Siemens
Industry
Online
Support

APPLICATION EXAMPLE

WinCC Unified Security Blueprint for a Wastewater / Water Treatment Plant

Guideline for Secure Configuration V1.0

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. **The application examples are not subject to standard tests and quality inspections of a chargeable product and may contain functional and performance defects or other faults and security vulnerabilities. You are responsible for the proper and safe operation of the products in accordance with all applicable regulations, including checking and customizing the application example for your system, and ensuring that only trained personnel use it in a way that prevents property damage or injury to persons. You are solely responsible for any productive use.**

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. Any further use of the application examples is explicitly not permitted and further rights are not granted. You are not allowed to use application examples in any other way, including, without limitation, for any direct or indirect training or enhancements of AI models.

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 and to terminate your use of the application examples at any time. 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://www.siemens.com/global/en/general/terms-of-use.html) shall also apply.

Cybersecurity information

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

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

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

For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry.

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

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

1. Preface

Cybersecurity needs to be considered as a holistic approach that covers not only the technology, but also the implemented processes based on valid standards such as ISO 27001 (ISMS/IT) and IEC 62443 (IACS/OT).

Therefore, Industrial Automation and Control Systems (IACS) require a comprehensive and established cybersecurity framework which addresses and – where applicable – implements security policies, procedures, and guidelines to ensure a secure operation of the plant.

This blueprint is intended to provide basic guidance for end customers, original equipment manufacturers, and system integrators to securely set up water and wastewater treatment plants. The document serves as a minimum design reference in addition to the product documentation of the automation devices.

Experience has shown that subsequent modernization or plant expansion work is made much easier if the automation project is configured 'in conformance with security standards' as far as possible right from the start. Consequently, users shall adhere to certain rules to ensure that the security functional requirements will offer the required security level in the future.

The recommended methodology, the Defense-in-Depth concept, is based on the IEC 62443 standard and the results of many practical experiences.

SIMATIC WinCC Unified

At the core of the blueprint is SIMATIC WinCC Unified, the preferred SCADA system for small-scale water and wastewater treatment plants. WinCC Unified combines SIMATIC HMI and SCADA into a single product, enabling the configuration and management of runtimes for various device types through one unified engineering system. This centralized approach ensures consistent implementation of security policies, protective measures, and system hardening throughout all visualization devices used in the plant.

NOTICE

Assessing risks for customer projects

A risk assessment, i.e. Threat and Risk Analysis (TRA), must be carried out for each customer project, even if the blueprint is implemented exactly as described.

In the TRA, on which the blueprint is based, assumptions were made regarding the protection level and the impact on the plant in the event of a successful cyber-attack. These assumptions may vary per customer, which could also result in a different risk level. The blueprint is a model solution/proposal on how security requirements from the IEC 62443, among others, can be implemented in the best possible way with Siemens products.

If the customer system is built in deviation from this blueprint, it is imperative to carry out a risk assessment to determine how this deviation might impact the system's security**.**

2. Security strategies

Faced with a growing number of attacks – malware, unauthorized access, denial of service, manipulation of data, etc. – securing automation and IT systems must be given the highest priority in every plant and project. Additionally, with digitalization as a major industry trend, the number of networked systems and thus the number of potential vulnerabilities will continue to grow.

Plant operators, system integrators, and original equipment manufacturers must give high priority to protect the automation and control systems against manipulation and malware. This is required to ensure both availability and quality, as well as to meet national and international standards and requirements.

