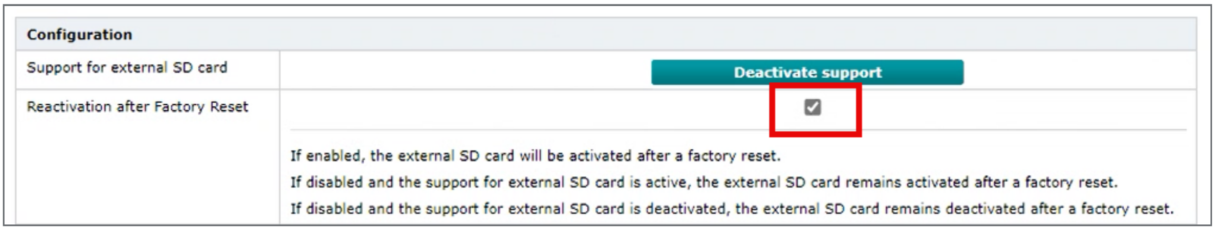
System Message	
Information	Attention: The support for the external SD card has been enabled. The full activation requires a system reboot
Warning	Use of external SD card requires physical protection of the device! Ensure that only authorized personal has access to the SD card! SD card contains sensitive private data which might be readable by persons accessing it.

↪ **Note** the system message at the bottom!



System Message	
Information	Attention: The support for the external SD card has been enabled. The full activation requires a system reboot
Warning	Use of external SD card requires physical protection of the device! Ensure that only authorized personal has access to the SD card! SD card contains sensitive private data which might be readable by persons accessing it.

- Enable the Reactivation after Factory Reset checkbox.



Configuration	
Support for external SD card	Deactivate support
Reactivation after Factory Reset	☑ If enabled, the external SD card will be activated after a factory reset. If disabled and the support for external SD card is active, the external SD card remains activated after a factory reset. If disabled and the support for external SD card is deactivated, the external SD card remains deactivated after a factory reset.

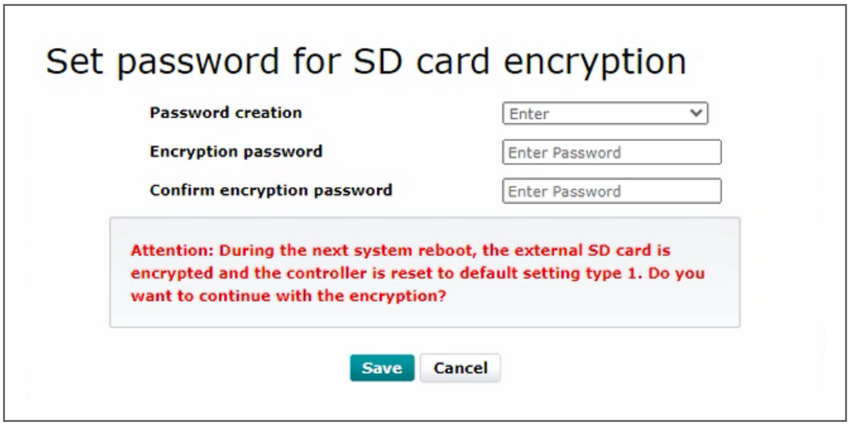
- Proceed with encrypting the SD card as described below.

> **Note:** When using the external SD card under the Security Profile, **encryption is mandatory**! Proceed with the steps in the next section.

Encrypting the SD card

> **Note:**
>
> - During the encryption or decryption process a *reset to default settings type 1* needs to be performed; the data on the SD card is deleted but the IP address setting is retained.
> - The following steps need to be done in exactly this order. Do not skip a step, do not do anything else in between with your device!

- Make sure to have a proper LIC SD card in the slot.
- In the Data protection section on the SD Card WBM page, click on Activate encryption to prepare the SD card encryption.
  ↪ The Set password for SD card encryption dialog opens.



Set password for SD card encryption

Password creation: Enter

Encryption password: Enter Password

Confirm encryption password: Enter Password

Attention: During the next system reboot, the external SD card is encrypted and the controller is reset to default setting type 1. Do you want to continue with the encryption?

