Siemens
Industry
Online
Support

APPLICATION EXAMPLE

WinCC OA Blueprint for a Waste Water Treatment / Water Treatment Plant

Guideline for Secure Configuration

SIEMENS

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

Abbreviations **6**

1. Preface **7**

2. Security Strategies **8**

2.1. IEC 62443 Overview 8

2.2. Defense-In-Depth Concept 10

2.2.1. Plant Security 10

2.2.2. Network Security 11

2.2.3. System Integrity 11

2.3. Blueprints for Reference architectures in Water and Wastewater 12

3. Blueprint – Wastewater Treatment Plant **13**

3.1. Process Description 13

3.1.1. Mechanical Treatment 13

3.1.2. Biological Treatment 14

3.1.3. Sludge Treatment 15

3.1.4. Sewer System 15

3.2. System Architecture 16

3.2.1. System Components of the Blueprint Water 16

3.3. Zones and Intended Operational Environment 20

3.3.1. Central Control Room 20

3.3.2. Engineering Room 20

3.3.3. Server Room 20

3.3.4. Control System Network 20

3.3.5. Application Bus 21

3.3.6. Demilitarized Zone (DMZ) / Perimeter Network 21

3.3.7. Process Control Network 21

3.3.8. Controller Cabinets 21

3.3.9. WLAN Access 21

3.3.10. External Pump Station, Medium – Remote Station 21

3.3.11. Well Service Water – Remote Station 22

3.3.12. Storm Water Tank 1 – Remote Station 22

3.3.13. External Pump Station, Small – Remote Station 22

3.3.14. External Metering Station – Remote Station 22

3.3.15. Storm Water Tank 2 – Remote Station 22

3.3.16. External Zones 22

3.4. Data Exchange between zones 23

4. Protection Goals 24
4.1. Physical access 25
4.2. Power supply system 26
4.3. Firewall 26
4.4. Internal & organizational measures 26

5. Security Measures 27
5.1. Secure Network Design 27
5.1.1. Network Segmentation 27
5.1.2. Zone Boundary Protection 27
5.1.3. Network Access Protection 28
5.1.4. Administration of Network Devices 28
5.1.5. Protection Measures Against Denial-of-Service 29
5.2. Identity and Access Management 29
5.2.1. Authentication Mechanisms for Users and Components 30
5.2.2. Management of Identifiers and Credentials 31
5.2.3. Account Management and Configuration of Access Rights and Privileges 32
5.2.4. Control of Access via Untrusted Networks (Remote Access) 32
5.3. Attack Surface Reduction 33
5.3.1. Least Functionality 33
5.4. Secure Channels and Encryption 33
5.4.1. Secure Channels 33
5.4.2. Sensitive Data 33
5.5. System Integrity Protection 34
5.5.1. Software and Information Integrity 34
5.5.2. Security Functionality Verification 34
5.5.3. Input & Output Validation and Error Message Sanitization 34
5.5.4. Support for Control System Backup and Recovery 35
5.5.5. Time Distribution and Synchronization 35
5.6. Security Logging and Monitoring 36
5.6.1. Monitoring Access from Untrusted Zones 36
5.6.2. Logging of Security-Related Events 36
5.6.3. Audit trail 37

6. Hardening and Configuration of the System Components 38
6.1. Assumptions 38
6.2. Firewalls for Secure Communication Between the Zones 38
6.2.1. Palo Alto 440 NGFW 39
6.2.2. SCALANCE Network Security Devices 41
6.3. Network Components for Wireless Communication 45

6.4. Network Components SCALANCE XC and XF 47
6.5. TeleControl TIM 1531 IRC 48
6.6. TeleControl RTU3051C 48
6.7. Industrial Ethernet CP 1543-1 49
6.8. Central Plant Clock 51
6.9. Workstations and Server 51
6.9.1. General Hardening Measure for Workstation and Server 51
6.9.2. Additional Hardening Measures 52
6.9.3. Hardening Measures for SINEC NMS 52
6.9.4. Hardening Measures for PM ANALYZE 53
6.9.5. Hardening Measures for SIMATIC Energy Manager Pro 53
6.10. Automation Devices SIMATIC S7-1500 / S7-1200 54

7. User Management 57
7.1. Domain Controller 57
7.2. User Management Component 57
7.2.1. UMC Ring Server 57
7.3. User Authentication and Authorization for WinCC OA 57
7.3.1. Benefits of using Active Directory for user authentication 58

8. Malware Protection and Application Control 59

9. Patch Management 60
9.1. Patch Management for WinCC OA Components 60
9.2. Patch Management of Automation and Network Components 60

10. Backup and Recovering 61

11. Optional Security Measures 62
11.1. Threat Prevention Subscription for Font- and Back-Firewalls 62

12. Links and Literature 64

13. Attachment – List of security measures according to IEC 62433-3-3 67

14. Appendix 77
14.1. Service and support 77

Abbreviations

ADSL	Asymmetric Digital Subscriber Line
ATV	Abwassertechnische Vereinigung
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol
EPS	Endpoint Security
GSM	Global System for mobile network
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAD	Industrial Anomaly Detection
IPSec	Internet Protocol Security
IWLAN	Industrial Wireless Local Area Network
PPTP	Point-To-Point Tunneling Protocol
KVM	Keyboard Video Mouse
L2TP	Layer Two Tunneling Protocol
NMS	Network Management System
RADIUS	Remote Access Dial In User Service
RDP	Remote Desktop Protocol
PLC	Programmable Logic Controller
RTC	Real Time Clock
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information Event Management
SPAN	Switched Port Analyser – mirror port
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TPS	Threat Prevention Subscription
TRA	Threat and Risk Analysis
UMC	User Management Component
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WinCC OA	SIMATIC WinCC Open Architecture
WSUS	Windows Server Update Service
WWTP	Wastewater Treatment Plant

1. Preface

This documentation is intended to help system integrators to setup a water plant more securely.

As a distinctly open SCADA system, SIMATIC WinCC Open Architecture (WinCC OA) can be flexibly adapted to a wide range of customer needs. The system software provides the configuration engineer with a great deal of freedom in terms of project configuration, as well as in the design of the business logic and visualization.

Experience has shown that subsequent modernization or plant expansion work is made much easier if the automation project is configured "in conformance with SIMATIC WinCC Open Architecture (WinCC OA)" as far as possible right from the start. This means users must adhere to certain basic rules to ensure that the provided system functions will offer optimum usability in the future.

This manual serves as a compendium in addition to the product documentation for SIMATIC WinCC Open Architecture (WinCC OA) and the automation devices. The basic steps for project creation and parameter assignment are described in the form of instructions.

The guideline directly reflects the recommended methodology (Defense-in-depth concept in accordance with IEC 62443), which is based on the results of a great deal of practical experience. The description relates to working with the project and the parameter settings of the components it contains but not the application itself.

2. Security Strategies

Faced with a growing number of attacks (e.g. malware, unauthorized access, denial of service, manipulation of data etc.), securing automation and IT systems against attacks and manipulation is a top priority in almost every plant and project. Additionally, with digitalization as a major industry trend, the number of networked systems and hence, the number of potential weaknesses, will continue to grow.

Plant engineers and operators need to set a high priority to protect the automation and control systems against manipulation and malware to fulfill availability, quality and national and international standard requirements.

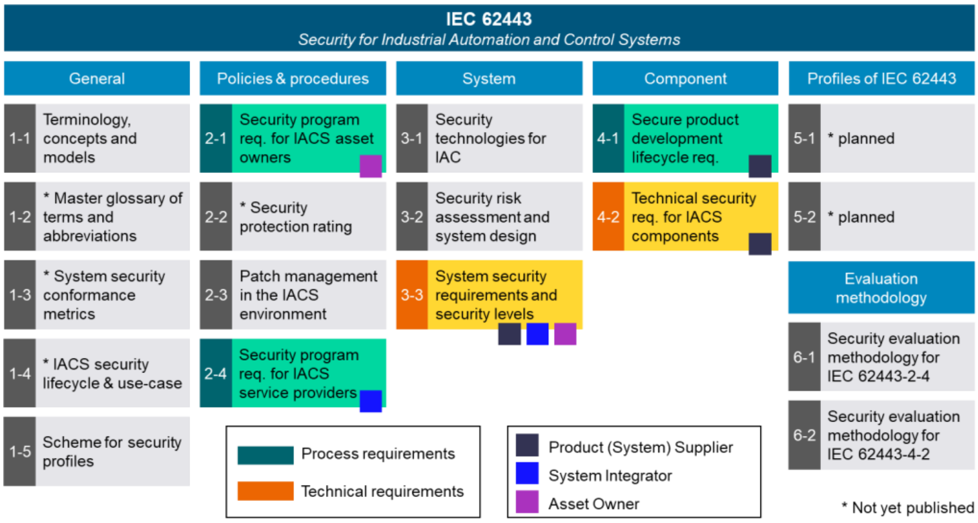
Due to the enormous variety of attacks and the complexity in the process industry, it is often not easy to identify risks and threats and to adapt the right security strategy.

Having good, regular and well secured backups, a good cybersecurity strategy including isolating critical systems, using appropriate software, having the latest security patches installed and having well security trained staff is essential.

2.1. IEC 62443 Overview

Industrial security as specified in recent guidelines should be treated as a lifecycle concern. To fully address the need for more secure systems, plant owners must consider all phases of the solution lifecycle, from the development of systems to their eventual replacement. The IEC 62443 series of standards considers the lifecycle as consisting of five phases: product or system development, specification, integration and commissioning, operations and maintenance and decommissioning. An overview of the standard is shown in the following figure:

Figure 2-1: Overview of IEC 62443



IEC 62443

Security for Industrial Automation and Control Systems

General	Policies & procedures	System	Component	Profiles of IEC 62443
1-1 Terminology, concepts and models	🟩 2-1 Security program req. for IACS asset owners 🟪	3-1 Security technologies for IAC	🟩 4-1 Secure product development lifecycle req. ⬛	5-1 * planned
1-2 * Master glossary of terms and abbreviations	2-2 * Security protection rating	3-2 Security risk assessment and system design	🟧 4-2 Technical security req. for IACS components ⬛	5-2 * planned
1-3 * System security conformance metrics	2-3 Patch management in the IACS environment	🟧 3-3 System security requirements and security levels ⬛ 🟦 🟪		Evaluation methodology
1-4 * IACS security lifecycle & use-case	🟩 2-4 Security program req. for IACS service providers 🟦			6-1 Security evaluation methodology for IEC 62443-2-4
1-5 Scheme for security profiles				6-2 Security evaluation methodology for IEC 62443-4-2

🟩 Process requirements
🟧 Technical requirements

⬛ Product (System) Supplier
🟦 System Integrator
🟪 Asset Owner

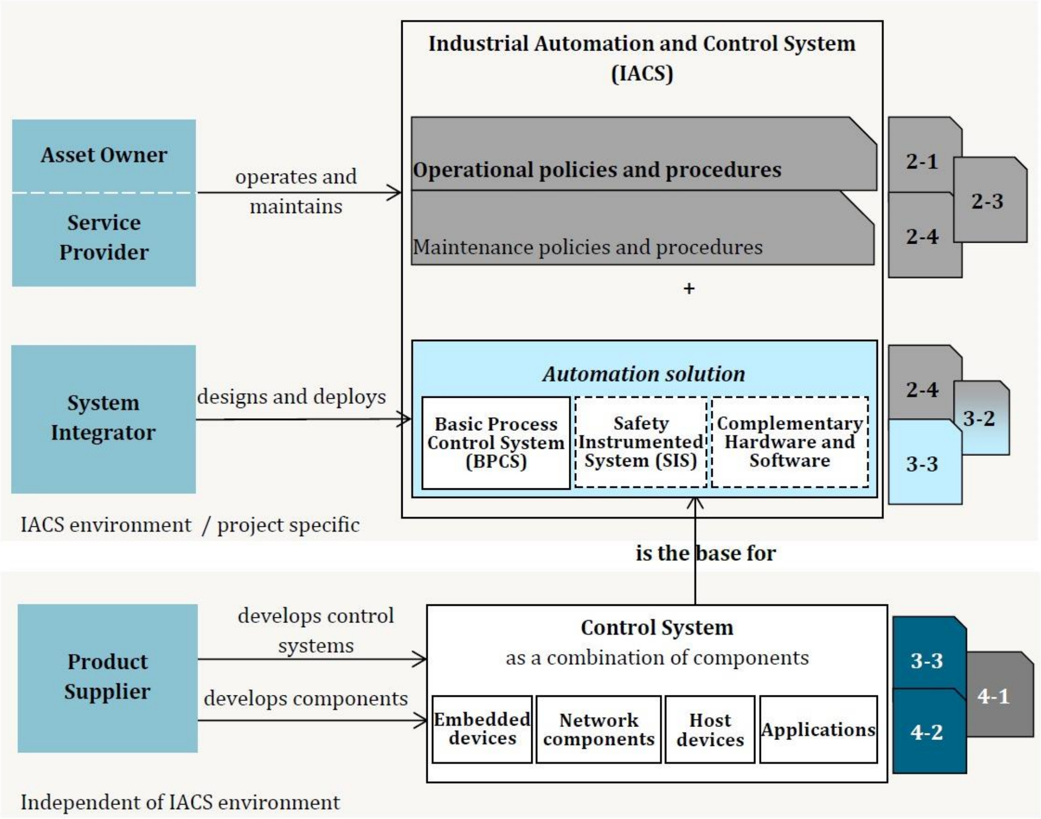
* Not yet published

There is clear accountability and a primary objective associated with each of these phases and security topics have to be coordinated and communicated between different roles and stakeholders (Figure 2-2):

- Product suppliers implement security measures, such as authentication, secure communication capabilities, or robust communication stacks in the components, as part of the product development process (e.g. IEC 62443 part 4-1)
- System integrators provide a secure design that matches the requirements resulting from exposure, threats, impacts, and the physical and technical operational environment as provided by the plant owner. The system integrator also defines and applies the secure configuration as well as performs verification and validation. System integrators need security information for the components from the product, e.g. how to configure the components securely.
- Plant owners address secure operation and maintenance, for example dealing with user management and handling of credentials, and with regular security patching.

These roles need to work together to obtain adequate security along the whole lifecycle of a system. Lack of adequate information, or different interpretation of security topics impedes the joint efforts of the various stakeholders.

Figure 2-2: Roles according IEC 62443

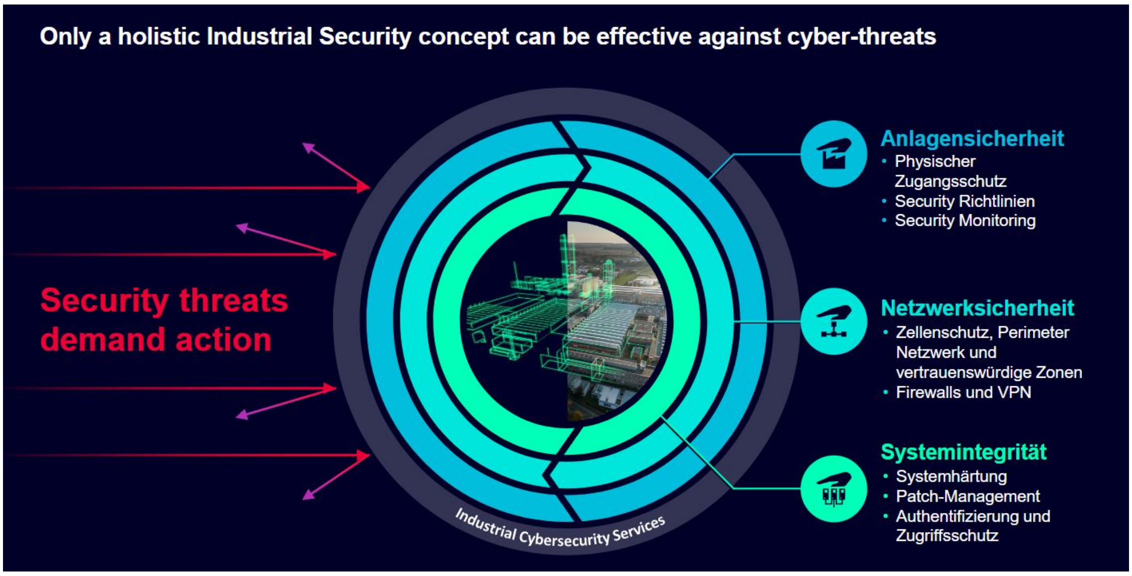

Industrial Automation and Control System (IACS)
Asset Owner
Service Provider
operates and maintains
Operational policies and procedures
Maintenance policies and procedures
2-1
2-3
2-4
+
System Integrator
designs and deploys
Automation solution
Basic Process Control System (BPCS)
Safety Instrumented System (SIS)
Complementary Hardware and Software
2-4
3-2
3-3
IACS environment / project specific
is the base for
Product Supplier
develops control systems
develops components
Control System
as a combination of components
Embedded devices
Network components
Host devices
Applications
3-3
4-1
4-2
Independent of IACS environment

2.2. Defense-In-Depth Concept

All-embracing protection of industrial facilities against cyberattacks must act on all levels at the same time, from the operational to the bay level, from access control to copy protection. The IEC 62443 recommend the Defense-in-Depth concept as a comprehensive protection scheme therefor.

The automation control system with Defense-In-Depth must be defended through multiple levels of security and action, meaning that the plant owners and solution providers must address varied and very different security issues. From plant security to network security up to system integration and organizational measures.

Figure 2-3: Defence-In-Depth



Only a holistic Industrial Security concept can be effective against cyber-threats

Security threats demand action

Anlagensicherheit

- Physischer Zugangsschutz
- Security Richtlinien
- Security Monitoring

Netzwerksicherheit

- Zellenschutz, Perimeter Netzwerk und vertrauenswürdige Zonen
- Firewalls und VPN

Systemintegrität

- Systemhärtung
- Patch-Management
- Authentifizierung und Zugriffsschutz

2.2.1. Plant Security

- Physical security measures:
  Control of physical access to spaces, buildings, individual rooms, cabinets, devices, equipment, cables and wires. The physical security measures must be based around the security cells and the responsible persons. It is also important to implement physical protection at remote single station systems.
- Organizational security measures:
  Security guidelines, security concepts, set of security rules, security checks, risk analyses, assessments and audits, awareness measures and training.

2.2.2. Network Security

- Division into security cells:
  A comprehensively secured network architecture subdivides the control network into different task levels.
  Perimeter zone techniques should be employed for this. This means that systems set up in the perimeter network (DMZ – Demilitarized Zone) are shielded by one or more firewalls (front firewall and back firewall or three-homed firewall) from other networks (e.g. Internet, office network). This separation enables access to data in the perimeter network without having to simultaneously allow access to the internal network to be protected (e.g. automation network). As a result, risks of access violations can be significantly reduced.

- Securing access points to the security cells:
  A single access point to each security cell (should be Implemented by a firewall) for authentication of users, employed devices and applications, for direction-based access control, for assignment of access authorizations, and for detection of intrusion attempts.
  The single access point functions as the main access point to the network of a security cell and serves as the first point of a control of access rights to a network level. i.e. the external pump station or storm water tank as indicated in the blueprint are dedicated security cells.

- Securing the communication between two security cells over an "insecure" network:
  Certificate-based, authenticated and secure communication should always be used when the perimeter zone technique is used and there is communication across the access points. Tunnel protocols such as L2TP (Layer Two Tunneling Protocol), IPSec (IPSecurity) and OpenSSL (Open Transport Layer Security (TLS) and Secure Sockets Layer (SSL) Protocol) can be used for this. Furthermore, communication is possible using protocols that are secured by server-based certificates, such as RDP (Remote Desktop Protocol) or a website published via HTTPS. In this case, communication takes place across the firewall using TLS (Transport Layer Security) or SSL (Secure Sockets Layer) technology.

2.2.3. System Integrity

- System hardening:
  Adjustments to a system to make it more resistant to attacks.

- User management and role-based operator authorizations:
  Task-based operation and access authorizations (role-based access control)

- Patch management:
  Patch management is the systematic procedure for installing updates on plant systems.