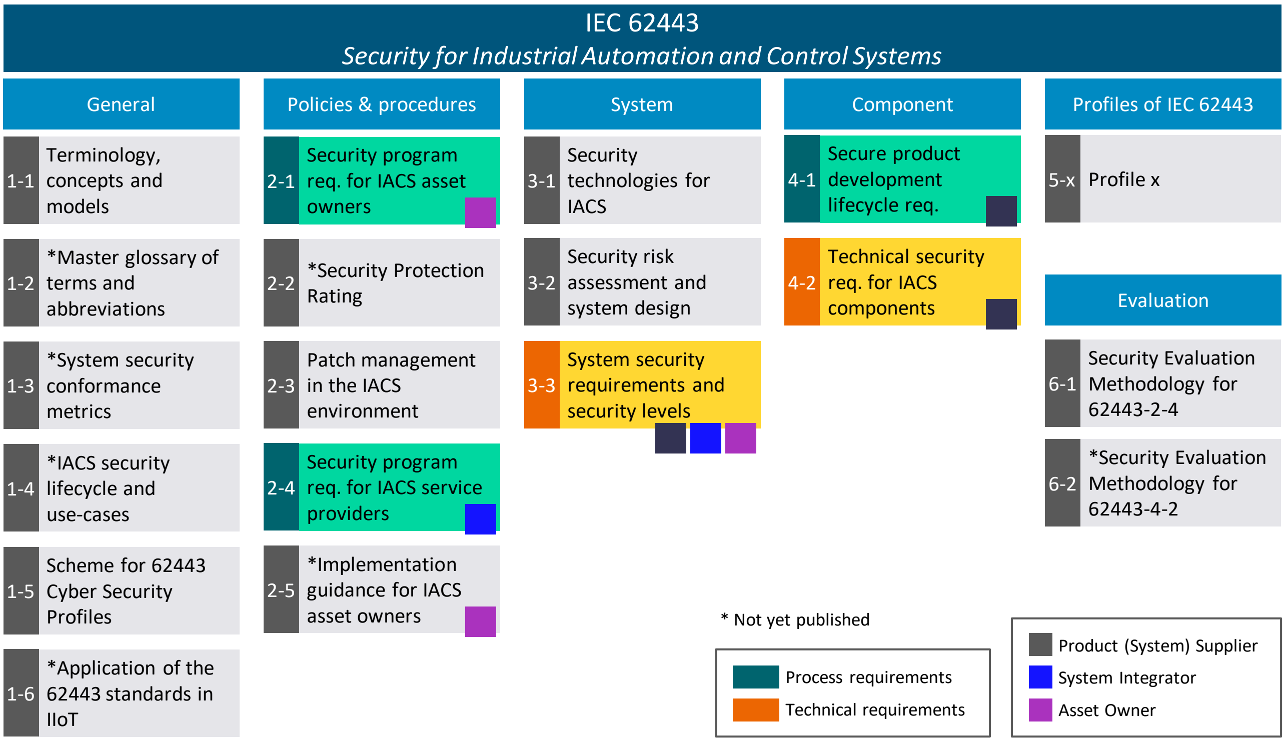
Due to the ever-growing variety of attacks and the complexity in the process industry, it is often not easy to identify risks and threats, and to adapt the right IT and OT security strategy. Holding consistent, regular, and well secured backups, and implementing a comprehensive cybersecurity strategy including isolating critical systems, using appropriate software, having the latest security patches installed and having staff and suppliers well trained in security should be a given.

2.1. IEC 62443 overview

IEC 62443 comprises a set of international standards aimed at enhancing the cybersecurity of industrial automation and control systems (IACS). The standards cover diverse facets of cybersecurity for industrial automation systems, including network security, system integration, security management, and risk assessment.

IEC 62443 is purposefully designed to offer a consistent and comprehensive methodology for safeguarding industrial automation systems. The series of standards provides explicit guidelines, requirements, and best practices to assist companies in effectively implementing cybersecurity measures within their industrial automation systems.

An overview of the different parts of the standard is shown in the figure below.



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 IACS	4-1 Secure product development lifecycle req.	5-x Profile x
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	**Evaluation**
1-3 *System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels		6-1 Security Evaluation Methodology for 62443-2-4
1-4 *IACS security lifecycle and use-cases	2-4 Security program req. for IACS service providers			6-2 *Security Evaluation Methodology for 62443-4-2
1-5 Scheme for 62443 Cyber Security Profiles	2-5 *Implementation guidance for IACS asset owners			
1-6 *Application of the 62443 standards in IIoT				

* Not yet published

Process requirements
Technical requirements

Product (System) Supplier
System Integrator
Asset Owner

Figure 2-1: Overview of IEC 62443.