- Here you can assign a password or have one generated automatically:

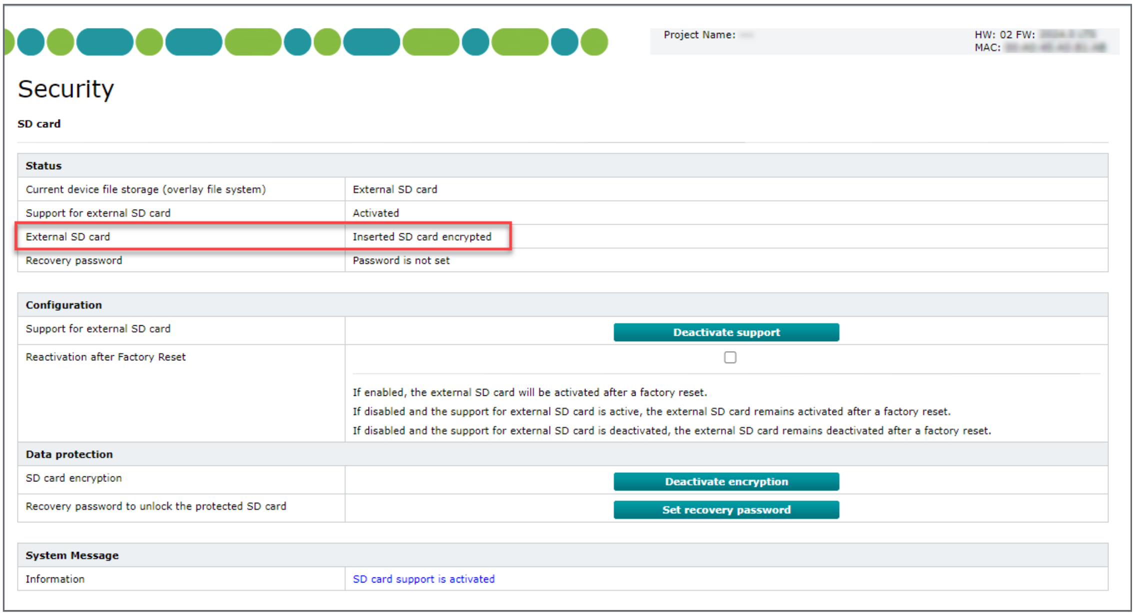
  Option 1: Enter your own password

  - From the Password creation drop-down menu, select Enter.
  - Prepare a password that meets the requirements.
  - Enter the same password in the Encryption password and Confirm encryption password input fields.

  Option 2: Generate a password

  - Select **Generate** from the Password creation drop-down menu.
    ↪ A password that meets the requirements is generated automatically.
- Store a note of the password used with this SD card (identifiable by the serial number on the back side) in a safe place.
- Click on Save.
  ↪ The encryption password is saved on the controller and the SD card encryption is scheduled for execution.
  ↪ In the Status section of the SD Card WBM page you can read now: *Encryption request present*.
- Reboot the controller (e.g., via the Cockpit WBM page).
  ↪ The SD card is encrypted and bound to the controller.
  Note: Due to the encryption, this step may take some time.
  ↪ The PLCnext Control is *reset to default setting (type 1)*.
  ↪ The controller boots from the encrypted SD card.
- Refresh the SD Card WBM page in your browser to see the changed status:

  WBM page as of firmware release >= 2024.0 LTS on controllers with an optional SD card:



Project Name: [redacted]

HW: 02 FW: [redacted]
MAC: [redacted]

Security

SD card

Status	
Current device file storage (overlay file system)	External SD card
Support for external SD card	Activated
External SD card	Inserted SD card encrypted
Recovery password	Password is not set

Configuration	
Support for external SD card	Deactivate support
Reactivation after Factory Reset	□ If enabled, the external SD card will be activated after a factory reset. If disabled and the support for external SD card is active, the external SD card remains activated after a factory reset. If disabled and the support for external SD card is deactivated, the external SD card remains deactivated after a factory reset.