- Malware detection & prevention:
  Use of suitable and correctly configured virus scanners and whitelisting software

2.3. Blueprints for Reference architectures in Water and Wastewater

With all these requirements in mind, it is quite understandable that project teams can feel overwhelmed by the task to ensure adequate defense-in-depth security concepts for systems designed and deployed in an engineering project.

For each of these topics mentioned in section 0, there are plenty of technical solutions, tools, and best practices available – but project teams lack the time and expertise to choose a suitable solution for each security topic. Hence, it is a common pitfall to focus on some topics in depth, while overlooking others.

To facilitate security engineering and helping to avoid this pitfall, Siemens has developed several blueprints for automation and control systems. These blueprints provide guidance in form of references to specific resources and make sure that the engineering project produces all security documents prescribed by IEC 62443-2-4. Based on a standard solution using the WinCC OA SCADA system, the blueprints are designed to meet the requirements of a specific yet typical Water and Wastewater application.

3. Blueprint – Wastewater Treatment Plant

The blueprint represents the typical system architecture for a Wastewater Treatment Plant (WWTP) based on WinCC OA.

The blueprint architecture reflects also the configuration for a Water Treatment Plant (WTP).

The process parts are divided as follows for the different plant types:

Table 3-1 – Overview Plant Types

Waste Water Treatment Plant	Water Treatment Plant
Mechanical treatment	Raw water feed
Biological treatment	Filtration, wash- pure water
Sludge treatment	Sludge treatment, Neutr.

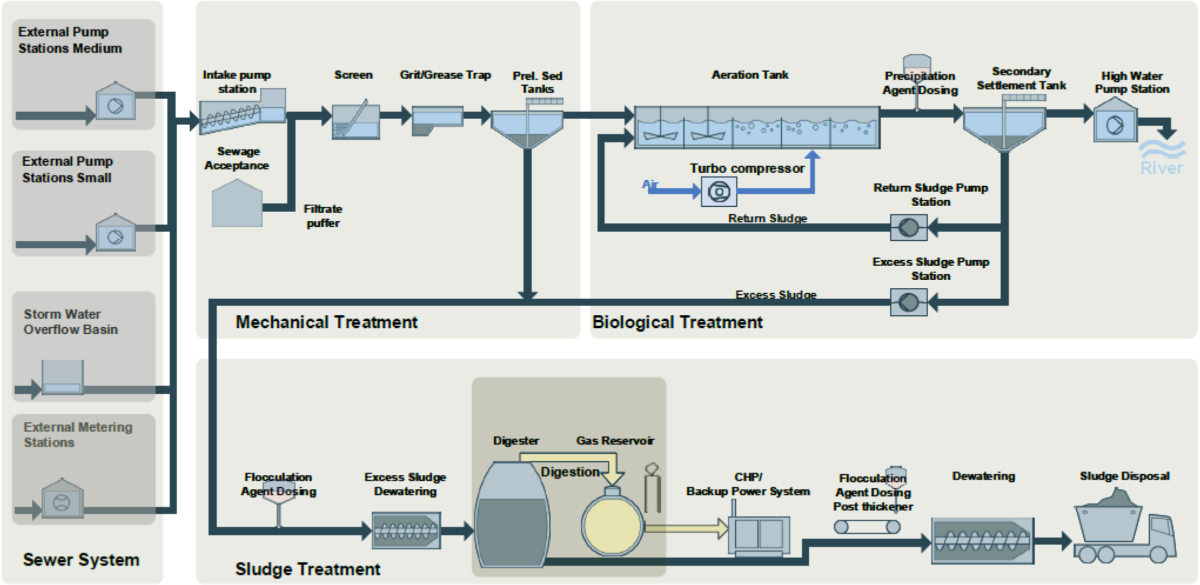
3.1. Process Description

A Wastewater Treatment Plant is collecting the sewage from appr. more as of 100 000 households and cleaning in different process steps the sewage in the way that the cleaned water can be re-use.

The process of the Wastewater Treatment Plant for the blueprint is shown in Figure 3-2.The process has the following main process parts:

- Mechanical treatment
- Biological treatment
- Sludge treatment
- Sewer System

Figure 3-1 – Process Overview



3.1.1. Mechanical Treatment

In this process part, the collected sewage is feed from the sewer system into the treatment plant and cleaned from coarse components and settle able contamination, e.g. sand, small stones or glass splinter.

The intake pump station is used for lifting the sewage coming from the sewer system to the mechanical treatment area of a Wastewater Treatment Plant. The screw or centrifugal pumps are controlled by the outlet flow of the intake pump station. These pumps ensure that the mechanical treatment is feeding by steady inlet flow for a higher process quality

The Screen removes coarse components from the sewage. The sewage is charged by the screening unit to a washing press. The washing press thickens the coarse components in the sewages and charges the screening into a container. The cleaned sewage is feed by a channel to the sand and grease trap

The grit / grease trap is used to remove coarse, settle able contamination from the sewage, e.g. sand, small stones or glass splinter. The sand / grease trap consists of a sedimentation tank and a scraper bridge with a chassis and a rake blade. Heavy, mineral solid (mainly sand) are settling on tank ground and undissolved grease and oil, swimming on the water surface are moved by a grease blade into a grease hod.

The primary sedimentation tank is used to separate further settling and swimming solids from the sewage. The sewage is flowing very slowly through the primary sedimentation tank. Thus, solids are settling on the ground of the tank.

3.1.2. Biological Treatment

Biological wastewater treatment process is used to remove any contaminants that left after the mechanical treatment.

The aeration tank is divided into two parts

- Denitrification tank
- The anoxic condition in the denitrification tank transduces nitrate into nitrogen and reduce the N-load of the sewage.
- Nitrification tank
- In the nitrification tank the organic load of the sewage is reduced by the use micro-organism. Therefor dissolved oxygen (DO) in the water is necessary. Turbo compressors are pumping air in the nitrification tank.

The secondary settlement tank is used to clean the water from the sludge. The sludge which is heavier as the water is sediment on the button of secondary settlement tank. A continuously rotating scraper move the excess sludge to a receiving tank. From the receiving tank return sludge pumps pump sludge back to the aeration tank. Excess sludge pumps pump the excess sludge to the sludge treatment.

Sludge which is lighter than water is swimming on the water surface and is collected by a floating sludge removal device mounted on the scraper and is pumped is pump to the sludge thickener.

The high-water pump station, if required is used to pump the cleaned water to a river.

3.1.3. Sludge Treatment

This process is used to manage and dispose of sewage sludge produced during sewage treatment. Sludge is mostly water with amounts of solid material removed from liquid sewage.

The sludge thickening is used to fill the digester with sludge. The sludge – primary or excess sludge – can be thickened in the sludge thickener before filling in the digester.

The digester is part of the sludge treatment of a Wastewater Treatment Plant. The anaerobe treatment of the sludge is used for stabilization of the sludge through the decomposition of organic content (solved or suspended). The emerging biogas is used for energy production because of its methane content.

The gas reservoir and the gas flare are part of the sludge treatment of a Wastewater Treatment Plant. The gas reservoir is used to store the biogas from the digester and to ensure a stable gas supply of the combined heat and power plant (CHP) and a heating system.

For dewatering, the sludge has to be conditioned, because of the strong adhesion of the water on the solid matters. A flocculation agent station is dosing flocculation agent controlled by the turbidity and the flow rate in the inlet of the decanter.

3.1.4. Sewer System

The sewer system is the intake station of the Wastewater Treatment Plant and feeds the plant with by using pump stations.

The external pump station is connected to the sewage channel. The sewage flows from the sewage channel into the mechanical preliminary treatment, where the coarse screen removes coarse components from the sewage. After the coarse screen the sewage flows into a sewage collection chamber. The external pump station is feeding the intake pump station of the Wastewater Treatment Plant.

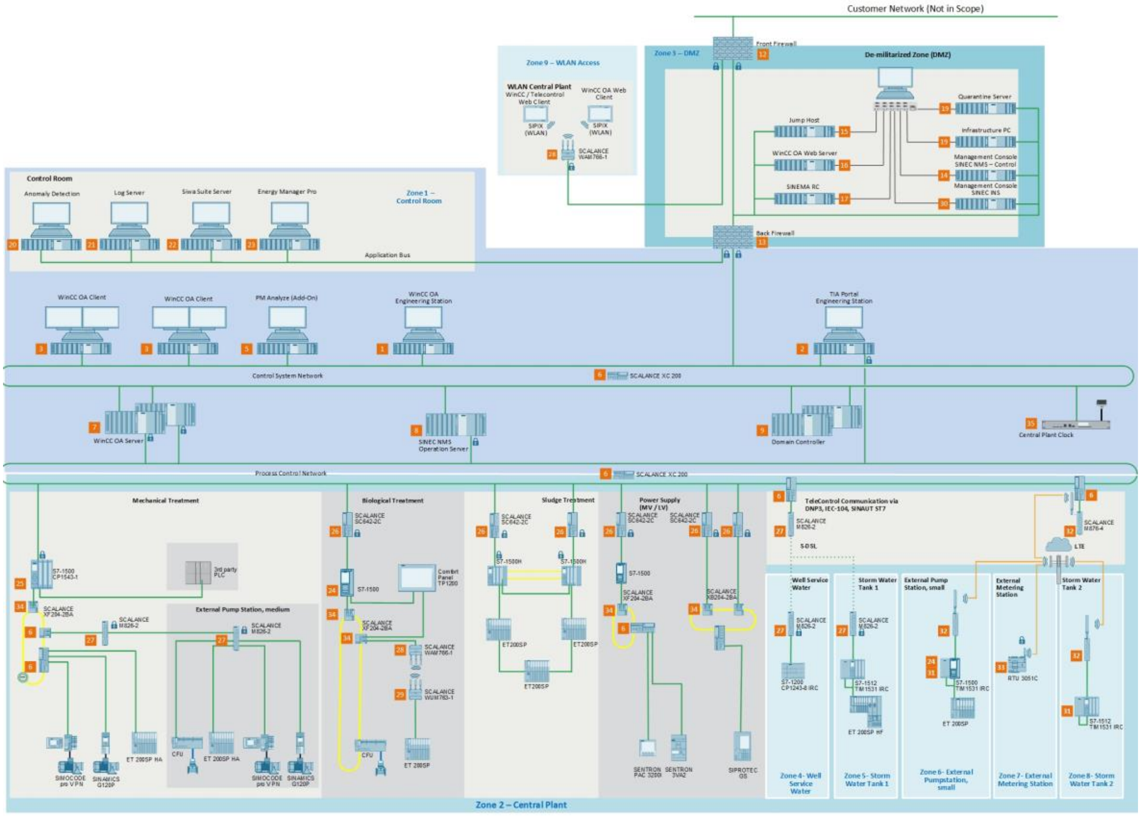
The storm water tank is connected to a sewage channel via an inlet overflow wall. In case of a heavy rain impact, the water/sewage mixture is flowing over a overflow wall into the storm water tank and reducing the load on the downstream sewage plant. After the heavy rain event, as soon as the flow through the sewage channel is normalized, the sewage mixture from the storm water tank is slowly returned to the sewage channel.

External Metering Station is used to measure the volume of water coming from residential and commercial buildings by a public Wastewater system.

3.2. System Architecture

The WinCC OA system architecture for the blueprint Wastewater Treatment Plant is shown in Figure 3-2

Figure 3-2 - WinCC OA System Architecture



3.2.1. System Components of the Blueprint Water

The IEC 62443 classifies the system components into three device types:

- Host / Application:
- Workstation build from Commercial off-the-shelf (COTS) PC hardware running a COTS operating system and one or several applications.
- Network component:
- Device that facilitates data flow between devices in a network, or restricts the flow of data in a network, but does not directly interact with a control process.
- Embedded Device:
- Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process (for example PLCs, field sensor devices).

The system components used in the Blueprint for the water industry are listed in the following tables.

Host / Application

Table 3-2 – Hosts

Component	Function
1 - WinCC OA Engineering Station	PC station for centralized plant-wide SCADA engineering. Online changes and extensions of the data model. Integration of new devices. Online application changes (operation screens, driver settings, business logic). Distributing changes to the SCADA server.
2 - TIA Engineering Station	PC station for centralized plant-wide engineering for PLC devices. Configuration of the hardware. Configuration of the communications networks. Configuration of continuous and sequential process sequences. Operator control and monitoring strategies. Compilation and downloading of all configuration data to all target automation devices.
3 - WinCC OA Client	Used for operator, control and monitoring. WinCC OA clients access the data of the WinCC OA servers, visualize this data and allow operators to control the process.
5 - PM ANALYZE	Add-On to prepare and create special reports to be conformed with ATV regulations.
7 - WinCC OA Server, redundant	The hot stand by redundant servers contain all the data of the connected automation devices and systems. Each server contains a measurement archives and an alarm archive. They establish the communication connection to the automation devices. The WinCC OA servers provide the process data to the WinCC OA clients.
8 - SINEC NMS – Operation Server	A network management system for monitoring and managing industrial networks. Operation is used displays detailed information about its monitored devices and displays the devices in network topologies.
9 - Domain Controller, redundant	Provides Active Directory Service and Time information.
14 - SINEC NMS Control UMC	A network management system for monitoring and managing industrial networks. Control is used for monitoring and administration of the entire network.
16 - WinCC OA Web Server	Provides the possibility to operate and monitor a plant via Internet / Intranet using a WINCC OA ULC UX Client. When a browser tries to connect to the ULC UX - URL of the WinCC OA Web Server, the Web server returns the ULC UX web page and automatically starts a local WinCC OA UI manager. This server-side UI manager transfers displayed information of the UI into HTML 5 interpretable data chunks.
17 - SINEMA RC Server	Provides secure remote access from the Internet to underlying networks for maintenance, control and diagnostics purposes.
15 - Jump Host	Provides access to plant via terminal or remote communication.
19 - Infrastructure PC	Used for Windows Updates, antivirus application and Quarantine Server.
20 - Anomaly Detection	Monitors network traffic and assets for abnormal device behavior and network communication anomalies. Sends alarms in case of network security problems.
21 - Log Server with SIEM Tool	Central Server to save all logged information from the plant.

Component	Function
22 - SIWA Suite Server	Consists of SIWA Optim, LeakControl, Sewer Wastewater control, infrastructure simulation.
23 - Energy Manager Pro	Energy data management system to create the basis for economical energy operation management to increase energy efficiency and thus reduce energy costs.
30 - SINEC INS	SINEC INS (Infrastructure Network Services) is the software tool for central network services that are frequently required, especially in the Operational Technology (OT) sector. Clear and easy to use, SINEC INS ensures that you can efficiently use frequently required services such as RADIUS and syslog servers in your network.

Network Components

Table 3-3 – Network Components

Component	Function
6 - SCALANCE XC Series	Router and switches to connect host systems and embedded devices to the Terminal and Process Control Network.
12 - Front Firewall	Protects the control system from external zones, like Corporate Lan and allows mainly certificate-based, encrypted and signed access to station in the DMZ.
13 - Back Firewall	Protects the Control System Network production network from the DMZ network and allows mainly certificate-based, encrypted and signed access of individual and trusted remote stations/networks.
26 - SCALANCE SC642-2C	Network router with firewall used to establish secure communication from Process Control Network to S7-1500.
27 - SCALANCE M826-2	Router for SHDSL communication on private communication infrastructure. Used for secure communication with remote stations, e.g. Storm Water Tank 1. Possible communication protocols are PROFINET, DNP3, IEC 60870-5-104, SINAUT ST7 via Telecontrol
28 - SCALANCE WAM766-1	IWLAN - Access Point for PROFINET Wireless communication based on IEEE 802.11ax.
29 - SCALANCE WUM763-1	IWLAN - Client for PROFINET wireless communication based on IEEE 802.11ax.
31 - TIM 1531 IRC	Communication module for WAN remote communication via possible communication protocols are DNP3, IEC 60870-5-101/104, SINAUT ST7 via Telecontrol.
32 - SCALANCE M876-4	Router for wireless GSM/UMTS/LTE communication on public communication infrastructure. Used for secure communication with remote stations, e.g. External Metering Station or Storm Water Tank 2 Possible communication protocols are DNP3 IEC 0870-5-104, SINAUT ST7 via Telecontrol.
34 - SCALANCE XF204-2BA	PROFINET network switch (managed) with redundancy manager to connect a PROFINET-Ring / Line to S7-1500.

Embedded Devices

Table 3-4 – Embedded Devices

Component	Function
24 - S7-1500 (H), optional redundant	PLC with 3 integrated Interfaces for PROFINET and / or Process Control Network Communication High availability optional.
25 - S7-1500	PLC with 3 integrated Interfaces for PROFINET and / or Process Control Network Communication High availability optional. CP1543-1 for extra Security communication
27 - S7-1200	PLC with additional CP1243-8 IRC for secure communication.
33 - RTU3051C	Monitor and control small outstations without connection to an energy supply system. In telecontrol networks, the RTU is used to connect the

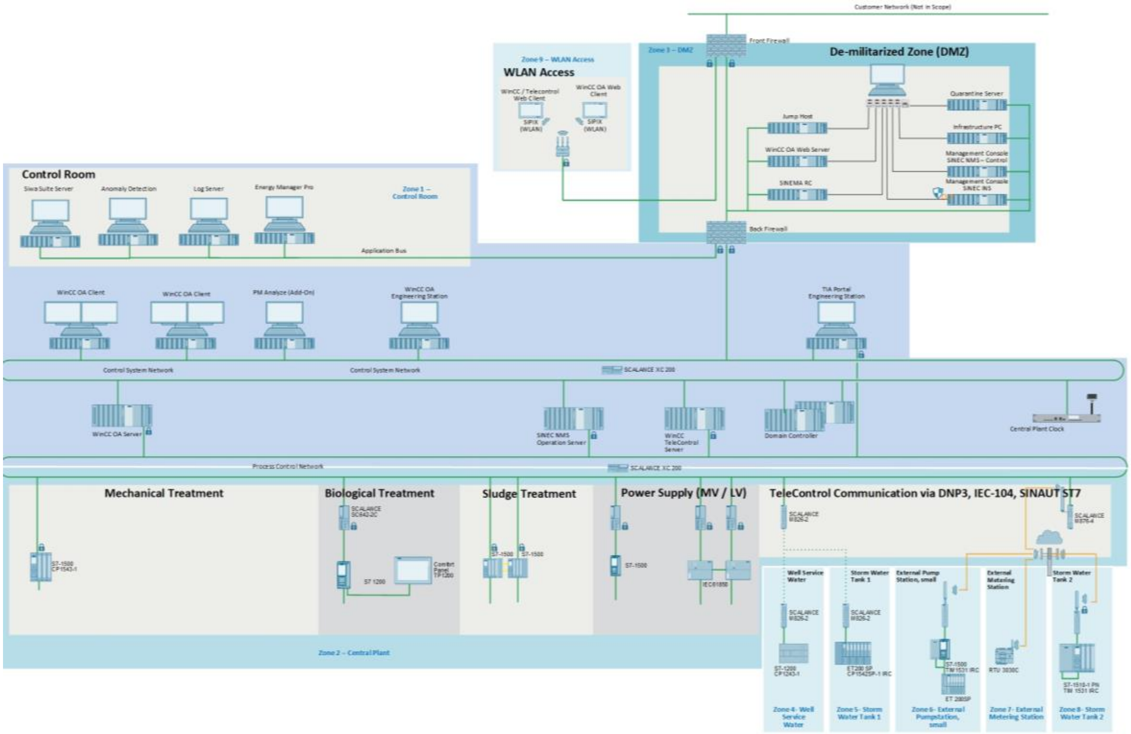
Component	Function
	remote stations to the control center via the mobile communication like LTE and 5G.
35 - Time Server	Relevant for components equipped with an internal hardware clock or real time clock (RTC) to keep the process control system with a standard time.

3.3. Zones and Intended Operational Environment

The Blueprint Wastewater Treatment Plant is structured into zones with similar security trust characteristics. The overview of the defined zones shown in Figure 3-3.