System lifecycle

Security guidelines underscore the importance of considering industrial security as a lifecycle concern. To ensure the development of more secure systems, plant owners must consider all phases of the solution lifecycle – from system development to eventual replacement. The IEC 62443 standard recognizes five crucial phases in this lifecycle: product or system development, specification, integration and commissioning, operations and maintenance, and decommissioning. Additionally, it provides clear accountability, and a primary objective associated with each of these phases.

Roles and stakeholders

Security topics must be coordinated and communicated between different roles and stakeholders (refer to 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 – IEC 62443 part 4-1 and IEC 62443 part 4-2.
- 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 – IEC 62443 part 3-3. System integrators need security information from the product supplier, such as manuals and guidelines to configure the components securely.
- Plant owners and service providers address secure operation and maintenance, such as dealing with user management and handling of credentials, or implementing regular security patches – IEC 62443 part 2-1, IEC 62443 part 2-3 and IEC 62443 part 2-4.

These roles need to coordinate and work together to achieve adequate security over the whole lifecycle of a system. Lack of coordination, insufficient information sharing, or differing interpretations of security topics impedes the joint efforts of the various stakeholders.

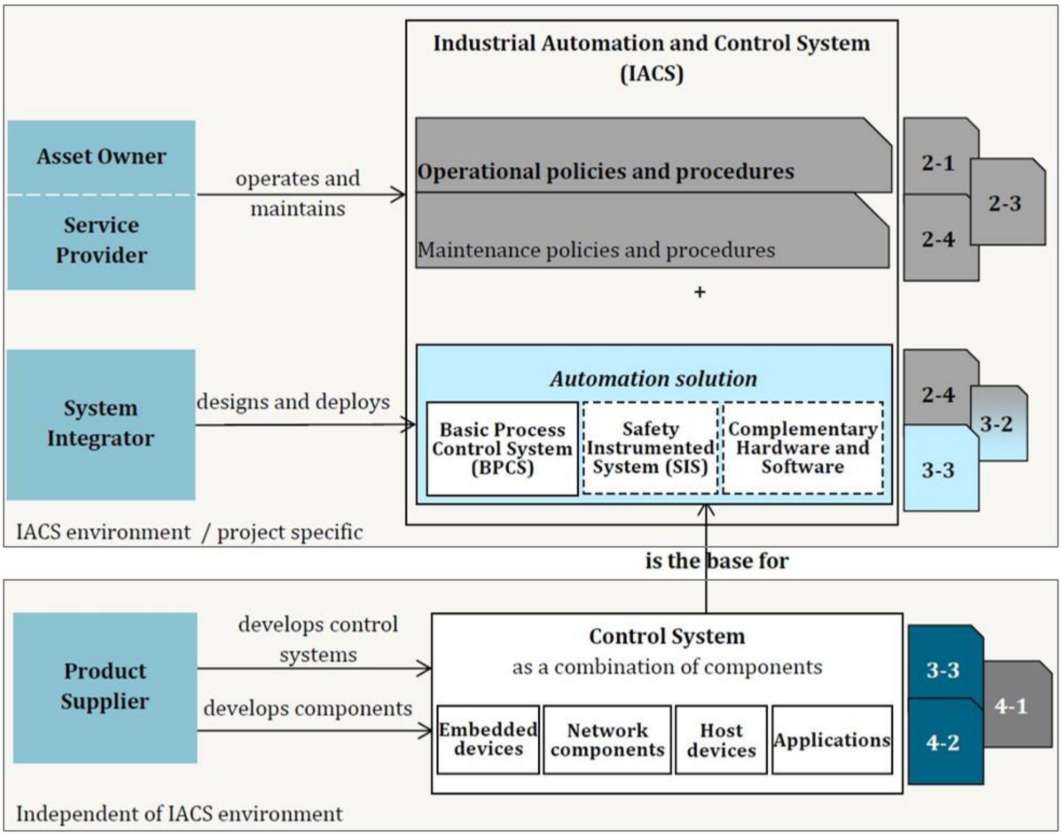

Industrial Automation and Control System (IACS)
Asset Owner