Data protection	
SD card encryption	Deactivate encryption
Recovery password to unlock the protected SD card	Set recovery password

System Message	
Information	SD card support is activated

Setting the recovery password

You need a recovery password if you want to use an encrypted LIC SD card with another controller to which the LIC SD card is not bound, for example if a controller needs to be replaced. The recovery password corresponds to the encryption password with which the LIC SD card was originally encrypted.

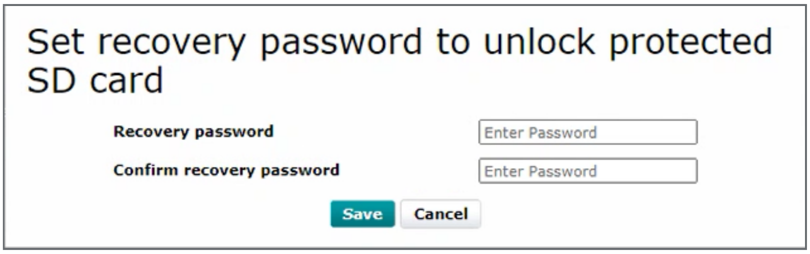
If a LIC SD card is encrypted and therefore bound to a specific controller, an encryption password has been set. The recovery password corresponds to that encryption password. To use the encrypted LIC SD card with another controller, you have to set its recovery password in the WBM of this controller. With the set recovery password, the LIC SD card is unlocked during the next reboot of the controller.

To unlock and use the protected LIC SD card with another controller (e.g., after replacing the controller due to a defect), you have to set its recovery password in the WBM of that controller, too. Only this way the LIC SD card can be unlocked during the next reboot of that controller.

Assigning the recovery password

You can assign the recovery password in the **Recovery password to unlock the protected SD card** area:

- Click on **Set recovery password**.
  ↪ The **Set recovery password to unlock protected SD card** dialog opens.