The figure also shows the physical location (Server Cabinets, Controller Cabinets, and Central Control Room) and the networks (Control System Network, Application Bus, Perimeter network (DMZ) and Process Control Network) of the internal zones.

Figure 3-3 - Zones Overview



3.3.1. Central Control Room

The central control room contains the Operator Workstations (WinCC OA Client 1 and 2).

Access to the central control room is restricted to authorized personnel only.

3.3.2. Engineering Room

The engineering room contains the TIA Engineering Station for the automation devices and the WinCC OA Engineering Station.

Access to the engineering room is restricted to authorized personnel only.

3.3.3. Server Room

The server room contains the Server Cabinets that enclose the entire client/server chassis' and Firewalls/Switches. In addition, the server room contains a rack mounted KVM switch that serves as local console for all the servers (DMZ and Control System Network) that do not have KVM screens located in the Central Control Room.

Access to the server room is restricted to authorized personnel only.

3.3.4. Control System Network

The Control System Network contains the servers and clients for the WinCC OA system as shown in the system architecture, Figure 2-3.

For a higher availability, the Control System Network has a ring design. This setup avoids communication failures if, for example, the line is damaged or interrupted at a particular point.

3.3.5. Application Bus

The Application Bus contains the server for special application:

- Energy Manager Pro.
- SIWA Suite – Sewer Application.

3.3.6. Demilitarized Zone (DMZ) / Perimeter Network

The DMZ (Demilitarized Zone) contains the servers that need to be accessed from, or need access to external systems/zones:

- SINEC NMS Control UMC.
- Jump Host.
- WinCC OA Web Server.
- SINEMA RC Server.
- Infrastructure PC (e.g. virus scan server, WSUS patch server, quarantine system).
- SINEC INS

The DMZ exists only physically within the server cabinets located in the server room.

3.3.7. Process Control Network

The Process Control Network connects all automation devices (e.g. SIMATIC S7-1500 controller) to the WinCC OA servers, the TIA Engineering Station and the SINEC NMS Server. The following main process parts are controlled by own automation devices:

- Mechanical treatment.
- Biological treatment.
- Sludge treatment.
- Power Supply (MV and LV).

There is no connection between the Control System Network or DMZ to the Process Control Network.

The Process Control Network also follows a ring design. This setup avoids communication failures if, for example, the line is damaged or interrupted at a particular point.

3.3.8. Controller Cabinets

Controller cabinets contain the automation devices (SIMATIC S7-1500 controllers) which are located at various physical locations inside the central plant area and are connected to the Process Control Network.

3.3.9. WLAN Access

The Wireless Access zone is connected to the Front Firewall and provides restricted access to devices in the DMZ (normally limited to HTTPS access to Web Server or via RDP to a Terminal Server).

The Wireless Access Points are located where required throughout the site and provide wireless access for Tablet PCs or Mobiles.

Connection to the Wireless Access Points will be encrypted and require wireless clients to have knowledge of the specific wireless "key" or they are authenticated via 802.1x protocol (RADIUS (network access restriction).

3.3.10. External Pump Station, Medium – Remote Station

The remote station is used to feed the intake pump station of the Wastewater Treatment Plant (WWTP). The communication between the central plant of a WWTP and the remote station is established by a privately owned infrastructure.

To ensure the encapsulation of the communication between the remote station and Process Control Network, the router SCALANCE XF204-2BA incl. "VD" adapter for Variable Distance is used.

3.3.11. Well Service Water – Remote Station

The remote station is used to provide service water to the Wastewater Treatment Plant (WWTP). The service water is produced from wells which are typically located outside the central plant of a WWTP. The communication between the central plant of a WWTP and the remote station is established by a private owned infrastructure.

To ensure the encapsulation of the communication between the remote station and Process Control Network, the router SCALANCE M826-2 is used.

3.3.12. Storm Water Tank 1 – Remote Station

The remote station is used to reducing in case of a heavy rain event the load on the downstream Wastewater Treatment Plant (WWTP). The communication between the central plant of a WWTP and the remote station is established by a private owned infrastructure.

To ensure the encapsulation of the communication between the remote station and Process Control Network, the router SCALANCE M826-2 is used.

The communication will be via Virtual Private Network for setting up and operating a secure connection (tunnel) between two secure IT systems or networks across an insecure network. Both partners have to authenticate themselves when opening the tunnel. During operation, data transmission is protected by encryption against viewing by unauthorized persons and the introduction of undetectable changes

3.3.13. External Pump Station, Small – Remote Station

The remote station is used to feed the intake pump station of the Wastewater Treatment Plant (WWTP). The communication between the central plant of a WWTP and the remote station is established via LTE (4G).

To ensure the encapsulation of the communication between the remote station and Process Control Network, the router SCALANCE M876-4 is used.

3.3.14. External Metering Station – Remote Station

The remote station is used to measure the volume of water coming from residential and commercial buildings by a public Wastewater system. The communication between the central plant of a WWTP and the remote station is established by public networks.

To ensure the encapsulation of the communication between the remote station and Process Control Network, the switch SCALANCE M876-4 is used.

3.3.15. Storm Water Tank 2 – Remote Station

The remote station is used to reducing in case of a heavy rain event the load on the downstream Wastewater Treatment Plant. The communication between the central plant of a WWTP and the remote station is established by public networks. To ensure the encapsulation of the communication between the remote station and Process Control Network, the switch SCALANCE M876-4 is used.

3.3.16. External Zones

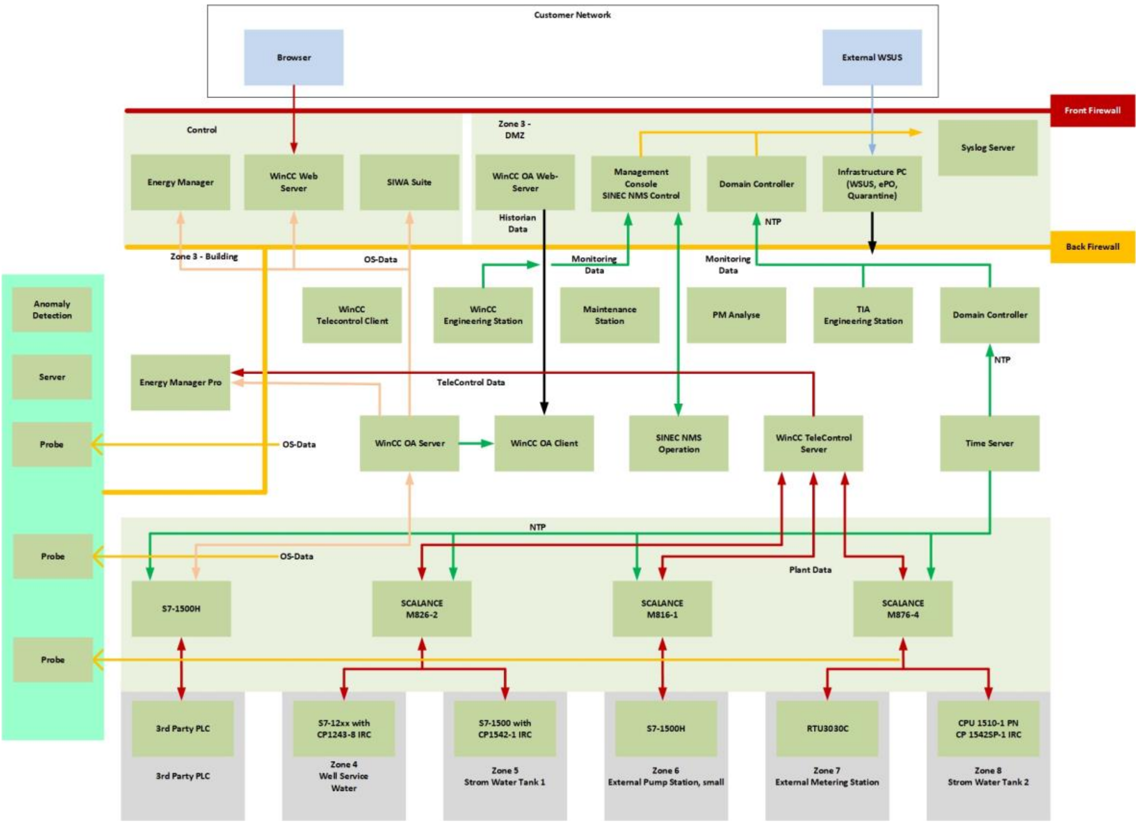
The Blueprint Wastewater Treatment Plant has two external zones: Customer Network (WAN) and Internet/UT

These zones conventionally provide update services to the applications running in the DMZ. The associated network connections for these services are, by convention, initiated (sourced) from the DMZ to the appropriate provider (destination) in the company network. A few, limited services like web or remote desktop clients are initiated from the company network, to the DMZ (Windows updates, virus pattern).

3.4. Data Exchange between zones

Data traffic and connections between the servers and applications in the respective zones are shown in a generic overview in the following picture.

Figure 3-4 - Overview of Data Exchange



4. Protection Goals

Protection goals for a solution in terms of confidentiality, integrity and availability can differ from plant to plant. Due to these differences, an individual Threat and Risk Analysis (TRA) has to be conducted for each plant and automation control system solution project. This should be done as a delta TRA on top of the existing TRA here.

For the generic blueprint Wastewater Treatment Plant, the following data and functionalities have been identified as sensitive with respect to confidentiality, integrity and availability in the following table:

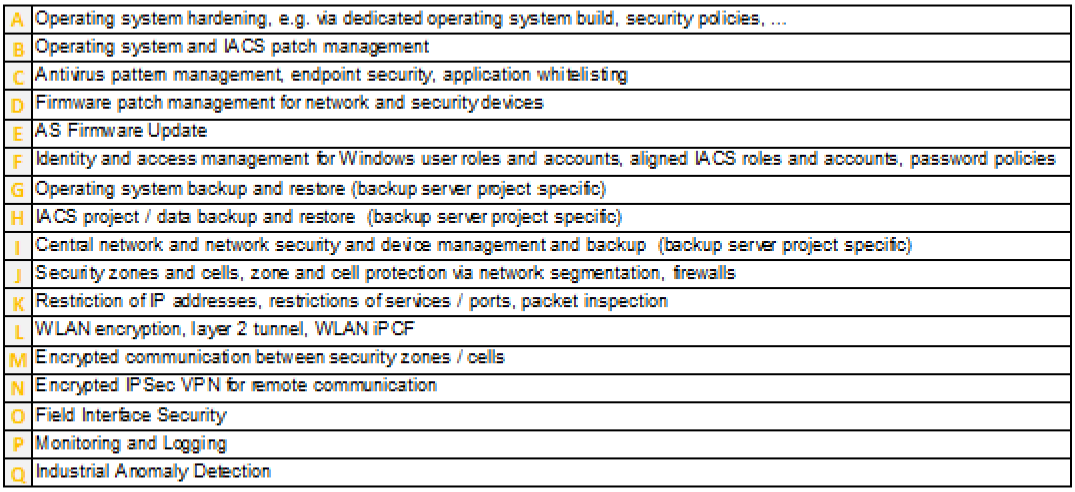
Table 4-1 – Protection Goals

Protection Goals	Description of the Protection Goals	Associated Main Components / Assets
Confidentiality	• User Passwords • Process data • Customer assets information • Internal process data become public, e.g. measurement data of the effectivity of cleaning processes • Project engineering data within scripts and panels	• Domain Controller • WinCC OA Server, S7-1500 -Controller
Integrity	• Historian data • Measurement data • Integrity of the water treatment process (e.g. use of correct chemical dosing) • Project Configuration & Engineering data • Integrity of Gas process (Methane)	• PM Analyze • WINCC OA Server, WinCC OA Engineering Stations • WinCC OA Engineering, S7-1500 Controller • SINEC NMS • S7-1500 Controller, WinCC OA Engineering Station
Availability	• Wastewater Treatment Plant availability • Availability of Storm Water Tank / Sewer Network / Intake Pumping Station (Gate Valves) • Floatation, Digester (Bacteria)	• S7-1500 Controller • S7-1500 H Controller • S7-1200 Controller

For the specified protection goals, the impact on the plant in the event of confidentiality, integrity and availability violations is assessed and the resulting measures prioritized through a threat and risk analysis (TRA).

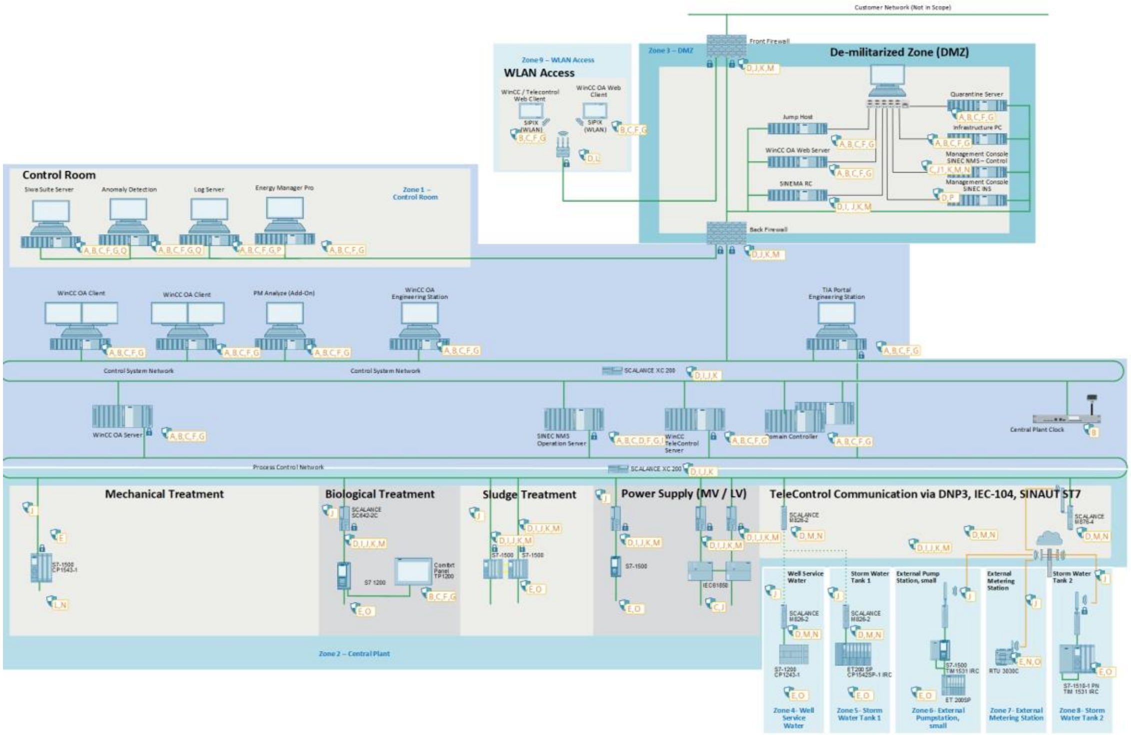
The following graphic shows the protection goals of the individual components in the zone overview.

Figure 4-1 – Legend of Protection Goals



A	Operating system hardening, e.g. via dedicated operating system build, security policies, ...
B	Operating system and IACS patch management
C	Antivirus pattern management, endpoint security, application whitelisting
D	Firmware patch management for network and security devices
E	AS Firmware Update
F	Identity and access management for Windows user roles and accounts, aligned IACS roles and accounts, password policies
G	Operating system backup and restore (backup server project specific)
H	IACS project / data backup and restore (backup server project specific)
I	Central network and network security and device management and backup (backup server project specific)
J	Security zones and cells, zone and cell protection via network segmentation, firewalls
K	Restriction of IP addresses, restrictions of services / ports, packet inspection
L	WLAN encryption, layer 2 tunnel, WLAN iPCF
M	Encrypted communication between security zones / cells
N	Encrypted IPSec VPN for remote communication
O	Field Interface Security
P	Monitoring and Logging
Q	Industrial Anomaly Detection

Figure 4-2 – Protection Goals for Zones



A generic TRA for this blueprint was conducted. This can provide some hints about possible threats and risks, but the TRA must be done for every plant individually.

4.1. Physical access

Perimeter security

Access to the facility to sabotage operations / processes → Fencing and barriers, surveillance cameras and lighting, security personnel.

Physically disrupt / manipulate remote stations → Fencing, surveillance cameras and lighting.

Manipulation to critical infrastructure, such as backup power supply systems → Tamper evident seals to detect unauthorized access attempts.

Secured parts & buildings

Access to central site / buildings for attackers → Access control, 2-factor authentication for access.

Physical access to steal data → Monitoring of all assets, different access levels (for employees) to the different areas of the facility, securing / locking server rooms and control cabinets.

Physical access to steal/destroy hardware → Securing / locking all hardware components.

Malware/sabotage from third-party personnel → Contractor management, background checks on third-party personnel that require access to the facility.

Unsecured / exposed parts and buildings / remote Stations (valves, reservoirs, pumps, metering stations...)

Attackers may gain access to these less secured networks → System & communication monitoring in SCADA.

Attackers may destroy / disable these stations → Redundant external systems (wells, pumps etc.)

Attackers may alter data in these stations → Treat them as unsecure parts, allowed communication is minimized.

Network & Windows PCs

Process Control Network/ Control System Network is secured, but access would be critical → Monitoring of network components, 802.1x, Industrial Anomaly Detection.

Windows may have unpatched vulnerabilities → Updates and / or Application Whitelisting.

4.2. Power supply system

Power supply from public grid → Monitor system, provide backup system.

Internal UPS → Backup system must be monitored and maintained.

4.3. Firewall

Exposed to internet, highest visibility even for script kiddies → Secure configuration.

Critical network part → Permanent central monitoring of firewall log data / Anomaly Detection

4.4. Internal & organizational measures

Access to infrastructure PCs, internals can tamper with them → Personal training, organizational procedures.

Access to operation PCs, internals can tamper with them → Personal training, organizational procedures.

Unsecured USB ports → System hardening, deactivation of USB ports.

Software updates can impact proper OS functionality → Application Whitelisting (can be an option instead of updates).

5. Security Measures

For the blueprint's Wastewater Treatment Plant, security measures are selected to fulfil security requirements and to mitigate any high risk identified in the blueprint specific Threat & Risk Analysis (TRA). The selected security measures are structured according to technical areas that contribute to the overall security of the blueprint security design and to cover all important aspects of the applicable IEC 62443 specifications.

The security measures described in the following sections are valid only for the blueprint's Wastewater Treatment Plant and the defined protection goals. For other solutions, the security measures can be different, based on the protection goals and high risks identified in the TRA.

5.1. Secure Network Design

One element for protecting the automation control systems and the networks is network security. The networks of automation control systems must be protected from unauthorized access and the interfaces to other networks, e.g. to the office network or remote maintenance access to the Internet, must be controlled, monitored and limited to the needed communication by using suitable technologies, e.g. firewalls.

5.1.1. Network Segmentation

IEC 62443-3-3	**SR 5.1 Network segmentation** **SR 5.1 RE 1 Physical network segmentation** **SR 5.1 RE 2 Independence from non-control system networks**

As part of implementing defense-in-depth, the automation system is segmented into security zones according to the blueprint shown in section 3.3. The zones are splitted so that system components with similar communication and protection needs are in one zone. The border between zones is called a trust boundary and the communication between these zones must be monitored and controlled, see section 5.1.2.

For the blueprint, segmentation is enforced between the central plant zone and the remote zone. The network is separated into the Control System Network and Process Control Network with dual-attached PCs, including firewalls, connect to both. These server PCs can propagate data to overlying systems.

The central plant zone, including the Process Control Network, spans the overall plant area with a lower level of physical protection compared to the building zone. It connects the subordinate subsystem zones (Zone 4 to Zone 8 in Figure 3-3) with the WinCC OA system in the central plant zone, where communication between these zones is implemented through encrypted VPNs.

Substations at remote locations outside the physical perimeter of the main plant must have a proper physical protection as no personnel is present at those substations. The network of those substation itself are own zones connected by encrypted VPNs with the central telecontrol server. This is to ensure an appropriate level of protection of the communication through the Process Control Network.