Service Provider
operates and maintains
Operational policies and procedures
Maintenance policies and procedures
+
2-1
2-3
2-4
System Integrator
designs and deploys
Automation solution
Basic Process Control System (BPCS)
Safety Instrumented System (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

Figure 2-2: Roles according to IEC 62443.

2.2. Defense-in-Depth concept

Ensuring comprehensive protection against cyberattacks for industrial facilities requires a simultaneous approach across all levels, spanning from operational to bay levels and from access control to copy protection. IEC 62443 advocates the Defense-in-Depth concept as a comprehensive protection strategy. This approach for Operational Technology (OT) incorporates multiple layers of protection to safeguard a network or system against potential attacks, recognizing that no single security tool or measure is adequate for full system protection.

The Defense-in-Depth concept operates on the principle that deploying various layers of security is essential to compel attackers to overcome multiple barriers before gaining access or compromising a system. The identified security layers within this concept include plant security, network security, and system integrity.

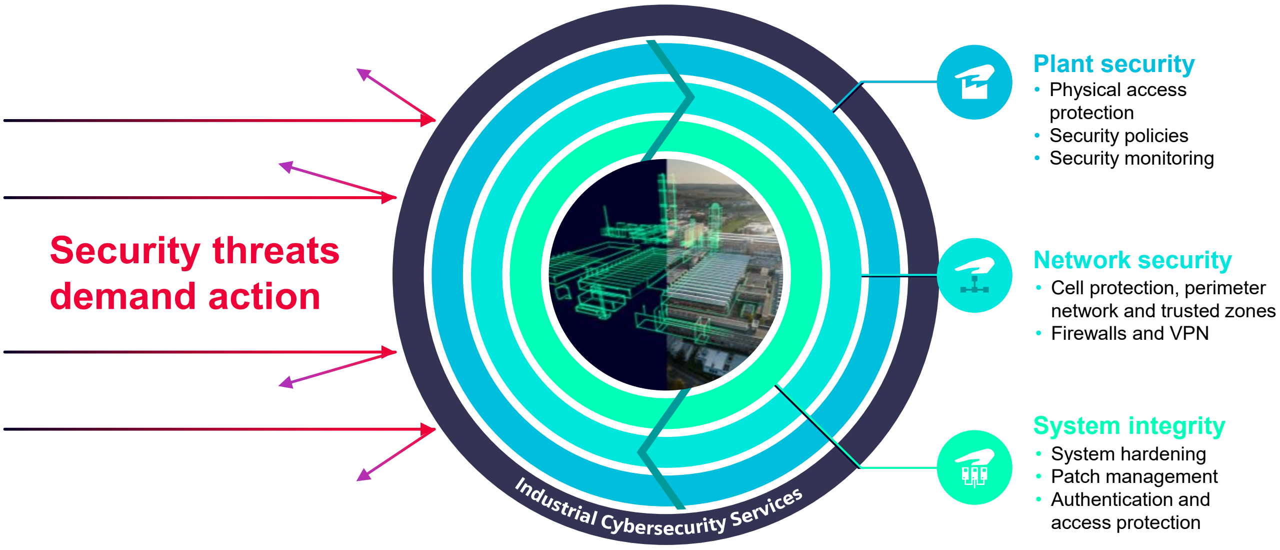

Security threats demand action
Industrial Cybersecurity Services
Plant security
• Physical access protection
• Security policies
• Security monitoring
Network security
• Cell protection, perimeter network and trusted zones
• Firewalls and VPN
System integrity
• System hardening
• Patch management
• Authentication and access protection

Figure 2-3: Defense-in-Depth concept.