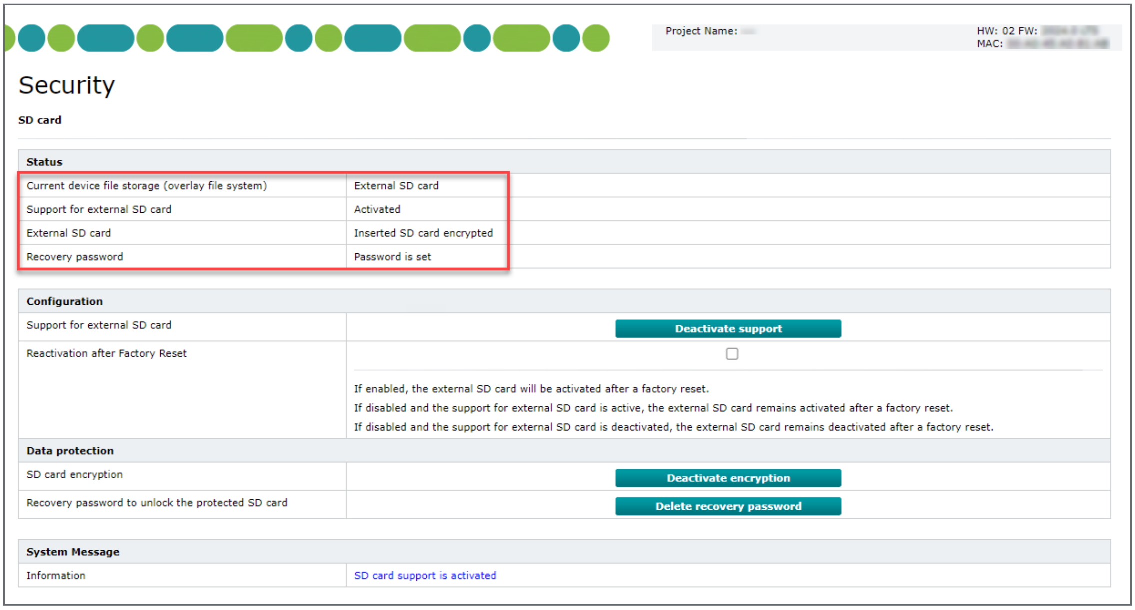


Set recovery password to unlock protected SD card

Recovery password	Enter Password
Confirm recovery password	Enter Password

- Enter the password in the **Recovery password** and **Confirm recovery password** input fields and click on **Save**.
  ↪ The password is stored in the controller.
  ↪ During a reboot this LIC SD card will be proven eligible for this controller.
- For further reference, store this password along with an identification (e.g., serial number) of the SD card and the controller in a safe place.
- Refresh the **SD Card** WBM page in your browser to see the changed status:

  WBM page on controllers with an optional SD card:



Project Name: [redacted]

HW: 02 FW: [redacted]
MAC: [redacted]

Security

SD card

Status	
Current device file storage (overlay file system)	External SD card
Support for external SD card	Activated
External SD card	Inserted SD card encrypted
Recovery password	Password is set

Configuration	
Support for external SD card	Deactivate support
Reactivation after Factory Reset	☐ If enabled, the external SD card will be activated after a factory reset. If disabled and the support for external SD card is active, the external SD card remains activated after a factory reset. If disabled and the support for external SD card is deactivated, the external SD card remains deactivated after a factory reset.
Data protection	
SD card encryption	Deactivate encryption
Recovery password to unlock the protected SD card	Delete recovery password

System Message	
Information	SD card support is activated

::

Port list

PLCnext Security Profile standard

Description	Protocol	Port
Common remoting, e.g. via PLCnext Engineer	TCP	Port 41100
HTTPS, Proficloud, eHMI (web server for eHMI and WBM)	TCP	Port 443

PLCnext Security Profile activatable

When components are switched on, further ports are enabled:

Description	Protocol	Port
NTP (Network Time Protocol)	UDP	Port 123
Common remoting, e.g. via PLCnext Engineer	TCP	Port 41100
SSH connections, e.g. for secure shell connection or SFTP connection	TCP	Port 22
HTTPS, Proficloud, eHMI (web server for eHMI and WBM)	TCP	Port 443
OPC UA®	TCP	Port 4840
MATLAB®/Simulink® in External Mode	TCP	Port 17725
SNMP (Simple Network Management Protocol)	TCP	Port 161
PROFINET unicast/multicast ports	UDP	Ports 34962 - 34964
PROFINET device ports	UDP	Ports 49152 - 65535
Syslog	TLS	Port 6514

PLCnext roles and rights list

User roles and their assigned access permissions in the various applications

The following overview shows the user roles implemented in the firmware and their access permission for different purposes. Some user roles have been introduced only with recent firmware updates.

Note: User roles that are not mentioned in a table do not have any access permission in the regarding context.

Web-based Management (WBM)

> **Note:** Visibility of WBM pages depends on the device and firmware release in use.
> In addition, some WBM pages could have been deactivated by settings in the System Services.

		User role										
WBM pages	**Access permission for:**	Admin	SecurityAdmin	SecurityAuditor	CertficateManager	UserManager	Engineer	Commissioner	Service	DataViewer	DataChanger	Viewer
Information or **Overview** section	General Data	√	√	√	√	√	√	√	√	√	√	√
	Network configuration	√			√	√	√	√	√	√	√	√
	Cockpit	√	√	√	√ [1]	√ [1]	√ [2]	√ [2]	√ [2]	√ [1]	√ [1]	√ [1]
Diagnostics section	PROFINET	√	√	√	√	√	√	√	√	√	√	√
	Local Bus	√	√	√	√	√	√	√	√	√	√	√
	Notifications	√	√	√	√	√	√	√	√	√	√	√
	Integrated UPS	√	√	√	√	√	√	√	√	√	√	√
Configuration section	Network - LAN Interfaces tab	√	√	√ **read-only**			√ **read-only**	√ **read-only**	√ **read-only**			
	Network - Netload Limiter tab	√	√	√ **read-only**			√	√ **read, reset**	√ **read, reset**			
	Date and Time [3]	√	√	√ **read-only**	√ **read-only**	√ **read-only**	√ **read-only**	√ **read-only**	√ **read-only**	√ **read-only**	√ **read-only**	√ **read-only**
	System Services	√	√									
	PLCnext Store	√	√									
	Proficloud (legacy platform)	√										
	Proficloud Services (V3 platform)	√	√									
	SPLC	√	√				√		√			
	Fan Control	√	√									
	Web Services	√	√									