All communication between external zones and the water treatment plant like an operator's office network or remote access must pass through the DMZ. This is also implemented as a separate zone connected to the building zone.

The network segmentation implemented as part of this blueprint is in line with the recommendations provided by

- \25\ - WinCC OA Security Guideline (chapter 6.1: Security Cells and Network Architecture)
- \2\ - All-round protection with Industrial Security - Network Security

5.1.2. Zone Boundary Protection

IEC 62443-3-3	**SR 5.2 Zone boundary protection** **SR 5.2 RE 1 Deny by default, allow by exception** SR 5.2 RE 2 Island mode

All communication between the security zones must be monitored and controlled. To enforce the required communication rules and to ensure secure communication between the different zones, firewalls with VPN (IPsec) functionality are deployed as security measure. All unknown network traffic not allowed by any firewall rule will be blocked by these network devices as the firewall policy enforces the 'deny-by-default, allow-by-exception' principle.

For protecting the plant network boundary, DMZ (Demilitarized zone) hosts provide additional application-level control as all communication from external zones is terminated in the DMZ. This ensures that direct access to internal components, e.g. direct engineering access, is not possible. Instead, proxies or hosts in the DMZ are used. This includes for instance web access to the HMI, OPC-UA communication with central control~~,~~ or controlled transfer of security updates for inspection and subsequent rollout inside the plant.

Communication across the Process Control Network between the WinCC OA Servers and the remote stations is secured by SCALANCE S firewall appliances. These also implement strict firewall rules to reduce the attack surface for the Process Control Network of communication with connected remote locations.

Besides the network-based firewalls, the PC-based host firewalls need to be leveraged to provide an additional layer of protection. The configuration of the host firewall must be done during the WinCC OA installation.

Recommended configurations (rule sets) for the front and back firewalls as well as for the SCALANCE security network devices connecting the remote stations for the water treatment plant Blueprint are described in the sections 6.2, 6.3 and 6.4.

The above measures to protect zone boundaries of the blueprint are further complemented by adaptable security logging and monitoring measures that are described in detail in section 5.6.

5.1.3. Network Access Protection

IEC 62443-3-3	**SR 2.2 Wireless use control** SR 2.2 RE 1 Identify and report unauthorized wireless devices

While firewalls protect network zones at the boundaries, local access to the network can also be exploited by attacks. Some additional aspects need to be taken into account in this context:

- Restriction of access with mobile devices like service laptops.
- Protection of wireless access.

Users, software processes or devices accessing via wireless communication must be identified and authenticated. A commonly accepted security practice is to use state-of-the-art security profiles with strong authentication and encryption based on current 802.11 wireless communication standard. This is in order to authenticate and authorize access and monitor and enforce usage restrictions for wireless connections.

For protection against unauthorized access to the network via portable and mobile devices (e.g. service laptops, tablets and smartphones), common measures are hardening the deployed network devices and closing / disabling unused Ethernet ports. As a policy for portable devices, it is recommended that access to the WLAN is only allowed with proper user authentication.

The hardening measures and the configuration of the wireless devices of the blueprint are described in section 6.3.

5.1.4. Administration of Network Devices

Secure administration and configuration of network devices is of key importance due to their central role for availability of the plant internal and external communication, as well as their potential function to implement and enforce network segmentation.

All administrative access to network devices (e.g. routers, switches, firewalls, wireless network access points), used within the blueprint is performed through communication protocols that use state-of-the-art cryptographic protection (either Web-based through HTTPS or via SSH) with mutual authentication and strong encryption of all exchanged data. Unsecured legacy methods like HTTP or telnet – if supported at all - are disabled by default.

The management of human user access to such devices enforces role-based access control to implement least privilege and limit administrative access to authorized personnel.

Furthermore, user management and access control for administrative access is integrated with Active Directory based centralized account management through the SINEC NMS network management system that also allows central administration and updating the firmware of all managed SCALANCE network devices, see section 6.9.3.

5.1.5. Protection Measures Against Denial-of-Service

IEC 62443-3-3	SR 7.1	Denial of service protection

For the protection of solutions according to the blueprint against denial-of-service (DoS) attacks, two main aspects need to be covered.

On the one hand, DoS may target degradation of the overall availability of the plant network or individual devices e.g. through overloading with superfluous network communication. Here, the automation solution requires the capability to continue operation in a degraded mode during a DoS event.

On the other hand, the components protecting secure zones or being located within secure zones with critical roles in process control need to come with proven robustness against malformed network packages and network-level attacks, and either ignore such packages or switch to a defined state.

In the blueprint the main measures protecting from DoS attacks, include:

- Palo Alto's Front and Back Firewalls, that provide a general protection against common network level DoS attacks. The hardening measures and the configuration of the Palo Alto Firewalls are described in section 6.2.1.
- As part of the overall approach to industrial security in Siemens automation systems, the development process of all automation devices and software includes security considerations and regular penetration tests.
- \25\ - WinCC OA Security Guideline (chapter 6.2.2.5: Usage of WinCC OA mxProxy and restriction of open ports)
- \25\ - WinCC OA Security Guideline chapter 6.2.2.21: Keep secure settings in WinCC OA config file)

5.2. Identity and Access Management

User identification and authentication is supported and must be enforced on all interfaces that provide human user access. The human user interfaces include:

- Operator accounts for applications with user interfaces (e.g. HMI client, web interfaces).
- Operating system accounts.
- Engineering accounts (e.g. WinCC OA Engineering Station, TIA Engineering Station).
- Accounts for administrative access to network devices.
- User accounts for automation devices (online connection to SIMATIC S7-1500 controllers, access to the web server, access to the OPC UA server, etc.).

The user management and authentication solutions used for the blueprint's Wastewater Treatment Plant are described in section 7.

5.2.1. Authentication Mechanisms for Users and Components

IEC 62443-3-3	SR1.1 Human user identification and authentication SR 1.1 RE1 Unique identification and authentication SR 1.1 RE2 Multifactor authentication for untrusted networks SR 1.1 RE3 Account management SR 1.2 Software process and device identification and authentication SR 1.2 RE1 Unique identification and authentication SR 1.8 Public key infrastructure (PKI) certificates SR 1.9 Strength of public key authentication SR 1.9 RE1 Hardware security for public key authentication SR 1.10 Authenticator feedback SR 1.11 Unsuccessful login attempts SR 1.12 System use notification

Operating Systems

For operating system access, personalized Windows user accounts and groups are used. These can be centrally managed by an Active Directory (Windows Domain) which covers all Windows based machines connected to the Control System Network, application bus and DMZ networks. See section 7.1.

Exceptions to personalized (unique) accounts depend on configuration and operational procedures. These typically include accounts for machines that must be permanently operational and are used by several persons, such as control room operators. In these scenarios, it is important that local emergency actions and critical control system functions are not hampered by identification or authentication processes.

Applications

For application-level access (e.g. to WinCC OA clients), user authentication and account management is handled by an Active Directory server. All personal user accounts at components are assigned to domain groups. TIA Portal supports UMC (User Management Component), allowing engineering accounts to be integrated with the overall Active Directory service.

Network devices

Secure access to network devices is described in section 5.1.4 and can be integrated with the Active Directory managed groups and users through the UMC server running on SINEC NMS. The RADIUS server hosted on SINEC INS, provides the administrative access to the SCALANCE devices.

To prevent administrators getting locked out in the event of an authentication server failure, local user accounts can be created on network devices as a backup authentication mechanism. These local accounts can be configured with multifactor authentication for the SCALANCE devices shown below.

Table 5-1 – 2FA for SCALANCE devices

Device	Minimum firmware version
SCALANCE SC622-2C	V3.1
SCALANCE SC632-2C	V3.1
SCALANCE SC636-2C	V3.1
SCALANCE SC642-2C	V3.1
SCALANCE SC646-2C	V3.1
SCALANCE M800	V8.0
SCALANCE S615	V8.0

Automation devices

Access to SIMATIC controllers is user-based, ensuring that users attempting to connect are uniquely identified and authenticated.

Exceptions that require group-based authentication can be accomplished through the controller’s legacy access, that relies on passwords assigned to different access levels.

To gain further information regarding access control to SIMATIC PLCs, refer to section 6.10.

- \25\ - WinCC OA Security Guideline (chapter 6.2.2.9: Activate Kerberos encryption for WinCC OA systems)
- \25\ - WinCC OA Security Guideline (chapter 6.4.1: Usage of TLS/SSL for plant communication)
- \25\ - WinCC OA Security Guideline (chapter 6.4.1.5: Enforce usage of strong cipher suite)
- \25\ - WinCC OA Security Guideline (chapter 6.4.3: User Administration)
- \25\ - WinCC OA Security Guideline (chapter 6.4.3.2.1: Usage of Operating system (Windows or Linux) based user management)
- \25\ - WinCC OA Security Guideline (chapter 6.4.3.3: Single Sign On)
- \25\ - WinCC OA Security Guideline (chapter 6.4.3.5.2: Server-side Authentication for Managers with session binding)
- \25\ - WinCC OA Security Guideline (chapter 6.4.8: Configure System Use Notification)
- \44\ - Enabling 2FA for SCALANCE devices

5.2.2. Management of Identifiers and Credentials

IEC 62443-3-3	**SR 1.3 Account management** **SR 1.3 RE 1 Unified account management** **SR 1.4 Identifier management** **SR 1.5 Authenticator management** **SR 1.6 Wireless access management** SR 1.6 RE1 Unique identification and authentication

Active Directory

Centralization of account management reduces administration efforts. Microsoft Active Directory is used across the blueprint for the Windows-based host systems in the automation network. The blueprint supports the management of identifiers (e.g. username, host name) and passwords for the Windows domain accounts through the Windows AD domain controllers. This includes mechanisms for password recovery and reset mechanisms.

Through centralized management and integration with the domain controllers, there is no need for local management at machines.

User Management Component (UMC)

UMC is employed in the blueprint to centralize user management for Siemens’ software, network and automation devices, and it can be connected to Microsoft’s Active Directory.

SINEC NMS supports UMC, and it can be used in combination with SINEC INS to provide central user management for SCALANCE network devices. For further information on SINEC NMS, refer to section 6.9.3.

For automation devices, user management can be handled globally, via UMC (for S7-1500 controllers running FW 4.0 onwards), or locally, using TIA's "User Management & Access Control".

User Management & Access Control (UMAC)

TIA Portal's "User Management & Access Control" provides a centralized solution for managing all user-related tasks within a project. Policies can be set to enforce password strength based on minimum length and variety of character types.

Management of further security credentials e.g. for setting up secure communication, is described in detail in the respective product security manuals of WinCC OA and is supported by several tools and management consoles.

- \25\ - WinCC OA Security Guideline (chapter 6.2.2.9: Activate Kerberos encryption for WinCC OA systems)
- \25\ - WinCC OA Security Guideline (chapter 6.2.1.6: Delete or disable unneeded default users on OS Level)
- \25\ - WinCC OA Security Guideline (chapter 6.2.2.16: Limit usage of the root user)
- \25\ - WinCC OA Security Guideline (chapter 6.4.3.3: Single Sign On)

5.2.3. Account Management and Configuration of Access Rights and Privileges

The account management handling (users & groups) is done via the Active Directory. The least privilege approach should be applied to grant users only the minimum level of access or privilege required to fulfill its specific job, reducing the risk of unauthorized and unintended use of services or systems. Unused default system accounts used for the first installation of applications, system, devices, etc. should be removed.

UMC is employed for central user authentication, but it cannot handle user authorization. Therefore, access rights to a TIA Portal project (Engineering rights) and to automation devices (Runtime rights) need to be configured in the TIA Portal project itself.

5.2.4. Control of Access via Untrusted Networks (Remote Access)

As the blueprint solution is protected by Firewalls and a DMZ, no direct access is possible for users connecting to the plant from external networks that are considered untrusted by default. All possible access is to machines in the DMZ that are specifically configured and secured to allow access at application level. Remote users therefore require user accounts with special privileges and all such accounts are also controlled by Active Directory.

With SINEMA Remote Connect installed in the DMZ, remote access can be realized. In combination with a jump host solution, a highly secure remote access setup can be achieved, allowing access to the engineering station. In the remote access use case, the user will login to SINEMA RC server and establish a secure VPN connection to pass the unsecure networks, like the Internet. This connection can then be used to establish an RDP connection to the jump host station.

Furthermore, the user establishes a connection from the jump host station through the back-firewall to the engineering station, which must be scanned for malware and unauthorized file transmissions. Finally, the combination of SINEMA RC in the jump host solution with the back-firewall results in a high security and state-of-the-art remote access solution.

5.3. Attack Surface Reduction

The attack surface of the automation control system is formed by its interfaces.

5.3.1. Least Functionality

As the attack surface of a system is formed by its interfaces, two important security measures contribute to its reduction (“hardening”):

- Disabling all unnecessary interfaces.
- Protecting those interfaces with secure configuration that are either necessary or cannot be disabled.

Typical measures to protect such interfaces that are also applied in the blueprint, address:

- Physical communication interfaces (USB ports, Ethernet ports, diagnostics interfaces, wireless communication).
- System-level functionality especially with component external interfaces (unnecessary functions, software applications, ports, protocols and/or services.

All of the above is applied to different levels of components:

- Applications.
- Operating system (OS).
- Low-level interfaces in BIOS.

Recommended hardening measures for the blueprint to reduce the attack surface of the above described areas, are listed in chapter 6.6.

This also includes physical protection measures like locks or access-protected rooms, described as part of the intended operational environment of the zones in chapter 3.3.

Furthermore, removal of all temporarily enabled functions after commissioning must be ensured, e.g. related to debug and test interfaces, and including accounts only needed for commissioning, to minimize the attack surface during plant operation.

Further information regarding least functionality for WinCC OA systems is provided by:

- \25\ - WinCC OA Security Guideline (chapter 6.2: Hardening)

5.4. Secure Channels and Encryption

5.4.1. Secure Channels

Encrypted channels are a core measure to protect data during the transit across untrusted zones. For traffic within a trusted zone, the need to use secure channels is individually analyzed, balancing threats and costs.

Only proven and non-repudiated encryption and hashing algorithms must be used. Policies and procedures regarding key management must address periodic key changes, key destruction, key distribution and encryption key backup, complying with defined standards.

5.4.2. Sensitive Data

The data considered sensitive is identified by the protection goals in section 4. For such data, access restrictions as well as protected and encrypted storage are described in the respective product or component manuals.

As result, the following default security measures are recommended in the blueprint’s context:

- Secure communication for all traffic to and from the plant, i.e., between the servers in the DMZ and external communication end points. Dedicated IPsec VPN protected channels between the main plant and all remote stations, to achieve independence from the security capabilities of utilized communication infrastructure (e.g. WWAN or WLAN radio).
- Encryption of the PLC’s confidential data (e.g. private keys) through password protection.
- Secure communication within trusted zones for sensitive data transmission (e.g. OPC UA, HTTPS, secure OUC, etc.). Real-time communication requirements must be considered.

5.5. System Integrity Protection

The integrity of the system must be protected against unauthorized changes of software and data, and these changes must be detected, recorded and reported.

This especially includes protection against malware, with focus on the different interfaces that – if used without care or with intention - could introduce malware through data transfer via USB sticks or other mobile devices, or through users browsing infected Web pages or opening infected email-attachments.

Depending on the malware, a broad range of impacts are possible, ranging from using up computational resources or locking down components to establishing remote control of a client or server by an attacker. Targeted malware could also manipulate the system behavior.

The recommended malware protection measures for the blueprint are described in section 8.

5.5.1. Software and Information Integrity

Besides technical support to secure workflows for updating software and configuration and additional measures like digitally signed software updates, the protection of the system against malware and unauthorized changes can be implemented using:

- Virus scanner software:
- Virus Scanner software detects, blocks and removes malware (if necessary and configured).
- For the actual operational environment of the blueprint water based on WinCC OA, specific configuration recommendations apply, see section 8. These are important to ensure that the use of virus scanning software on the computers of an automation plant do not interfere with the process mode of a plant. Examples include:
    - Configuration is aligned with availability requirements and generates alarms but does not proactively disable or shut down parts of the system functionality that may result in loss of control of the production system (e.g. for an OS server).
    - Configuration is adjusted to minimize potential impact on performance on the critical software applications during runtime.
- Whitelisting technologies:
- Whitelisting and Application Control are techniques that only allow the execution of trusted applications or restrict file operations to specific ones. Whitelisting either complements or is used as an alternative to virus scanning solutions.
    - Whitelisting, list-based: Software processes and services that are part of a managed whitelist and are classified as trustworthy are allowed to run. All others (like malware introduced into the whitelisted component, unapproved tools) will be blocked from execution.
    - Whitelisting, rule-based (Application Control): Rules are defined to decide whether an application can be started or restrict the allowed file operations.

On the stations and servers of the blueprint, virus scanner software is installed with the capability to keep the virus patterns up to date using an infrastructure server for exchange of virus pattern files in the DMZ. Whitelisting is installed on the stations and servers of the blueprint. Section 8 describes these protection measures in detail. It is important to note that typical malware exploits vulnerabilities in the installed software components and services, and both virus scanner and whitelisting solutions must be complemented by an up-to-date security patch level. The patch management procedures for the Blueprint are described in section 9.

- \25\ - WinCC OA Security Guideline (chapter 6.6: Virus Scanner)

5.5.2. Security Functionality Verification

It is important to ensure the correct functioning of the implemented security measures. The verification of the intended operation of security measures is performed during the Factory Acceptance Test (FAT), Site Acceptance Test (SAT) with appropriate security tests and is recommended to be performed afterwards on a regular basis (e.g. during scheduled maintenance).

- \25\ - WinCC OA Security Guideline (chapter 6.8: Security Tests)

5.5.3. Input & Output Validation and Error Message Sanitization

WinCC OA ensures aspects like input validation and controlled output through an overall secure development process. The secure development process is certified according to the IEC 62443 framework for security in industrial control systems (part 4-1, secure development).

5.5.4. Support for Control System Backup and Recovery

The goal of backup and recovery is, that the operator or asset owner can recover and reconstitute to a known state after a disruption of failure. Further details can be found in section 10.

5.5.5. Time Distribution and Synchronization

In the blueprint, the central plant clock is connected to both the Control System Network and the Process Control Network. The domain controller on the Control System Network uses the time telegram from the central plant clock and provides the time to all domain members (e.g. OS clients and servers, MES systems, OPC server). The S7-1500 controllers connected to the Process Control Network get the time signal directly from the central plant clock.

Recommended measures and further details about the time distribution and synchronization is provided in section 6.8.

5.6. Security Logging and Monitoring

IEC 62443-3-3	SR 1.13 Access via untrusted networks SR 1.13 RE1 Explicit access request approval

Security features and capabilities described in the above subsections are complemented by security logging and monitoring of security related actions and events across all required system components. In addition to the logging and monitoring focused on the controlled process that is thoroughly covered by the capabilities of the regular automation control system, information from security logs and monitored events are important to discover or perform forensics in case of cyber security incidents.

In addition to security logging and monitoring, additional industrial anomaly detection capabilities can be added. See section 0.

5.6.1. Monitoring Access from Untrusted Zones

As described in section 5.1, the blueprint's Wastewater Treatment Plant is protected by a DMZ that allows full control of all network communication and remote access from external, potentially untrusted, networks. Security logging and monitoring covers both firewalls realizing the DMZ as well as the PC based systems within the DMZ. Hence, all user or system-level access and all communication sessions at network (TCP/IP) level are covered.

The blueprint covers various remote stations like wells, tanks, or external pumps and metering stations. Communication lines between the central plant and remote stations are monitored via the SCALANCE network devices which implement the secure connections.

- \25\ - WinCC OA Security Guideline (chapter 6.1.8.4: Protected Service Access)

5.6.2. Logging of Security-Related Events

For the protected zones of the blueprint's Wastewater Treatment Plant, including building and central plant zones, security logging is performed for PC-based WinCC OA systems, SCALANCE network devices and SIMATIC PLCs. The PC-based systems maintain security logs for both application level and operating system level events. Security logs can be exported through standardized communication protocols (Syslog, SNMP) to central servers. These servers centrally collect security log information from the system components and provide interfaces that can be integrated with asset owner's superior SIEM solutions (Security Information Event Management). Further details on optional SIEM functionalities are described in section 0.

Monitoring of Palo Alto Front & Back Firewall is done with Panorama Management Software. In general, all access to security logs is secured and restricted to authorized users of the automation solution through the system capabilities described in section 5.2. Hence, all access to security log data is also covered by the security and logging capabilities.

Syslog clients are configured on the automation devices to enable better tracking and monitoring of critical PLC changes and operations. In the event of security-relevant events, such as user logins, configuration changes or operating state changes, messages are generated in a separate message memory of the PLC. The configurable forwarding to external Syslog servers / SIEM systems enables its integration into existing security monitoring systems.

- \25\ - WinCC OA Security Guideline (chapter 6.7: Logging, audit, maintenance and asset management)
- \51\ - Security Events in WinCC OA

5.6.3. Audit trail

To fulfill the requirements for change management all changes shall be centrally executed either via the WinCC OA or TIA ES (concerning automation equipment) or via SINEC NMS (concerning network components). In this way, audit reports can be generated at any time to prove which human user has done which changes.

SINEC INS can be used as a Syslog server to monitor changes and security events for automation and network components. Direct local access to PLCs or SCALANCE devices should be used only during first time commissioning, not later in the operation and maintenance phase.

- \25\ - WinCC OA Security Guideline (chapter 6.7: Logging, audit, maintenance and asset management)
- \49\ - SIMATIC NET: Network management SINEC INS

6. Hardening and Configuration of the System Components

For the components used in the Blueprint Wastewater Treatment Plant various hardening measures must be considered according to the Threat and Risk Analysis and the defined protection goals, see section 4.

The recommended hardening measures and configurations describe in the following sections are only valid for the Blueprint Wastewater Treatment Plant.

For any deviation to the Blueprint, a Threat and Risk Analysis must be conducted, and the hardening measures and configuration must be adopted accordingly.

6.1. Assumptions

IEC 62443-3-3	**SR 1.7 Strength of password-based authentication** **SR 1.7 RE1 Password generation and lifetime restrictions for human users** **SR 1.7 RE2 Password lifetime restrictions for all users**

Besides the hardening measures for the automation control system the defense-depth-concept recommend physical and organizational security measures which are in the responsibility of the plant owner.

In evaluation of the possible security risks for the Blueprint Wastewater Treatment Plant the following physical security measures are assume:

- Unauthorize access to the central plant and buildings are prevent by physical measures. Only authorized personnel have access.
- Unauthorize access to the remote stations are prevent by physical measures. Access to the remote stations is monitored, e.g. using door switches. Only authorized personnel have access.
- All cabinets having a locking system with semi-cylinders
- All cabinets, both on the main part of Wastewater Treatment Plant and the remote stations, are installed in lockable control or server rooms. Access to control or server rooms are limited to authorized personnel (maintenance) only.
- The Control System Network is installed in one building with high physical protection as shown in Figure 3-3
- The Process Control Network is running in central plant of the Wastewater Treatment Plant with physical access control as shown in Figure 3-3 General Hardening Measures

For all components used in the Blueprint Wastewater Treatment Plant the following general hardening measures shall be considered to ensure the secure configuration during the plant operation

- The latest released firmware versions shall be installed. Firmware versions for all Siemens components are available on the Siemens Industry Online Support \4\.
- For all components the latest released patches shall be installed. The patches for Siemens components are available on the Siemens Industry Online Support \4\. Further information regarding patch management given in section 9.
- For the virus scanner installed on the workstation and server always the latest virus pattern must be installed. Further information available is available in:
- \25\ WinCC OA Security Guideline - WinCC OA Security Guideline (chapter 6.6: Virus Scanner)
- The standard user and password on all devices must be changed before the first installation. The same password shall be not used for different users and systems and shall be protected and inaccessible to unauthorized persons.
- Further information given in section 7.
- For SCALANCE components the hardening measures describe in \5\ – Checklist for Setting Up SCALANCE Devices shall be considered and centrally executed by SINEC NMS.

6.2. Firewalls for Secure Communication Between the Zones

The communication between the security zones must be monitored and controlled as descried in section 5.1.2.

The plant network boundary is protected using a Front- and Back-Firewall, creating the Demilitarized Zone (DMZ) of the blueprint. The hardening measures and the configuration of the firewalls are described in section 6.2.1. For further information see:

- \25\ WinCC OA Security Guideline (chapter 6.1: Security Cells and Network Architecture)

The communication between the security zones within the automation control system is secured by SCALANCE network security devices. The hardening measures and the configuration of these devices are described in section 6.2.2.

6.2.1. Palo Alto 440 NGFW

Front Firewall:

- Protects both the DMZ network and the internal networks from Untrusted network(s) (Corporate firewall interface or Internet interface.)
- Allows Servers in the DMZ to securely communicate with public servers. Both outgoing and incoming data is screened utilizing DPI.

Back Firewall:

- Data that needs to go to and from the Process Control Network is screened and controlled using a multi-factor approach restricting traffic up to Layer 7 to the applications and services that are required for operation Data that needs to go to and from the Process Control Network is screened and controlled using a multi-factor approach restricting traffic up to Layer 7 to the applications and services that are required for operation

The recommended hardening measures and the configuration of the Front – and the Back-Firewall are listed in Table 6-2.

Figure 6-1 – DMZ with Front- and Back-Firewall

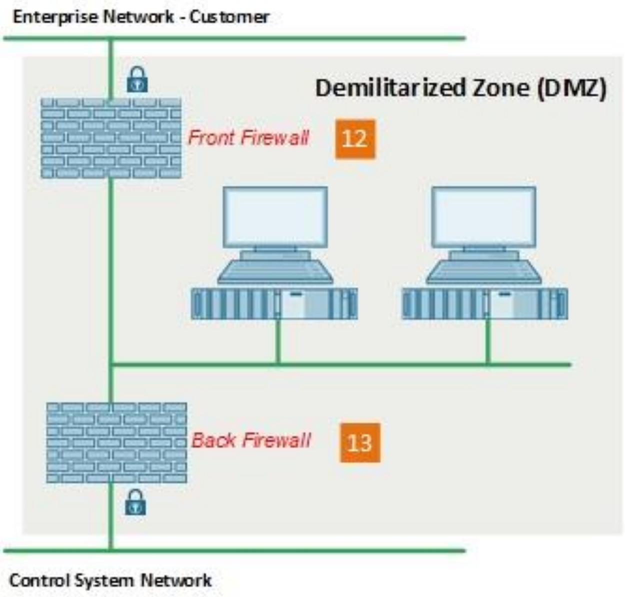


Table 6-1 – Front- and Back-Firewall

Function	SCI	Supplier	Type	MLFB
Front-Firewall	12	Palo Alto	440 NGFW	9LA1110-6SY12-1AB1
Back-Firewall	13	Palo Alto	440 NGFW	9LA1110-6SY12-1AB2

For the firewalls listed in the following general hardening measures must be considered at least:

Table 6-2 – Hardening measure for the Firewalls

No.	Security Topic	Hardening Measure	Documents
1	Restrict IP addresses	Restrict the access only to those IP addresses that needed	\39\
2	Restrict services	Do not allow access over the unsecure protocol HTTP or Telnet, require SSH and/or HTTPS	\39\
		Set the encryption min. version to TLSv1.2	\39\
3	Change admin credentials / user management	Change the default username	\39\
		Change the default password	\39\
		Configure an account for each person who needs access and give them only the rights that they need	\39\
		Use multi-factor authentication (RADIUS or SAML)	\39\
		Configure a strict password policy	\39\
4	Dedicated management interface	Use the dedicated management interface in a separate management LAN or VLAN	\39\
5	Security policy rules and profiles	Scan all traffic destinated to the management interface for threats	\39\
		Create a security profile, enable extended packet capture	\39\
		Configure inbound inspection and SSL Forward Proxy	\39\
6	Logging	Set up logging for configuration changes	\39\
		Set up logging for unauthorized login attempts	\39\
7	SNMP	Use SNMP v3	\39\
		Set an SNMP string that is not easy to guess	\39\
		Only enable SNMP on internal interfaces	\39\
8	Certificates	Replace the default certificate with a certificate signed by the organization’s enterprise CA	\39\
9	Updates	Keep the PAN-OS and all software packages up to date.	\39\

Further information about the configuration of the Palo Alto Next Generation Firewall provide:

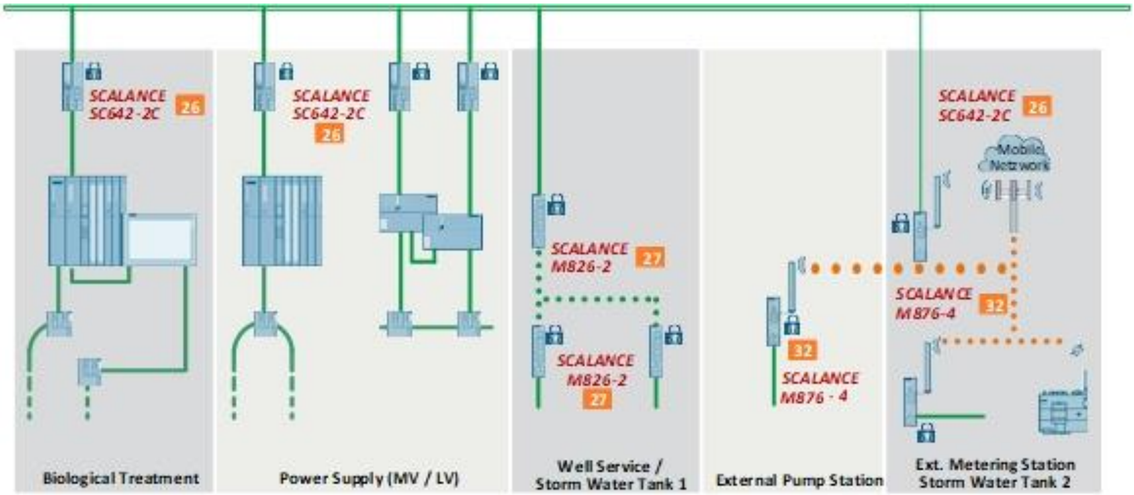
- \6\ – PAN-OS Administrator’s Guide

- \7\ – Palo Alto Website about PAN-OS
- \39\– Palo Alto - Best Practices for Securing Administrative Access section

6.2.2. SCALANCE Network Security Devices

In the Blueprint the secure communication on the Process Control Network and to the remote stations is implemented by the use of SCALANCE network security devices as shown in Figure 6-2. The following table are different showcases for interconnection.

Figure 6-2 – SCALANCE security network devices



The following types of the SCALANCE network security devices are used in the Blueprint:

Table 6-3 – SCALANCE Security Network Devices

Function	SCI	Supplier	Type	MLFB
Secure Communication between Process Control Network and • S7-1500 Controller • Station Gateway	26	Siemens	SCALANCE SC642-2C	6GK5642-2GS00-2AC2
Secure Communication between Process Control Network and • Remote Station *Well Service Water* • Remote Station *Storm Water Tank 1*	27	Siemens	SCALANCE M826-2	6GK5826-2AB00-2AB2
Secure Communication between Process Control Network and the Remote Station *External Pump Station, small*	32	Siemens	SCALANCE M876-4	6GK5876-4AA10-2BA2
Secure Communication between Process Control Network and the Remote Stations *External Metering Station* and *Storm Water Tank 2*	32	Siemens	SCALANCE M876-4	6GK5876-4AA10-2BA2
Secure Communication between Process Control Network and S7-1500 to 3rd Party PLC in Mechanical treatment S7-1500 to internal MRP-ring	25	Siemens	SIMATIC Net CP 1543-1	6GK7543-1AX00-0XE0

For the SCALANCE devices listed in Table 6-2 the following general hardening measures have been at least to considered:

Table 6-4 – Hardening measures for SCALANCE network security devises

No.	Security Topic	Hardening Measure	Documents
1	Secure Network	Quality of service (QOS) priority is set to "DSCP"	\5\ – Section 3.10
		Deactivate Spanning Tree if not required	\5\ – Section 3.11.2
		Deactivate Passive listing	\5\ – Section 3.11.3
2	Identity and Access Management	Use central authentication via RADIUS /UMC /AD. Establish password policy (complexity and change frequency) and deploy changes centrally and regularly via SINEC NMS.	\5\ – Section 3.4 \43\ – Section 7
3	Reduction of Surface Attack	Disabling of unencrypted and non-required protocols. Details provides Table 6-3	\5\ – Section 3.3
		Disable of PROFINET interface completely	\5\ – Section 3.7
		Restrict the DCP access to "Read-Only"	\5\ – Section 3.9.1
		Disabling of unused ports	\2\ – Section 5.71 \5\ – Section 3.14.1
		Disable all non-required services, like DHCP or DNS	
4	Secure Channels and Encryption	No Action required (see Table 6-6	
5	System Integrity	Use of NTP for time synchronization. If available, the secure NTP variant to be used	\5\ – Section 3.2
6	Logging and Monitoring	Activate Syslog client. Please refer also to Section 0	

The following table shows the settings for the protocols:

Table 6-5 – Protocols

No.	Protocol	Settings
1	Telnet Server	Disabled
2	SSH Server	Disable and use SINEC NMS for configuration of all network devices
3	HTTP Services	HTTPS only
4	DCP Server	Read-Only
5	SNMP • SNMP v1/v2 Read-only • SNMP v1 Traps • SINEMA Configuration Interface	Use SNMP v3 • Disabled • Disabled • Disabled

The secure communication between the zones is established by using IPsec VPN and the internal firewall. Table 6-6 and Table 6-7 shows the settings, therefore.

Table 6-6 – IPsec VPN configuration

No.	Topic	Settings
1	Remote End	Remote Mode: Standard Remote Type: Manual
2	Connection	Keying Protocol: IKEv2
3	Authentication	Use CA-Certificates Don't use PSK
4	Phase 1	Use default Ciphers At least use • Encryption: AES128 GCM 16 • Authentication: SHA256 • Key derivation: DH group 14 Don't use Aggressive Mode
5	Phase 2	Use default Ciphers and Auto Firewall Rules At least use • Encryption: AES128 GCM 16 • Authentication: SHA256 • Key derivation: DH group 14

Table 6-7 – Firewall settings

No.	Topic	Settings
1	Predefined IPv4	Disable all service for all VLAN which are not required

The following table list additional settings for the used types of the SCALANCE network security devices.

Table 6-8 – Additional settings

No.	Type	Settings
1	SCALANCE SC642-2C	Deactivate MRP
2	SCALANCE M826-2	Create an own VLAN for SHDSL and Transfer subnet. The firewall shall be activated to restrict the access
		Use IPsec communication between 2 M826-2 to connect the subnets using SHDSL connection (transfer subnet)
3	SCALANCE M876-4	Mobile wireless configuration • Authentication Method: Auto • Data Roaming: Disable
		SMS: Disable SMS services, if not needed

No.	Type	Settings
		No service should be accessible via usb0 (mobile wireless interface). See firewall configuration Table 6-7

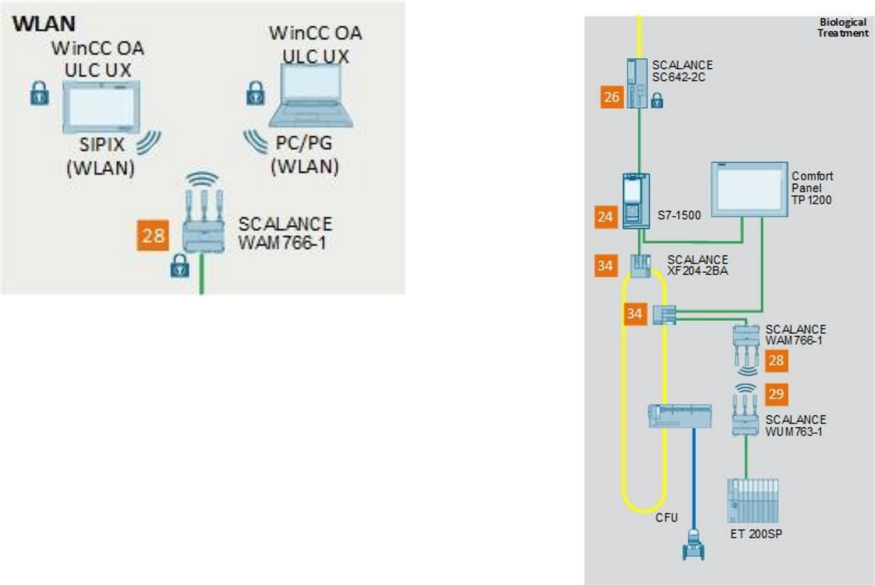
Further information about the configuration of the SCALANCE Security network devices provide:

- \5\ – Checklist for Setting Up SCALANCE Devices
- \8\ – SCALANCE SC-600 – Web Based Management (WBM)
- \9\ – SCALANCE SC-600 – Operating Instructions)
- \10\ – SCALANCE M800 Web – Based Management (WBM)
- \11\ – SCALANCE M874, M876 – Operating Instructions
- \12\ – SCALANCE M826 – Operating Instructions
- \13\ – SCALANCE M874, M876 – Operating Instructions
- \43\ – User administration for SCALANCE devices with RADIUS protocol

6.3. Network Components for Wireless Communication

Wireless communication by IWLAN is used in the Blueprint to connect I/O field devices like the Compact Field Unit (CFU) with PROFINET to automation controller S7-1500. Furthermore, tablets used for mobile configuration and operation are connected by IWLAN to the automation control system, see Figure 6-3.

Figure 6-3 – Wireless Communication



The following types of the SCALANCE Wireless devices are used in the blueprint:

Table 6-9 – SCALANCE Wireless devices

Function	SCI	Supplier	Type	MLFB
IWLAN – Access Point for the PROFINET wireless communication to I/O field devices and also used for communication with mobile laptops and tablets used in the central plant (please consider also CLP and observe national approvals)	28	Siemens	SCALANCE WAM766-1	6GK5766-1GE00-7DA0
IWLAN – Client for PROFINET wireless communication to I/O field devices (please consider also CLP and observe national approvals)	29	Siemens	SCALANCE WUM763-1	6GK5763-1AL00-3DA0

The hardening measures for the SCALANCE wireless devices are listed in

- Table 6-4 – Hardening measures for SCALANCE network security devises.
- Table 6-5 – Protocols.

In addition to these general hardening measures and configuration the following hardening measures must be considered:

Table 6-10 – Additional Hardening measures SCALANCE W

No.	Security Topic	Hardening Measure	Documents
1	WLAN encryption	Enable AES encryption for iPCF	\5\ – Section 3.12.1
2	WLAN layer 2 tunnel	Set Mac mode to 'Layer 2 tunnel'. This is only possible if only SCALANCE devices are used.	\5\ – Section 3.12.2
3	WLAN iPCF	Use iPCF if time-critical data, e. g. PROFINET are transferred via the radio link.	\5\ – Section 3.12.3

Further information about the configuration of the SCALANCE Wireless devices provide:

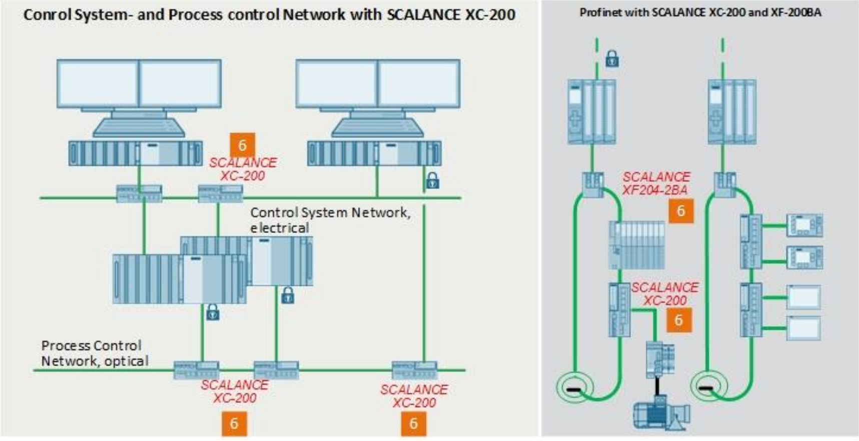
- \5\ – Checklist for Setting Up SCALANCE Devices
- \14\ – SCALANCE WAM766 – Operating Instructions
- \15\ – SCALANCE WUM763 – Operating Instructions

6.4. Network Components SCALANCE XC and XF

The connection of the workstation and server to the respective networks (e.g. DMZ-Subnet or Control System Network) and the connection of PROFINET devices to PROFINET networks are implemented in the blueprint using the following SCALANCE series.