		User role										
WBM pages	**Access permission for:**	Admin	SecurityAdmin	SecurityAuditor	CerficateManager	UserManager	Engineer	Commissioner	Service	DataViewer	DataChanger	Viewer
Security section	Security Profile	√	√									
	User Authentication	√	√			√						
	LDAP configuration	√	√			√						
	Firewall	√	√									
	SD Card	√	√									
	Certificate Authentication	√	√		√							
	Syslog Configuration	√	√									
Administration section	Firmware Update	√	√									
	PLCnext Apps	√	√				√					
	License Management	√	√									

[1] *These user roles can only change the user password.*

[2] *These user roles cannot reboot or reset.*

[3] *These user roles can access the Date and Time page with "read-only" rights:*

- *FileReader*
- *FileWriter*
- *EHmiLevel1 to EHMILevel10*
- *EHmiViewer*
- *EHmiChanger*
- *SoftwareUpdate*
- *SafetyEngineer*
- *SafetyFirmwareUpdater*

PLCnext Engineer

All unreported roles in this table do not have access permissions for PLCnext Engineer.

		User role										
PLCnext Engineer	**Access permission for:**	Admin	SecurityAdmin	Engineer	Commissioner	Service	DataViewer	DataChanger	Viewer	EHmiViewer	EHmiChanger	SafetyEngineer
PLCnext Engineer user interface	View values in the cockpit (e.g., utilization)	√	√	√	√	√	√	√	√			
	Transfer a project to the controller	√		√	√							
	Start (cold/warm restart) or stop the controller	√		√	√	√						
	Restart the controller (reboot)	√										
	Reset the controller to default setting type 1	√										
	View online variable values	√	√	√		√	√	√	√			
	Overwrite variables	√		√		√						
	Set and delete breakpoints	√		√		√						
	Download safety-related programs to the controller	√		√ [4]								√ [5]
	Start or stop safety-related programs	√		√ [4]								√ [5]
	Debug safety-related programs	√		√ [4]								√ [5]
PLCnext Engineer HMI application	View online variable values	√	√							√	√	
	Overwrite variables	√									√	

[4] *As of firmware 2023.0 LTS, safety permissions for the Engineer user role are always enabled. As of the firmware 2023.0.1 LTS hotfix: if the Security Profile is enabled, safety permissions for the Engineer user role are disabled. If needed, use the SafetyEngineer user role in addition. See detailed description of combined safety user roles.*

[5] *Do not use this user role alone. This role is designed for use as an add-on to other user roles, e.g. Engineer. See detailed description of combined safety user roles.*

Applications and services

All unreported roles in this table do not have access permissions for the mentioned applications and services.

Note: Additional roles may be necessary, e.g. for use with the Device and Update Management.

		User role										
Application or service	**Access permission for:**	Admin	SecurityAdmin	Engineer	Service	DataViewer	DataChanger	Viewer	FileReader	FileWriter	SoftwareUpdate	SafetyFirmwareUpdater
SD card, parameterization memory	SFTP access to the file system with an SFTP client [6]	√										
Shell	SSH access to the shell [6]	√										
By means of dedicated tools	Update safety-related firmware on the controller	√										√
OPC UA® access by means of a client application	View online variable values	√	√	√	√	√	√	√				
	Overwrite variables	√		√	√		√					
	Read files (OPC UA file transfer must be enabled via PLCnext Engineer)	√							√			
	Write files (OPC UA file transfer must be enabled via PLCnext Engineer)	√								√		
	Update firmware on the controller	√									√	
Device and Update Management (DaUM)	Update firmware, software and projects	√										

[6] *Authentication with a user name and password is **always** required for SSH or SFTP access, even if user authentication is disabled.*

OPC UA® security compliance list

Note: If the Security Profile is activated, you must always use *sign & encrypt*.