- SCALANCE XC-200.
- SCALANCE XF-200BA.

Figure 6-4 – SCALANCE XC-200 and XF-200BA


Conrol System- and Process control Network with SCALANCE XC-200
6
SCALANCE XC-200
Control System Network, electrical
Process Control Network, optical
SCALANCE XC-200
6
SCALANCE XC-200
6
Profinet with SCALANCE XC-200 and XF-200BA
SCALANCE XF204-2BA
6
SCALANCE XC-200
6

The hardening measures for the SCALANCE XC-200 and XF-200BA devices are listed in

- Table 6-4 – Hardening measures for SCALANCE network security devises.
- Table 6-5 – Protocols.

In addition to these general hardening measures and configuration the following hardening measures must be considered:

Table 6-11 – Additional Hardening measures SCALANCE XC-200 & XF-204 BA

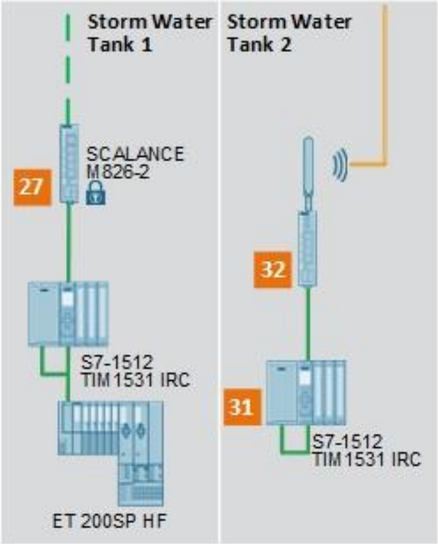
No.	Security Topic	Hardening Measure	Documents
1	Ring Redundancy	Disable ring redundancy, if the device is not operated in a ring	\5\ – Section 3.11.1
2	PROFINET	If the SCALANCE Device is used in a PROFINET Network the PROFINET interface functionality must be enabled.	\5\ – Section 3.7

Further information about the configuration of the SCALANCE XC-200 and XF-204 provide

- \5\– Checklist for Setting Up SCALANCE Devices
- \16\ – SCALANCE XC-200 / XF-200BA Web Based Management (WBM)
- \17\ – SCALANCE XC-200 – Operating Instructions
- \18\ – SCALANCE XF-200BA – Operating Instructions

6.5. TeleControl TIM 1531 IRC

Figure 6-5 - Telecontrol TIM 1531 IRC



The TIM 1531 IRC is used to connect remote stations via public or private infrastructures to the TeleControl endpoint (integrated in the WinCC OA server). It contains a telegram buffer for continuous recording of data including time stamp if the communication path is faulty or a communication partner is missing.

The following hardening measures are recommended:

Table 6-12 – Hardening measures TIM 1531 IRC

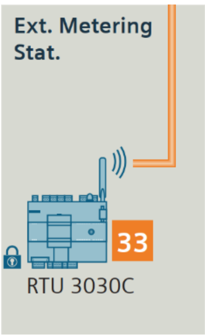
No.	Security Topic	Hardening Measure	Documents
1	MSC protocol	Use of MSCsec	\19\ – Section 1.4
2	Time synchronization	Use of NTP. If available, the secure NTP variant to be used	\19\ – Section 1.4
3	SNMP	Use of SNMPv3	\19\ – Section 1.4
4	Web Server access	Use of HTTPS only	\19\ – Section 1.4

Further information about the configuration of the TIM 1531 IRC provide:

- \19\ – TIM 1531 IRC – Manual

6.6. TeleControl RTU3051C

Figure 6-6 - TeleControl RTU3051C



The compact SIMATIC RTU3051C is used to monitor and control outlying stations that are geographically distributed and not connected to a power supply network. The RTU can store process data and transfer it via mobile wireless to a master station.

To ensure a secure communication between the RTU3051C in the remote station and the TeleControl endpoint, an encrypted communication to the SINEMA RC server is used.

The following hardening measures are recommended:

Table 6-13 – Hardening measures RTU3051C

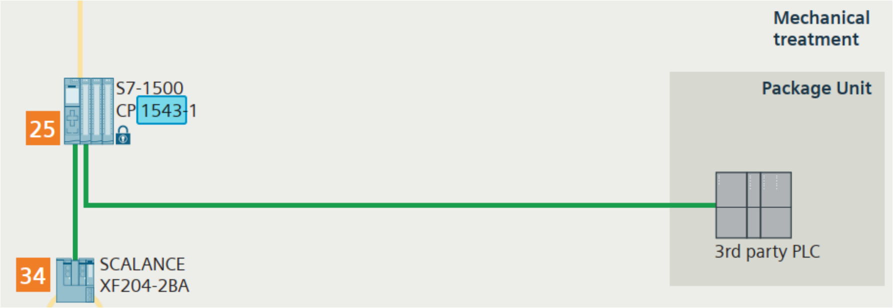
No.	Security Topic	Hardening Measure	Documents
1	VPN	Use of OpenVPN, Configure RTU as OpenVPN client	\20\– Section 3.7 and 6.15.2
2	HTTPS for WAN	HTTPS for WAN enable SMS incoming off	\20\ – Section 6.13
3	Web Server access	Use of HTTPS only	\20\– Section 6.15.3

Further information about the configuration of the RTU3051C provide:

- \20\ – RTU3051C – Operating Instruction

6.7. Industrial Ethernet CP 1543-1

Figure 6-7 - Secure communication via CP 1543-1

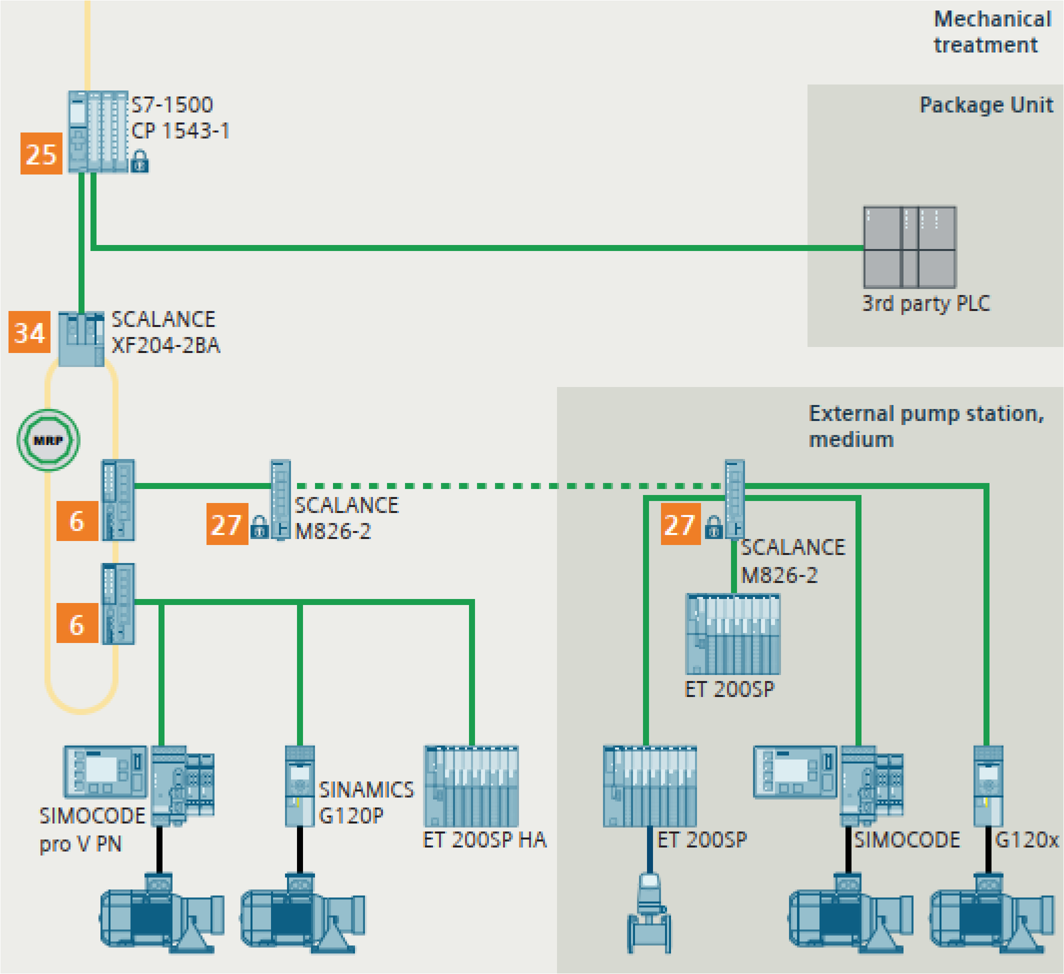


The secure communication within the automation devices S7-1500 and the external systems like the pump station is established in blueprint by the Industrial Ethernet CP 1543-1.

Table 6-14 – CP 1543-1

No.	Device	MLFB
1	SIMATIC NET CP 1543-1	6GK7543-1AX00-0XE0

Figure 6-8 – Use of CP 1543-1



The configuration of the firewall functionalities and VPN tunnel (via IPSec) to external stations is done directly in the TIA engineering tool.

The Industrial Ethernet CP 1543-1 provide the following security functions:

Table 6-15 – Security functions CP 1543-1

No.	Security Function	Description
1	Firewall	• IP firewall with stateful packet inspection (layer 3 and 4) • Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2) • Bandwidth limitation • Global firewall rules
2	Communication made secure by IPsec tunnels	The CP 1543-1 can be grouped together with other security modules during configuration. IPsec tunnels are created between all security modules of a VPN group. All internal nodes of these security modules can communicate securely with each other through these tunnels
3	Logging	To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a syslog server.
4	HTTPS	For the encrypted transfer of Web pages, for example in process control
5	FTPS	For encrypted transfer of files
6	NTP (secured)	For secure time-of-day synchronization and transmission
7	SNMPv3	For secure transmission of network analysis information safe from eavesdropping

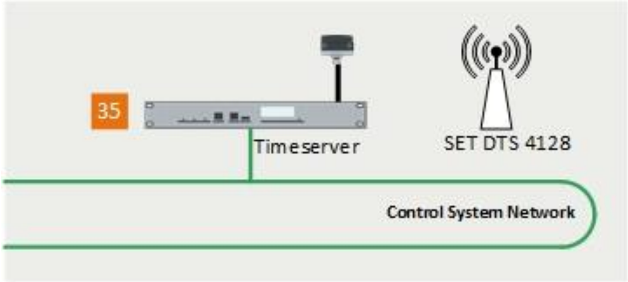
No.	Security Function	Description
8	Protection for devices and network segments	The firewall and VPN protective function can be applied to the operation of single devices, several devices, or entire network segments

Detailed descriptions of the use and configuration of the CP 1543-1 is provided by:

- \22\ – Industrial Ethernet CP 1543-1 Advanced – Manual
- Use of CP 1543-1
- \21\ – Industrial Ethernet Security, basics and application, section 1.8
- Configuration of the firewall in standard mode
- \21\ – Industrial Ethernet Security, basics and application, section 4.1.1
- Configuration of the firewall in advance mode
- \21\ – Industrial Ethernet Security basics and application, section 4.3
- \23\ – SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Communication

6.8. Central Plant Clock

Figure 6-9 - Time synchronization via Timeserver



The central plant clock manages the time centrally for the entire plant and synchronizes all of the other plant components via their interfaces. The central plant clock is connected to the Control System Network.

The Domain Controller receives the time signal from the central plant clock and transfers the time to the server connected on the Control System Network and the DMZ Sub net. The OS Server transfers the time signal to connected OS-Clients.

The automation devices S7-1500 receive the time signal directly from central plant clock.

The recommended secure measures are:

- Use of NTP (Secure).
- Use of SNMPv3.

Further information regarding the configuration of the time synchronization for WinCC OA systems is provided by:

- \25\ WinCC OA Security Guideline (chapter 6.1.2: Highly Secure Large System)

6.9. Workstations and Server

In the Blueprint Wastewater Treatment Plant for all Workstations and Server the Siemens Industrial Workstations (IPC) for WinCC OA are used. On these IPC's the necessary operating system and SIMATIC WinCC OA software is running.

The hardening measures describe in the following sections are valid for Siemens Industrial Workstations (IPC) for WinCC OA

- \41\ – Recommended Security Settings for IPCs in the Industrial Environment
- \25\ – WinCC OA Security Guideline (chapter 6.2.2: Hardening WinCC OA)

6.9.1. General Hardening Measure for Workstation and Server

The following general hardening measures for the workstations and server have to be considered:

Table 6-16 – General Hardening measures for workstations & server

No.	Security Topic	Hardening Measure	Documents
1	Secure Network	Use of the Firewall	\25\ – Section 6.2.2.5
2	Identity and Access Management	BIOS settings	\25\ – Section 6.2.1.3
		User administration with Active Directory and SIMATIC Logon	Detailed description provides section 7
3	Reduction of Surface Attack	Remove unnecessary Windows components	\25\ – Section 6.2.1.1
		Disable Windows services	\25\ – Section 6.2.1
		Disable Automation License Manager (ALM) server functionality if the plant is in operation	\25\ – Section 6.2.1.1
		Enable SMB signing	\25\ – Section 6.2.1.9
		Blocking of USB storage media • Lock or disabling with other mechanical means • Restricting access with Windows group policy	\25\ – Section 6.2.1.5
4	Secure Channels and Encryption	Enable encrypted communication	\25\ – Section 5.6
5	System Integrity	Use of Whitelisting	Detailed description provides section 8 \25\ – Section 6.2.1.11
		Installation of Virus scanner	Detailed description provides section 8 \25\ – Section 6.6
		Digital signatures for application	\25\ – Section 6.2.2.18
		Patching of operating system	Detailed description provides in section 9 \25\ – Section 6.5.2.1.2
		Backup of engineering and system data	Detailed description provides section 10 \25\ – Section 6.9
6	Logging and Monitoring	Use of User Administration	\25\ – Section 6.4.3

Some of the above mention hardening measures can be set in the Group Policy Objects (GPOs) of Windows. In the Blueprint the GPOs are made centrally on the Domain Controller, see section 7.

6.9.2. Additional Hardening Measures

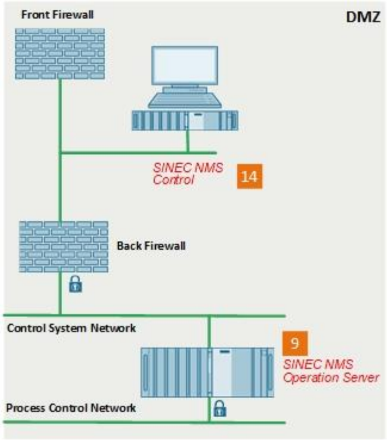
For some of the WinCC OA workstations and server additional hardening measures are recommended.

- \25\ – WinCC OA Security Guideline Hardening (chapter 6.2.2: Hardening WinCC OA)
- \25\ – WinCC OA Security Guideline Hardening (chapter 6.3: Administration and Configuration of OS)

6.9.3. Hardening Measures for SINEC NMS

SINEC NMS is a software for monitoring and administration of networks and their devices and consists of the "Control" component and at least one "Operation" component. In the Blueprint the components of SINEC NMS are configured as shown in the following figure:

Figure 6-10 – Overview of SINEC NMS



- Control is used for monitoring and administration of the entire network
- Operation is used displays detailed information about its monitored devices and displays the devices in network topologies.

The user management of SINEC NMS is implemented by use of the User Management Component (UMC). For WinCC OA the UMC server of SINEC NMS shall be installed. The local user can be integrated into Active Directory on the Domain Controller.

In addition to the hardening measures mention in section 6.9.1 it is recommended to install the SNMPv3 protocol component delivered together with SINEC NMS.

The use of whitelisting is not recommended, because it can influence the functionality of SINEC NMS.

Further information on SINEC NMS provides

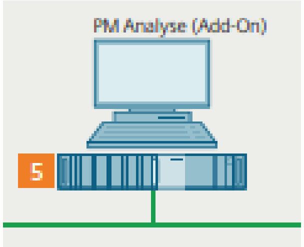
- \28\ – Network management SINEC NMS

6.9.4. Hardening Measures for PM ANALYZE

PM ANALYZE is used in the Blueprint to prepare and create special reports to be conformed with ATV regulations and consists of the following modules:

- PM Server: Installed on the PM ANALYZE Server.
- PM Agent: A HTTPS server installed on the OS Server.
- PM ANALYZE Client.

Figure 6-11 – Overview of PM Analyze



In addition to the hardening measures listed in Table 6-14 the following measure must be considered:

- Whitelisting OS-Sever.
- The use of Whitelisting on the PM ANALYZE station is not recommended.

\29\ – Overview of Premium Add-ons for SIMATIC WinCC

6.9.5. Hardening Measures for SIMATIC Energy Manager Pro

SIMATIC Energy Manager is the energy management system for industry, certified in accordance with ISO 50001. With SIMATIC Energy Manager, energy flows and consumption values are visualized in processes in detail. The values assign to the relevant consumers or cost centers and identify why changes have occurred. The system helps to increase energy efficiency and thus reduce energy costs.

The acquisition component of Energy Manager Pro is communicating via OPU UA (HA) with the WinCC OA Web Server station in the DMZ.

In addition to the hardening measures listed in Table 6-14 the following measure has to be considered:

- SIMATIC Energy Manager Pro uses the Microsoft Information Service (IIS). Recommend setting provide:
- \33\ – SIMATIC Energy Manager PRO V7.5 - Installation, Chapter 3.1

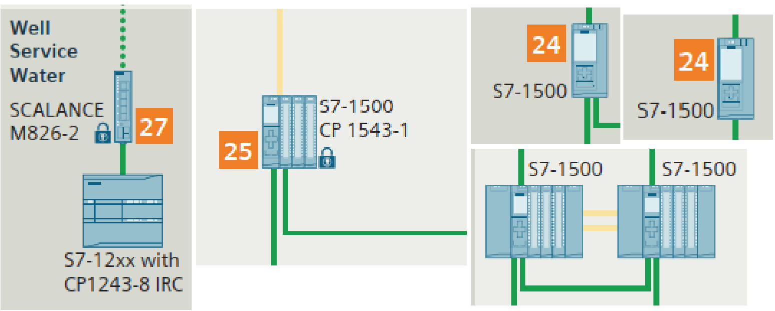
Further information about the SIMATIC Energy Manager Pro provide:

- \31\ SIMATIC Energy Manager PRO V7.5 – Operation
- \32\ SIMATIC Energy Manager PRO V7.5 – Acquisition
- \33\ SIMATIC Energy Manager V7.5 – Installation
- \34\ SIMATIC Energy Manager PRO V7.2 - System Manual

6.10. Automation Devices SIMATIC S7-1500 / S7-1200

In the blueprint, the automation devices SIMATIC S7-1500 and S7-1200 are used to control the main part of the Wastewater Treatment Plant.