OPC UA® Server

Profile: Embedded 2017 UA Server

Facets:

- Global Certificate Management Server Facet
- User Token - User Name Password Server Facet

SecurityPolicy:

Availableas sign and as sign & encrypt:

- Basic256Sha256
- Aes128-Sha256-RsaOaep
- Aes256-Sha256-RsaPss

OPC UA® Client

Profile: Minimum UA Client Profile

SecurityPolicy:

Availableas sign and as sign & encrypt:

- Basic256Sha256
- Aes128-Sha256-RsaOaep
- Aes256-Sha256-RsaPss

OpenSSL

Note: The OPC UA client and server use the OpenSSL library to validate X.509 certificates using the OpenSSL flag `X509_V_FLAG_X509_STRICT` . As firmware 2024.0 LTS is updated to OpenSSL 3.0, the X.509 certificate validation became more strict, especially for non self-signed certificates. This may cause the server to return the error `BadSecurityChecksFailed` on client connection attempts. Make sure that, according to OPC UA Part 6, client issuer as well as client application X.509 certificates are conform to **RFC 5280**, especially to the sections listed below. The same applies for user-managed server certificates.

- 4.1.1.2 signatureAlgorithm
- 4.1.2.6 Subject
- 4.2.1.1 Authority Key Identifier
- 4.2.1.2 Subject Key Identifier
- 4.2.1.3 Key Usage
- 4.2.1.6 Subject Alternative Name
- 4.2.1.9 Basic Constraints

Appendix

Appendix

In the appendix you find the following contents:

- Integrity check of downloaded software or firmware files: IEC 62443 requires mandatory integrity check of software or firmware downloaded via Internet against tampering attacks.
- Industrial Security application note: To achieve security in general, basic security measures need to be fulfilled. The Industrial Security application note contains information on handling components, solutions and PC based software.
- List of abbreviations

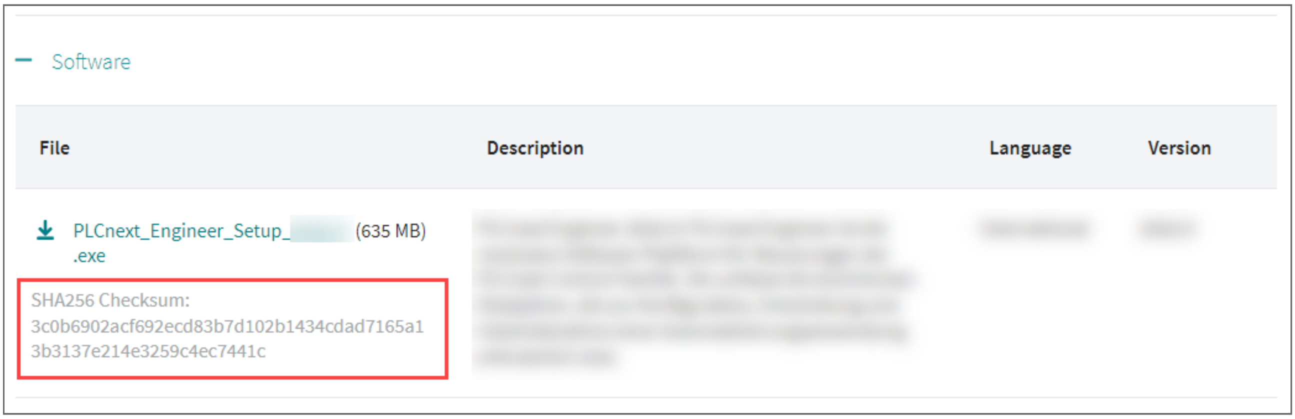
Integrity check of downloaded software or firmware files

IEC 62443 requires mandatory integrity check of software or firmware downloaded via Internet against tampering attacks.