Figure 6-12 – S7-1500 / S7-1200



The following configurations of the S7-1500 and S7-1200 automation devices are used in the blueprint:

Table 6-17 – Overview of S7-1500 and S7-1200

SCI	Function	Supplier	Type	MLFB
24	S7-1500 (H), optional redundant	Siemens	PLC with 3 integrated Interfaces for PROFINET and / or Process Control Network Communication. High availability optional.	6ES7515-2AM01-0AB0 6GK7543-1AX00-0XE0
25	Automation Device	Siemens	PLC with 3 integrated Interfaces for PROFINET and / or Process Control Network Communication. CP1543-1 for extra Security communication.	6ES7515-2AM01-0AB0 6GK7543-1AX00-0XE0
27	Automation Device	Siemens	PLC with additional CP1243-8 IRC for telecontrol and secure communication.	6ES7215-1AF40-0XB0

The secure communication between the automation devices and the Process Control Network is implemented in two different ways:

- CP 1543-1:
- For hardening measures and configuration, see Table 6-6.

- SCALANCE SC 624-2C:
- For hardening measures and configuration, see section 6.2.2.

Hardening of SIMATIC PLCs

Siemens PLCs have the following security features that can be applied to safeguard them:

- Access control**:**
- S7-1500 and S7-1200 controllers have an access control mechanism to restrict user access to specific PLC functionalities.

Table 6-18 – Access control rights

Access right	Permissions
HMI access	Only HMI access and access to diagnostics data are possible.
	Tags can be read and written via an HMI device.
Read access	Read-only access to the hardware configuration and the blocks is possible without entering a password.
	Can upload hardware configuration and blocks to the programming device.
	HMI access and access to diagnostics data are possible.
	Can change the operating state (RUN/STOP) and set the time-of-day.
Full access	The hardware configuration and the blocks can be read and changed by all users.
	Full access to all functions, including downloading blocks and hardware configuration into the PLC, executing test functions, changing the operating state (RUN/STOP), and performing firmware updates.

- Secure PG/PC and HMI communication:
- Transport Layer Security protocol (TLS) is used to safeguard PG/PC and HMI communication using standardized security mechanisms.
- Protection of the PLC’s confidential configuration data:
- Password-based protection to encrypt confidential configuration data of the controller (such as private keys for signing and decrypting messages).

Security-By-Default

To mitigate security risks and potential cyberattacks, all security settings are activated by default. This approach ensures protection against unauthorized access and guarantees the integrity and confidentiality of communication data, preventing interception or manipulation.

\23\ SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Communication
https://support.industry.siemens.com/cs/ww/en/view/59192925

- \23\ – SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Communication
    - \24\ – S7-1500 Manual collection
    - \26\ – Security with SIMATIC-S7 controllers
    - \27\ – SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16
    - \45\ – Configuration of the security functions in TIA Portal V17
    - \46\ – User Management & Access Control with TIA Portal V19
    - \47\ – Using Certificates with TIA Portal

7. User Management

User management in the blueprint's Wastewater Treatment Plant is managed centrally by the Active Directory Domain Service installed on the Domain Controller. Due to the centralized user management, the AGLP principle (Account, Global, Domain local, Permission) must be considered. According to this principle, the domain user accounts are initially assigned to the domain-global groups in the Active Directory. These groups are then assigned to local computer groups which, in turn, receive the permissions to the objects. This includes mechanisms for password recovery and reset mechanisms.

The logon user authentication for WinCC OA is based on the Windows domain groups.

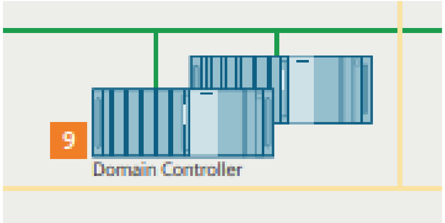
7.1. Domain Controller

The Domain Controller in the blueprint is redundantly designed and installed in Zone 1 – Building, see Figure 3-3. The Domain Controller can be installed in the Demilitarized Zone (DMZ) as well. With this, the administration of the Active Directory Domain Service can be managed by a central IT department.

If the domain controller is installed in the DMZ, it is recommended to install at least one domain controller in the security zone to ensure operation of the automation control system in case the connection to the DMZ fails.

If multiple subnets / security zones are present, at least one domain controller shall be provided in each security zone, depending on the requirements. See Figure 7-1.

Figure 7-1 – Domain Controller in the automation system



- \25\ – WinCC OA Security Guideline (chapter 6.4.3.2.1: Usage of Operating system (Windows or Linux) based user management)

7.2. User Management Component

The User Management Component (UMC) enables the setup of a centralized system for managing users and user groups across various Siemens' software and devices. Users and user groups can be transferred from Microsoft Active Directory.

7.2.1. UMC Ring Server

The UMC ring server represents the central configuration platform for user management. In this server, users are defined with the relevant group assignments for the UMC domain. To transfer users and groups from the Active Directory, the UMC ring server PC must be added to the AD Domain.

The UMC ring server can be realized in a redundant configuration to increase availability.

- \48\ – Central User Management with "User Management Component (UMC)"

7.3. User Authentication and Authorization for WinCC OA

The user authentication and authorization in the blueprint is handled by Windows domain groups, managed with the Active Directory. All personal user accounts at components are assigned to domain groups.

For operating system access, personalized Windows accounts and groups are used, which are centrally managed by the domain controller where all PC based machines in the Control System Network, application bus, and DMZ networks are covered. As personal user accounts are managed by the domain, all user passwords adhere to the complexity requirements.

WinCC OA allows to handle the user administration by Windows domain groups, managed with the Active Directory. This means that the user groups for a user are adopted from the Windows administration.

The group rights for the adopted groups need to be defined in WinCC OA. The user administration can be used like the WinCC OA administration with the exception that users or groups cannot be added or deleted.

When a user logs in, the system checks if the user is known in the system.

Further information on user authentication and authorization provided in:

- \25\ – WinCC OA Security Guideline (chapter 6.4.3.2: Usage of WinCC OA external authentication method)

7.3.1. Benefits of using Active Directory for user authentication

An active directory system allows the usage of mandatory requirements regarding the password strength which can be configured via the group policy editor. With enforced settings, it is possible to ensure good and strong password for users, protecting the project from weak passwords.

Beside a strong password, an Active Directory based user authentication mechanism allows the synchronization of users and groups inside a domain. This simplifies the process of initiating logins to a WinCC OA Client hosted within the same domain.

8. Malware Protection and Application Control

The integrity of the system has to be protected against unauthorized changes of software and data and the unauthorized changes have to be detected, recorded and reported.

In the blueprint the protection against malware and unauthorized changes is implemented using:

- Anti-Virus software:
- The latest version of the Anti-Virus Software McAfee Endpoint Security is installed on workstations and server of the Blueprint. McAfee Endpoint Security (EPS) activates additional functions going beyond the traditional virus scanner
- To ensure that the virus signatures files on all workstations and server are up to date, a virus scanner server is installed on Infrastructure PC in DMZ. This server receives its virus signatures from the update server of the respective virus scan manufacturer on the Internet or from an upstream virus scan server and manages its virus scan clients.
- Whitelisting techniques:
- The latest version of Trellix Application and Change Control is installed on the workstations and server of the Blueprint.
- McAfee Application Control can be used to block the start of unauthorized or unknown applications on workstations and server. After the installation activation of McAfee Application Control, all executable applications and files are protected against modification.

McAfee Endpoint Security and McAfee Application Control are not installed on all workstations and server in Blueprint.

Both, “Trellix Endpoint Security” and “Trellix Application and Change Control” and be configured and managed centralized by using the “Trellix ePolicy Orchestrator (ePO)”. This software is installed on the Infrastructure PC in DMZ.

Further information of the use and configuration Anti-Virus software and Whitelisting provides

- \25\ – WinCC OA Security Guideline (chapter 6.2.1.11: Whitelisting/Application Control)
- \30\ – Trellix Application Control Compatibility
- \38\ – Utilization of Whitelisting with Trellix Application Control for PCS 7 and WinCC

9. Patch Management

9.1. Patch Management for WinCC OA Components

IEC 62443 recommends the Defense-in-Depth concept as comprehensive protection of industrial facilities against cyberattacks. The protection of system integrity is one important part of the Defense-in-Depth concept, see section 5.5.

One measure to protect the system integrity of an automation control system is patch management as part of the comprehensive security concept.

Patch management is the systematic procedure for installing patches on the automation control system. Patches differ in:

- Patches for the Operating System Microsoft Windows.
- These are all types of updates, service packs, feature packs and similar installations, regardless as to whether or not these relate to security.
- Security updates for Operating System Microsoft Windows for security-related up-dates.
- Firmware and software patches because of vulnerabilities, both for Siemens software and products, and 3rd party components.

For Siemens software and products, security vulnerabilities are handled by the responsible Siemens product unit. This applies also for vulnerabilities in third-party components of a Siemens product, which will also be handled by the respective Siemens product unit.

Security vulnerabilities in 3rd-party components which are not owned by Siemens the plant owner has the responsibility to ensure that these components are during operation on the latest patch level.

The Windows Server Update Service (WSUS) installed on the Infrastructure PC in the DMZ of the Blueprint manages the Windows patches for the automation control system. The WSUS can receive the Windows patches either from the Microsoft Update server or from the server in the customer enterprise network. The WSUS is distributing the patches to all Windows-based PC's of the automation control system.

However, Microsoft has announced the deprecation of WSUS in 2025. Deprecation occurs when a product is no longer actively developed and might be removed in future updates. Currently, Microsoft are not planning to remove WSUS from Windows Server versions, including Windows Server 2025, and will continue to maintain it, but no new features will be added.

For all products from Siemens including third party components, Siemens is publishing on monthly basis advisories. The advisories are published here:

- https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications

Further information about patch management and WSUS provides

- \25\ – WinCC OA Security Guideline (chapter 6.5: Patch management and security updates)

9.2. Patch Management of Automation and Network Components

New firmware of automation devices shall be managed via the infrastructure PC. In case of SCALANCE network components, firmware updates shall be centrally deployed via SINEC NMS.

10. Backup and Recovering

Recovering and reconstituting an automation control system to a known state after a disruption of failure is an important topic in the Defense-in-Depth concept and recommended in the IEC 62443.

In a Backup and Restore strategy all the data which are necessary for recover and their loaction in the system are identified. The frequency of creating backups, the kind of backup (complete, differential or incremental) and the storage location of the backups are described in this strategy.

Data backup will be categorized as following:

- System Backup:
- System backup refers to a complete system image, e.g. a snapshot of current system. Following data is included:
  - Hardware-specific files (drivers).
  - Windows operating system files and settings.
  - Installed programs and their configurations.
  - Host devices (Hardware-specific files (drivers), Windows operating system files and settings, Installed programs and their configurations).
  - For system backup, Symantec System Recovery is recommended.
- Project Backup:
- Project backup mainly refers to the backup of the WinCC OA project.
- Component specific Data:
- Component specific data like databases~~,~~ or individual configuration of embedded or network devices requires to be backed up. SINEC NMS is used for component backup

Restoring systems is more critical than the creation of backups. This process has to be tested and reproduced to guarantee fast availability of the plant systems in case of emergency and minimize downtimes.

Further information about Backup and Restore provides

- \25\ – WinCC OA Security Guideline (chapter 6.9: Implement Backup and Restore concept)

11. Optional Security Measures

The configuration and hardening measure described in section 6 together with the security measures described in section 5 ensure a high level of the security and comprehensive protection based on the defense-in-depth concept.

With the use of further security measures, the level of security for an automation control system can be further increased. The following sections describe some of these measures, Siemens is providing.

Further information about the optional security measures provides

- \40\ – Siemens Industrial Security Service

11.1. Threat Prevention Subscription for Font- and Back-Firewalls

The Palo Alto Next Generation Firewalls described in section 6.2.1 can be enhanced with the Threat Prevention Subscription (TPS) option. We recommend the use of the TPS option if remote access is installed.

The Threat Prevention Subscription (TPS) includes an Intrusion Prevention and Detection System (IPS / IDS). TPS adds integrated protection against network-borne threats, including exploits, malware, command and control traffic, and a variety of hacking tools, through IPS functionality and stream-based blocking of millions of known malware samples. This TPS option must be ordered for every Automation Firewall Next Generation in addition.

Industrial Vulnerability Manager

Software and Hardware components embedded in Automation Control Systems and products are regularly affected by security flaws that shall be mitigated in order to reduce the risk of cyber-attacks on plants and factories. As part of a global patch management concept, it is needed to monitor the individual hardware and software components over the time in order to identify the flaws affecting them.

The Industrial Vulnerability Manager has the following features:

- Hosting of the list of components embedded in your ICS that shall be monitored over the time with regards to security flaws.
- Free assignment of the components to the created monitoring list.
- Integration with:
  - SIMATIC Management Console.
  - SINEC NMS.
  - TIA Portal.
  - Proneta.
  - SiESTA.
- Dashboards with charts and diagrams to highlight relevant information concerning the published security bulletins.
- Automatic release of security bulletins as soon as a new security flaw affecting a registered component is published by its component vendor.
- The security bulletins that are automatically generated contain the following information:
  - Description of the vulnerability.
  - CVSS (Common Vulnerability Scoring System) score and Priority status.
  - List of affected components.
  - Recommendations, workarounds and patch status.
  - Vendor advisory link.
- Assignment of a tag to the published security bulletins with regards to the handling status (“Open”, “Ongoing”, ”Closed”).
- The application is accessible via a secured web interface.

Industrial Anomaly Detection

The Siemens Industrial Anomaly Detection (IAD) is an important addition to the comprehensive Defense in Depth concept. It provides full transparency over the communication within an automation control system and the information how the components communicate with each other. Due to this, deviations can be easily detected and investigated by the plant owner.

The Siemens Industrial Anomaly Detection (IAD) can seamlessly be integrated in an automation control system and the following functionalities:

- Connection to the IAD sensor is implemented via a SPAN port (Switched port analyzer – mirror port)
- One sensor can work with the data of several SPAN ports
- Central console is used to monitor also the sensors
- Visualization and analysis are provided by the central console
- Sensor and center are installed on a Siemens IPC
- Events from the central console could be easily forwarded e.g. to a SIEM system

With SINEC Security Monitor, Siemens has launched a product on the market that enables network traffic to be mirrored and analyzed, thus enabling passive, continuous identification of all assets in the network. In addition, targeted active scans can be started with low impact if required. The detected assets are compared with an extensive database of known vulnerabilities to identify devices affected by vulnerabilities. Furthermore, the software is able to learn what normal communication in the network looks like and can detect anomalies using AI-based analysis.

Security Information Event Management (SIEM)

Rapidly growing cyber threats and evolving security risks require a preventive and industry-specific defense strategy.

Effective security starts with an overview of all the activities on systems, networks, databases and applications. To protect industrial automation systems against cyber threats, a security information and event management system (SIEM) can be used. This means safety-relevant incidents can be detected more quickly, plant operators informed earlier, and countermeasures initiated more quickly.

A SIEM system collects continuously network information and information from security devices, links it all up, analyzes and displays it, and derive the appropriate security measures.

SIMATIC Security Service Packages

Many of the SIMATIC products offer configurations to enhance the security level. However, these configurations are rarely found in the field – often due to a lack of security know-how.

Our industrial security experts support you in unleashing the full potential of your asset’s security level with tailored packages for SIMATIC automation systems.

Your benefits:

- Transparency over compliance with security standards.
- State-of-the-art implementation and configuration of security features.
- Maintaining the security level over the whole lifecycle.

Security Services can be ordered at your local Siemens contact person, see:

- \44\ – Industrial Security Services – Security Optimization – SIMATIC Security Service Packages

12. Links and Literature

Table 12-1 – Link list

No.	Document
\1\	All-round protection with Industrial Security - System Integrity https://support.industry.siemens.com/cs/de/en/view/92605897
\2\	All-round protection with Industrial Security - Network Security https://support.industry.siemens.com/cs/de/en/view/92651441
\3\	All-round protection with Industrial Security - Plant Security https://support.industry.siemens.com/cs/de/en/view/50203404
\4\	Siemens Industry Online Support https://support.industry.siemens.com/cs/ww/en/
\5\	Checklist for Setting Up SCALANCE Devices https://support.industry.siemens.com/cs/ww/en/view/109745536
\6\	PAN-OS® Administrator's Guide https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/getting-started
\7\	Palo Alto Website about PAN-OS https://docs.paloaltonetworks.com/pan-os.html
\8\	SCALANCE SC-600 – Web Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109754815
\9\	SCALANCE SC-600 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109754812
\10\	SCALANCE M800 Web – Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109751635
\11\	SCALANCE M874, M876 – Operating Instructions https://support.industry.siemens.com/cs/document/109972231
\12\	SCALANCE M826 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/99450800
\13\	SCALANCE M874, M876 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/74518712
\14\	SCALANCE WAM766 – Operating Instructions https://support.industry.siemens.com/cs/document/109973939
\15\	SCALANCE WUM763 – Operating Instructions https://support.industry.siemens.com/cs/document/109973938
\16\	SCALANCE XC-200 / XF-200BA Web – Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109750283
\17\	SCALANCE XC-200 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109743149
\18\	SCALANCE XF-200BA – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109750282
\19\	TIM 1531 IRC – Manual https://support.industry.siemens.com/cs/de/en/view/109748454
\20\	RTU3051C – Operating Instruction https://support.industry.siemens.com/cs/ww/en/view/109750942
\21\	Industrial Ethernet Security basics and application – Configuration Manual https://support.industry.siemens.com/cs/ww/en/view/109738463
\22\	SIMATIC NET: S7-1500 - Industrial Ethernet CP 1543-1 https://support.industry.siemens.com/cs/document/109973328

\23\ SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Communication
https://support.industry.siemens.com/cs/ww/en/view/59192925

\24\ S7-1500 Manual Collection
https://support.industry.siemens.com/cs/de/en/view/86140384

\25\ WinCC OA Security GuidelineLatest , registration required
https://www.winccoa.com/downloads/category/safety-security.html

\26\ Security with SIMATIC-S7 controllers
https://support.industry.siemens.com/cs/de/en/view/77431846

\27\ SIMATIC STEP 7 Basic/Professional V18 and SIMATIC WinCC V18
https://support.industry.siemens.com/cs/document/109815056

\28\ Network management SINEC NMS
https://support.industry.siemens.com/cs/de/en/view/109762749

\29\ PM Analyze
https://www.siemens.com/global/en/products/automation/industry-software/automation-software/scada/pm-add-ons.html

\30\ Trellix Application Control Compatibility
https://support.industry.siemens.com/cs/document/88653385

\31\ SIMATIC Energy Manager PRO V7.5 – Operation
https://support.industry.siemens.com/cs/document/109963217

\32\ SIMATIC Energy Manager PRO V7.5 – Acquisition
https://support.industry.siemens.com/cs/document/109963216

\33\ SIMATIC Energy Manager V7.5 Installation https://support.industry.siemens.com/cs/document/109963215

\34\ SIMATIC Energy Manager PRO V7.2 - System Manual
https://support.industry.siemens.com/cs/ww/en/view/109748841

\35\ SIMATIC NET: Industrial Remote Communication - Remote Networks SINEMA Remote Connect Operating Instructions
https://support.industry.siemens.com/cs/ww/en/view/109482122

\36\ Application example – Understanding and Using Firewall of Industrial Security Appliance
https://support.industry.siemens.com/cs/ww/en/view/22376747

\37\ Overview: Secure Remote Access with VPN
https://support.industry.siemens.com/cs/ww/en/view/26662448

\38\ Utilization of Whitelisting with Trellix Application Control for PCS 7 and WinCC
https://support.industry.siemens.com/cs/ww/en/view/88653385

\39\ Palo Alto - Best Practices for Securing Administrative Access section
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

\40\ Siemens Industrial Cybersecurity Services
https://new.siemens.com/global/en/products/services/industry/digital-industry-services/industrial-security-services.html

\41\ Recommended Security Settings for IPCs in the Industrial Environment
https://support.industry.siemens.com/cs/de/en/view/109475014

\42\ SIMATIC Process Control System PCS 7 Security concept PCS 7 & WinCC (Basic)
https://support.industry.siemens.com/cs/document/109973483

\43\ User administration for SCALANCE devices with RADIUS protocol
https://support.industry.siemens.com/cs/ww/en/view/98210507