After downloading a setup file for any application (Windows®/Linux), a firmware file for a controller from the Internet or a PLCnext Technology App from the PLCnext Store, prior to its installation you must verify that the file has not been corrupted or tampered. To do this, copy the published checksum string for the file before downloading the file from the provider's website, and save it to a plain text file.

Note: In the download section at relevant products on the Phoenix Contact website, a SHA256 checksum is specified for each downloadable software or piece of code.

Example for PLCnext Engineer by Phoenix Contact

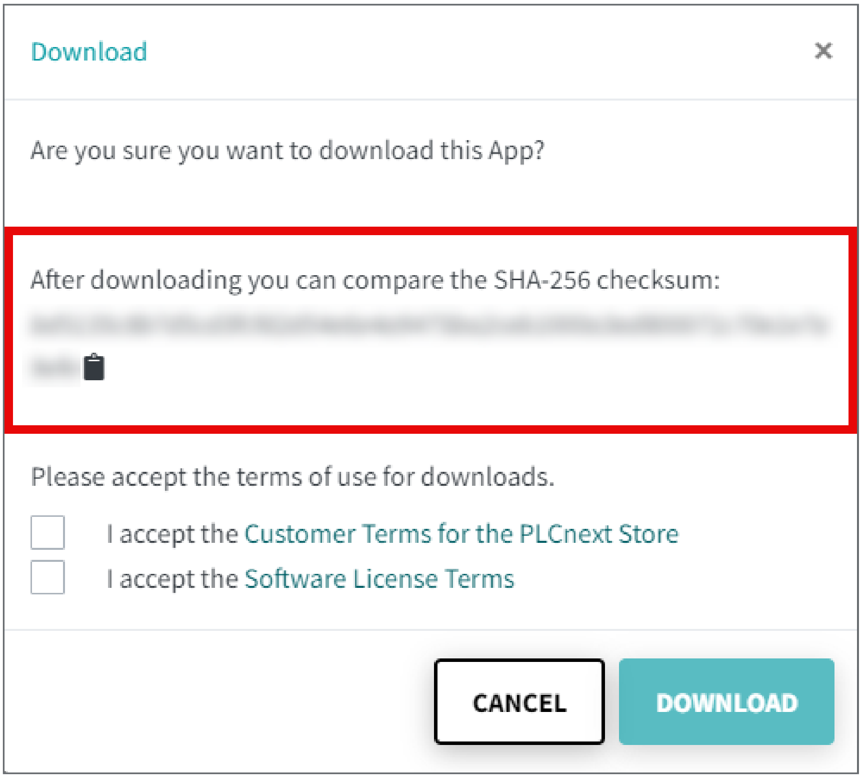


− Software

File	Description	Language	Version
PLCnext_Engineer_Setup_[redacted] (635 MB) .exe SHA256 Checksum: 3c0b6902acf692ecd83b7d102b1434cdad7165a13b3137e214e3259c4ec7441c	[redacted]	[redacted]	[redacted]

After downloading the setup file, use a suitable tool (such as 7-Zip) to calculate a SHA256 checksum over the downloaded file. If the calculated SHA256 checksum is identical with the checksum published by the provider, you can execute the software setup file, or you can install the firmware on the controller.

Example for a PLCnext Technology App from the PLCnext Store



Download ×

Are you sure you want to download this App?

After downloading you can compare the SHA-256 checksum:

Please accept the terms of use for downloads.

□ I accept the Customer Terms for the PLCnext Store

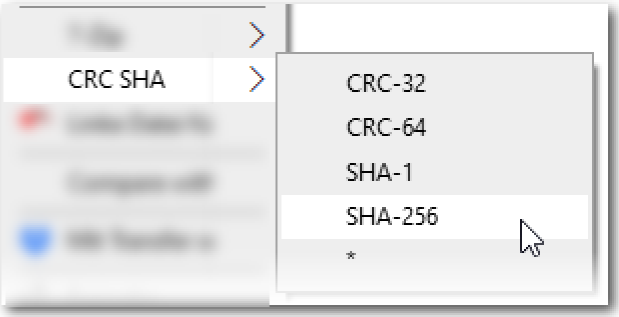
□ I accept the Software License Terms

After downloading the PLCnext Technology App, compare the SHA-256 checksum from the download dialog.

If the SHA-256 checksum is identical, the PLCnext Technology App can be executed.

Example using 7-Zip on Windows

- With 7-Zip installed, right-click the downloaded file in the file explorer; for *.zip* files, do not unzip before checking.
- Select the context menu entry CRC SHA → SHA-256 .



- Let 7-Zip calculate a checksum for the file, then copy that checksum under the one you picked from the provider's website and compare them. They need to be identical in each character.
- If the calculated SHA-256 checksum is identical, you can execute the software setup file, or you can install the firmware on the controller.

Industrial Security application note

To achieve security in general, basic security measures need to be fulfilled. The Industrial Security application note contains information on handling:

- Components
- Solutions
- PC based Software

It contains generic information how to protect components, networks, and systems against unauthorized access, and how to ensure the integrity and authenticity of data.

We strongly recommend using an **Information Security Management System** (ISMS) to manage all the technical, organizational, and personnel measures that are needed to ensure compliance with information security directives.

No matter if PLCnext Control devices are used as IEC 62443-4-1 / 4-2 certified components or in context with other security concepts, the measures described in this **PLCnext Security Info Center** and the Industrial Security application note should be considered.

Read more:

- Phoenix Contact Security Guideline– on this platform
- PLCnext Security Guideline – on this platform
- Industrial Security application note – current revision in the right panel of the Phoenix Contact Product Security Incident Response Team (PSIRT) website

List of abbreviations

CA	Certification Authority
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DMZ	Demilitarized Zone
FR	Foundational Requirement
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control System
ISMS	Information Security Management System
IT	Information Technology
NAT	Network Address Translation
OT	Operational Technology
PAT	Port and Address Translation
PKI	Public Key Infrastructure
PSK	Pre-shared Key
SPLC	Left-alignable, safety-oriented control for operating PROFIsafe® devices
SPLCProxy	A layer that is providing security extensions, dedicated safety roles and file system access rights to protect the SPLC (see Security and safety hardening).
SR	System Requirements
TLS	Transport Layer Security
VPN	Virtual Private Network

Phoenix Contact Security Advisories (PSIRT)

The **Phoenix Contact Product Security Incident Response Team (PSIRT)** gathers and analyzes any potential security vulnerabilities in Phoenix Contact products, solutions, and services. If a security vulnerability is identified, it will be listed on the PSIRT website under “Recent security advisories”, and a corresponding security advisory will be published. The website is updated periodically.

To stay up to date, Phoenix Contact recommends subscribing to the PSIRT newsletter (listed in the **SERVICE** box, under “Subscribe to PSIRT news”).

Anyone can submit information on potential vulnerabilities to Phoenix Contact PSIRT via email.

The aim of PSIRT is to work with vulnerability reporters professionally to handle any vulnerability claim that is related to Phoenix Contact products, solutions and services.

Legal information and imprint

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Copyright and licensing information

Copyright

This platform, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

Licensing information on open source software

Controllers of the PLCnext Control product family work with a Linux operating system.
All license information can be called using the “Legal Information” link on every page of the Web-based Management (WBM) on every PLCnext Control:

- Click on the “Legal Information” link on the bottom left of the WBM page.
  Licenses for all of the open source software used are shown.

How to contact us

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at phoenixcontact.com

Make sure you always use the latest documentation that is available for your products. It can be downloaded at phoenixcontact.net/products.

Our subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary. The subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

PLCnext Technology -
Security Info Center
Revision 017 | 2025