\44\ Enabling 2FA for SCALANCE devices
https://support.industry.siemens.com/cs/ww/en/view/109954344

\45\ Configuration of the security functions in TIA Portal V17
https://support.industry.siemens.com/cs/ww/en/view/109798583

\46\ User Management & Access Control with TIA Portal V19
https://support.industry.siemens.com/cs/ww/en/view/109973173

\47\ Using Certificates with TIA Portal
https://support.industry.siemens.com/cs/ww/en/view/109769068

\48\ Central User Management with "User Management Component (UMC)"
https://support.industry.siemens.com/cs/ww/en/view/109780337

\49\ SIMATIC NET: Network management SINEC INS
https://support.industry.siemens.com/cs/ww/en/view/109781023

\50\ Sending SIMATIC S7-1200/S7-1500 CPU Security Messages via Syslog to SINEC INS
https://support.industry.siemens.com/cs/ww/en/view/51929235

\51\ Security events in WinCC OA

https://www.winccoa.com/documentation/WinCCOA/latest/en_US/security_events/security_events.html

13. Attachment – List of security measures according to IEC 62433-3-3

This chapter describes the duties of the different stakeholders according to IEC 62433-3-3
(**SS**: System Supplier Siemens, **SI**: System Integrator, **EC**: End customer)

WinCC OA Chapter refers to the WinCC OA Security Guideline

https://www.winccoa.com/downloads/category/safety-security.html (registration required)

IEC 62443-3-3 Level 1			Chapter	WinCC OA Chapter
SR 1.1	Human user identification and authentication	SS: all different systems (WinCC, Windows OS, S7-1500, SCALANCE, TIA, SINEC NMS) provide the possibility for a user management SI: user authentication must be enabled and preconfigured for all systems	5.2.1	• User Administration • Activate Kerberos encryption for WinCC OA systems
SR 1.3	Account management	SS: all different systems (WinCC, Windows OS, S7-1500, SCALANCE, TIA, SINEC NMS) provide the possibility to manage user and roles		• Activate Kerberos encryption for WinCC OA systems
SR 1.4	Identifier management	SS: possible for all systems SI: must configure the unique identity		• Activate Kerberos encryption for WinCC OA systems
SR 1.5	Authenticator management	SS: possible for all systems		• Delete or disable unneeded default users on OS Level • Delete or disable all default users on WinCC OA level • Limit usage of the root user
SR 1.7	Strength of password-based authentication	SS: possible for all systems SI: must configure the minimum password requirements	6.1	• Single Sign On • Password strength
SR 1.10	Authenticator feedback	SS: fulfilled for all systems	5.2.1	• Usage of Operating system (Windows or Linux) based user management
SR 1.11	Unsuccessful login attempts	SS: fulfilled for Windows OS; all other systems through AD integration SI: must install and configure AD and brute force protection EC: must decide which system needs brute force protection	5.2.1	• Single Sign On
SR 1.12	System use notification	mainly needed for remote connections SS: possible for Windows OS, SCALANCE, WinCC OA SI: must configure and display the unique	5.2.1	• Configure System use notification

		system name for all different systems (WinCC faceplate, Windows Background, SCALANCE)		
SR 1.13	Access via untrusted networks	SS: possible, for example through VPN on the Automation Firewall	5.6.1	N/A on WinCC OA level, information available on System Level • Security Cells and Network Architecture
SR 2.1	Authorization enforcement	SS: functionality is based on Windows, WinCC OA and SCALANCE network components. These enforce this functionality SI: if non-Siemens components are used SI must ensure proper functionality		• Administration of Role-Based user authorizations
SR 2.3	Use control for portable and mobile devices	SS: blueprint has to include concept for hardening regarding data ports (USB, Ethernet,) SI: must implement the concept EC: must follow the concept		
SR 2.4	Mobile code	SS: blueprint has to include concept to prevent mobile code execution (macros, java, script, ActiveX...). Concept has to be based on Desktop UI Clients. Concept should exclude web clients => no mobile code needed SI: Implement hardening concept (execution of mobile code has to be disabled)		• WinCC OA User Interface Configuration • Whitelisting/Application Control
SR 2.5	Session lock	SS: functionality integrated in SCALANCE, WinCC OA and Windows; blueprint has to include advisories SI: must configure the log off function according to end customer requirement and blueprint advisories		• Automatic User Logout in WinCC OA
SR 2.8	Auditable events	SS: functionality integrated in SCALANCE, WinCC OA and Windows; WinCC OA provides logs		• User Administration • Activate Kerberos encryption for WinCC OA systems
SR 2.9	Audit storage capacity	SI: must provide enough storage capacity for log and process data for specific amount of time according to end customer / legal requirement WinCC OA provides logs		• Configure Fail-Safe mode of WinCC OA (Emergency Mode)
SR 2.10	Response to audit processing failures	WinCC OA provides logs		• Configure Fail-Safe mode of WinCC OA (Emergency Mode)
SR 3.1	Communication integrity	SS: communication integrity will be protected by TCP/IP mechanisms		• Usage of TLS/SSL for plant communication • Activate Kerberos encryption for WinCC OA systems

SR 3.2	Malicious code protection	SS: blueprint recommendation should be whitelisting; tested antivirus solutions are an alternative SI: must implement and configure the malware protection EC: must frequently update the patterns if antivirus solution is chosen		N/A on WinCC OA level, information available on System Level • Virus Scanner
SR 3.3	Security functionality verification	SI: must develop a checklist to verify the implementation of security measures after FAT, SAT and maintenance phase		• Virus Scanner • Security tests
SR 3.4	Software and information integrity	SS: Software should be protected through whitelisting and WinCC OA binary signatures. TIA / S7-1500 should be protected through UMC and protection level and online/offline check. WinCC OA protection must be described in the blueprint how to protect WinCC OA project data through Windows mechanisms. WinCC OA is still working to fulfill the requirement, should come in version 3.17 SI: must implement and configure security measures		• Digital signatures for binaries and libraries • Whitelisting/Application Control
SR 3.5	Input validation	SS: WinCC OA provides the functionality to validate inputs SI: must implement the syntax and content validation in the project		• Penetration tests
SR 4.1	Information confidentiality	SS: provided for Windows, WinCC OA and devices through user authentication and encryption SI: must implement and configure user right management EC: must define and establish process to store and transfer confidential data		Usage of TLS/SSL for plant communication • Activate Kerberos encryption for WinCC OA systems • Protection via authorization levels in WinCC OA
SR 4.3	Use of cryptography	SS: encrypted data (passwords) is stored according to best practices		• Usage of encrypted communication protocols • IPsec Bypass Technology • Usage of TLS/SSL for plant communication
SR 5.1	Network segmentation	SS: Blueprint setup implements automation network segmentation	5.1.1	• Security Cells and Network Architecture
SR 5.2	Zone boundary protection	SS: blueprint has to include firewall and zone concept (DMZ, external connection and especially internal network segments) SI: has to implement and configure firewall and zones	5.2.1	N/A on WinCC OA level, information available on System Level • Security Cells and Network Architecture

SR 5.3	General purpose person-to-person communication restrictions	SS: the blueprint should include blocking of person - person communication from IT / office network to the automation network (receiving of messages) in the zone concept SI: must implement and configure the blocking (in the firewall configuration)	N/A on WinCC OA level, information available on System Level • Security Cells and Network Architecture
SR 5.4	Application partitioning	SS: blueprint should define separate devices for critical functions like firewall, quarantine station, AD controller, WinCC OA server. Less critical functions like WSUS can be separated in instances (VMs). SI: must implement the functions on the devices	
SR 6.1	Audit log accessibility	SS: WinCC audit logs are accessible as Windows files	• Definition of Access Control List (ACL) • Secure Desktop – Kiosk-Mode
SR 7.2	Resource management	SS: blueprint needs to describe measures like hardening, resource planning, monitoring of resources (bandwidth, storage, CPU load, memory load...) SI: must implement resource management measures, monitoring and alarming EC: need to react on alarming	• Keep secure settings in WinCC OA config file • Configure Fail-Safe mode of WinCC OA (Emergency Mode)
SR 7.3	Control system backup	SS: blueprint need to include backup concept of OS, user software, projects, log data, configurations, ... SI / EC: need to define backup concept including backup schedules and responsibilities	• Implement Backup and Restore concept
SR 7.4	Control system recovery and reconstitution	SI: has to do a full system backup and test the restore to ensure recovery and reconstitution	• Restore procedure
SR 7.5	Emergency power	SS: blueprint must mention the need of emergency power SI / EC: must define the needed emergency power and implement it	
SR 7.6	Network and security configuration settings	SI: must implement the security guideline from SS (this document)	• Division in security cells
SR 7.7	Least functionality	SS: blueprint describes measures like hardening and user management SI: must implement least functionality according to hardening and user management guidelines	• Hardening

IEC 62443-3-3 Level 2			Chapter	WinCC OA Chapter
SR 1.1 RE 1	Unique identification and authentication	SS: all different systems (WinCC, Windows OS, S7-1500, SCALANCE, TIA, SINEC NMS) provide the possibility for a user-based Active Directory-based management SI: AD, UMC and interconnection (AD -> UMC, AD -> SCALANCE, AD -> OPC_OA, UMC -> TIA) configuration	5.2.1	• User Administration • Activate Kerberos encryption for WinCC OA systems
SR 1.2	Software process and device identification and authentication	SS: User authentication in windows, RADIUS identification at switches SI: must implement and configure identification EC: need to document the exchange process; new MAC address must be added in the RADIUS	5.2.1	• Server-side Authentication for Managers with session binding • Usage of TLS/SSL for plant communication
SR 1.8	Public key infrastructure (PKI) certificates	SI: if PKI is used, the implementation must be operated according to best practices	5.2.1	• Usage of TLS/SSL for plant communication
SR 1.9	Strength of public key authentication	SI: if PKI is used, the implementation must be operated according to best practices	5.2.1	• Enforce usage of strong cipher suite
SR 2.1 RE 1	Authorization enforcement for all users			• Administration of Role-Based user authorizations • Limit usage of the root user
SR 2.1 RE 2	Permission mapping to roles	SS: functionality is based on Windows, WinCC OA and SCALANCE network components. These enforce this functionality SI: must configure role-based permissions EC / SI: must map users to roles		• Single Sign On
SR 2.6	Remote session termination	SS: must be described in the blueprint; examples how to technically implement it (key switch for SCALANCE M as SINEMA RC endpoint. Can also be triggered through an output from PLC to automate the logout) SI: must implement a solution from the blueprint to terminate remote connection after specific amount of time and on demand		• Automatic User Logout in WinCC OA
SR 2.11	Timestamps	SS: functionality is based on Windows, WinCC OA and SCALANCE network components.		• Usage of TLS/SSL for plant communication • Integrity with MAC
SR 3.2 RE 1	Malicious code protection on entry and exit points	SS: fulfilled with quarantine station in the blueprint (local and remote transfer of data) SI: must implement and configure the solution		
SR 3.7	Error handling	SS: provides error analysis solutions SI, EC: can forward information; must provide minimal data based on "need to know principle"		• Penetration tests • Implement Risk assessment

				process based on VDI/VDE 2182
SR 3.8	Session integrity	SS: WinCC provides TLS security by default SI: must not disable TLS		• Server-side Authentication for Managers with session binding
SR 3.9	Protection of audit information	SS: Windows provides functionality to protect the security log. WinCC OA protects user interactions logs SI: must implement and configure user management according to the blueprint (Windows, WinCC OA, devices, log server...)		• Secure Desktop – Kiosk-Mode
SR 4.1 RE 1	Protection of confidentiality at rest or in transit via untrusted networks	SS: transfer via untrusted network (remote service) is secured through VPN in the blueprint SI: must implement and configure VPN		• Usage of TLS/SSL for plant communication • Activate Kerberos encryption for WinCC OA systems • Protection via authorization levels in WinCC OA
SR 4.2	Information persistence	SI / EC: must define, implement and configure data purge process		• System Decommissioning
SR 5.2 RE 1	Deny by default, allow by exception	SS: blueprint should include firewall configuration example for needed WinCC OA / automation communication (ethernet protocol, ports and applications... which are needed for NG features) SI: must implement and configure the firewall settings	5.1.2	N/A on WinCC OA level, information available on System Level • Security Cells and Network Architecture
SR 6.2	Continuous monitoring	SS: blueprint need to include and describe a continuous monitoring system (for example a SIEM or IAD). SI: need to implement and configure the continuous monitoring system		Handling of Security Incidents
SR 7.1 RE 1	Manage communication loads	SS: blueprint need to describe the capability of the SCALANCE devices and the firewall for managing communication loads SI: must implement devices capable to manage communication loads and configure the rate limitation	5.1.5	• Keep secure settings in WinCC OA config file • Usage of WinCC OA mxProxy and restriction of open ports
SR 7.3 RE 1	Backup verification	SS: blueprint need to mention backup verification SI / EC: need to define who is responsible for backup verification and implement the process		• Backup verification
SR 7.8 RE 1	Automation solution or IT infrastructure component inventory	SS: blueprint should mention the need and possibilities of asset management SI / EC: have to define and implement asset management		• Hardening

IEC 62443-3-3 Level 3			Chapter	WinCC OA Chapter
SR 1.3 RE 1	Unified account management	SS: possible for all systems SI: must configure unified accounts		• Activate Kerberos encryption for WinCC OA systems
SR 1.5 RE 1	Hardware security for software process identity credentials			• Single Sign On
SR 1.7 RE 1	Password generation and lifetime restrictions for human users	SS: Windows OS provide these options. All other systems can provide this capability by using AD authentication SI: must install and configure AD authentication	6.1	• Single Sign On • Password strength
SR 1.9 RE 1	Hardware security for public key authentication	SI: must be implemented in the PKI solution		Not yet available
SR 1.13 RE 1	Explicit access request approval		5.6.1	N/A on WinCC OA level, information available on System Level • Protected Maintenance Access of Access via untrusted networks
SR 2.3 RE 1	Enforcement of security status of portable and mobile devices	SS: blueprint has to include concept for quarantine station SI: must implement the concept EC: must follow the concept		
SR 2.4 RE 1	Mobile code integrity check	SS: integrated in the hardening concept; no mobile code needed in the concept SI: must implement hardening concept		• Whitelisting/Application Control • Mobile Code
SR 2.7	Concurrent session control	SS: blueprint already defines a secure infrastructure (VNC...) SI: must implement and configure DMZ and VNC		Not yet available
SR 2.8 RE 1	Centrally managed, system	SS: blueprint should include Log server SI: must implement log server and configure all components to send logs to the server		• User Administration • Activate Kerberos encryption for WinCC OA systems
SR 2.9 RE 1	Warn when audit record storage capacity threshold reached	SS: WinCC OA has the option to configure alarms for disk usage SI: choose log server which has the capability		• Configure Fail-Safe mode of WinCC OA (Emergency Mode)

		to send alarms. And must configure WinCC OA and log server accordingly to alarm the EC		
SR 2.11 RE 1	Internal time synchronization	SS: blueprint must include time server, all devices (SCALANCE, Windows, WinCC OA) has capability to synchronize SI: must implement and configure server and clients to synchronize		• Usage of TLS/SSL for plant communication • Integrity with MAC
SR 2.12	Non-repudiation	SS: WinCC OA has the option to log (configured) human user interactions		• User Administration • Server-side Authentication for Managers with session binding • Integrity with MAC
SR 3.1 RE 1	Cryptographic integrity protection	SS: WinCC OA Client <-> Server is always TLS secured. WinCC <-> S7-1500 should be OPC-UA with encryption; must be defined in the blueprint SI: must implement according to blueprint		• Usage of TLS/SSL for plant communication • Activate Kerberos encryption for WinCC OA systems
SR 3.2 RE 2	Central management and reporting for malicious code protection	SS: Whitelisting and antivirus solutions from Siemens provide centralized management SI: must implement and configure the centralized management		N/A on WinCC OA level, information available on System Level • Virus Scanner
SR 3.3 RE 1	Automated mechanisms for security functionality verification	SI: must develop and implement an automated solution to verify the implementation of security measures after FAT, SAT and maintenance phase		Not yet available
SR 4.2 RE 1	Purging of shared memory resources	SI / EC: must define, implement and configure data purge process of volatile memory resources		Usage of TLS/SSL for plant communication • System Decommissioning
SR 5.1 RE 2	Independence from non-control system networks	SS: yes, no connection to other networks is needed	5.1.1	• Security Cells and Network Architecture
SR 5.2 RE 2	Island mode	SS: blueprint should include examples for island mode concept including the process and technical implementation to switch to island mode	5.1.2	NA
SR 5.2 RE 3	Fail close	SS: the blueprint must define a zone architecture which provide the capability of independent, full operation of each segment SI: must implement the zone concept according to the blueprint	5.2.1	
SR 5.3 RE 1	Prohibit all general-purpose person			N/A on WinCC OA level, information available on System Level

				• Security Cells and Network Architecture
SR 6.1 RE 1	Programmatic access to audit logs	SS: audit logs are available as windows files. Programmatic access through 3rd party tools / scripts SI: has to check with EC if necessary and implement		• Required knowledge • Detection of security incidents
SR 7.1 RE 2	Limit DoS effects to other systems or networks	SS: blueprint need to describe various measures to limit possibility and effects of DoS. Especially the capability of the SCALANCE devices and the firewall for managing communication loads, system hardening, user rights management SI: must implement described measures	5.1.5	
SR 7.3 RE 2	Backup automation	SS: blueprint need to mention automation for backup options SI: need to implement backup automation		
SR 7.6 RE 1	Machine-readable reporting of current security settings	SI / EC: have to define and implement automated reporting of current security settings		• Secure handling of WinCC OA ASCII Manager

IEC 62443-3-3 Level 4			Chapter	WinCC OA Chapter
SR 1.1 RE 3	Multifactor authentication for all networks	SS: available for Windows OS SI: implementation and configuration	5.2.1	
SR 1.7 RE 2	Password lifetime restrictions for all users	SS: Available for WinCC OA and other systems and devices connected to AD except for local admin accounts SI: must configure password, certificate expiration for all accounts and users EC: must handle expiring accounts; must change local admin accounts where automatic expiration is not possible after specific time	6.1	• Usage of WinCC OA external Single Sign On • Password strength
SR 2.11 RE 2	Protection of time source integrity	SS: blueprint should describe secure time source (SICLOCK) SI: must configure security for the time source according to the blueprint		• Usage of TLS/SSL for plant communication • Integrity with MAC
SR 2.12 RE 1	Non	SS: all actions (humans, WinCC OA software component...) can be logged in WinCC OA SI: must configure and activate logging		• Usage of encrypted communication protocols • Integrity with MAC
SR 3.3 RE 2	Security functionality verification during normal operation	SI: must develop and implement an automated solution to verify the implementation of security measures during normal operation		Not yet available
SR 3.9 RE 1	Audit records on write	SI / EC: must implement, configure and use RO media concept for audit logs		

SR 4.1 RE 2	Protection of confidentiality across zone boundaries	SS: transfer through zone boundaries is secured through VPN in the blueprint SI: must implement and configure VPN

14. Appendix

14.1. Service and support

SiePortal

The integrated platform for product selection, purchasing and support - and connection of Industry Mall and Online support. The SiePortal home page replaces the previous home pages of the Industry Mall and the Online Support Portal (SIOS) and combines them.

- Products & Services
  In Products & Services, you can find all our offerings as previously available in Mall Catalog.
- Support
  In Support, you can find all information helpful for resolving technical issues with our products.
- mySieportal
  mySiePortal collects all your personal data and processes, from your account to current orders, service requests and more. You can only see the full range of functions here after you have logged in.

You can access SiePortal via this address: sieportal.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.
Please send queries to Technical Support via Web form: support.industry.siemens.com/cs/my/src

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.
For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page: siemens.com/sitrain

Industry Online Support app

You will receive optimum support wherever you are with the "Industry Online Support" app. The app is available for iOS and Android:

Available on the App Store

ANDROID APP ON Google play