By implementing multiple layers of protection, a company or organization can ensure that even if an attack is successful, the attacker does not immediately gain full access to the system or network. A Defense-in-Depth approach for automation control systems requires multiple levels of security and action, meaning that plant owners and solution providers must address varied and very different security issues. From system integrity and network security to plant security and organizational measures.

2.2.1. Plant security

Physical security measures

Control of physical access to buildings, individual rooms, cabinets, devices, equipment, cables, and wires. Physical security measures should include designated security cells and responsible individuals.

It is important to implement physical protection at remote single station systems. For example, the external pump station or the stormwater overflow tank, as indicated in the blueprint, are dedicated security cells.

Organizational security measures

Security guidelines, security concepts, security policies, security checks, risk analyses, assessments and audits, awareness measures and trainings.

2.2.2. Network security

Division into security cells

Secure network architectures imply subdividing the control network into distinct task levels. Perimeter zone techniques are crucial for achieving this. These techniques involve deploying systems within the perimeter network (DMZ) that are shielded by one or more firewalls (front-end firewall, back-end firewall, or a three-homed firewall) from other networks, such as the Internet or the office network.

This segregation allows access to data within the perimeter network without simultaneously granting access to the internal network, such as the automation network, that needs to be protected. Consequently, the risks of access violations can be significantly reduced.

Securing access points to the security cells

Each security cell should feature a single access point, typically facilitated by a firewall, to authenticate users, devices, and applications, implement direction-based access control, assign access authorizations, and detect intrusion attempts.

This single access point serves as the primary gateway to the network of a security cell and acts as the initial control point for managing access rights at the network level.

Securing communication between two security cells over an unsecure network

Certificate-based, authenticated and secure communication should always be employed when the perimeter zone technique is used and there is communication across access points. Tunnel protocols such as PPTP (Point-To-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), and IPSec (IP Security) are suitable options for this purpose.

Additionally, communication can be secured using protocols such as RDP (Remote Desktop Protocol) or HTTPS, which rely on server-based certificates. In such scenarios, communication takes place across the firewall using TLS (Transport Layer Security) or SSL (Secure Sockets Layer) technology. Vertical integration, from the plant to higher level systems, can also be protected with secure communication protocols such as OPC UA.

2.2.3. System integrity

System hardening

Adjustments to a system to make it more resistant against attacks.

User management and role-based operator authorization

Task-based operation and access authorizations (role-based access control).

Patch management

Systematic procedures for installing updates on plant systems.

Malware detection and prevention

Use of suitable and correctly configured virus scanners and whitelisting software.

2.3. Solution blueprint

Considering the large number of requirements involved, it's understandable that project teams may feel overwhelmed by the task of ensuring adequate Defense-in-Depth security concepts for systems designed and deployed in an engineering project. Section 2.2 highlights numerous technical solutions, tools, and best practices to take into consideration, but project teams often lack the time and expertise needed to select suitable solutions for each security aspect. Consequently, it is common for teams to focus extensively on certain topics while inadvertently neglecting others.

To facilitate the security engineering process, Siemens has developed a series of blueprints for automation and control systems. These security blueprints provide guidance in the form of references to specific resources and ensure that engineering projects generate all necessary security documents prescribed by IEC 62443-2-4. This approach aligns with both the IEC 62443-2-4 and IEC 62443-3-3 standards.

Using WinCC Unified as the SCADA system, this blueprint has been designed to meet the requirements of a specific, yet typical, small wastewater/water treatment plant.

3. Blueprint – Wastewater Treatment Plant

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

The WWTP covered in this document processes between 200 and 2,000 m³ per day. Most parts of the facility are located close to each other, with a maximum distance of 1000 meters. Decentralized buildings, such as the external pump station and the stormwater overflow tank, are connected using Remote Terminal Units (RTUs).

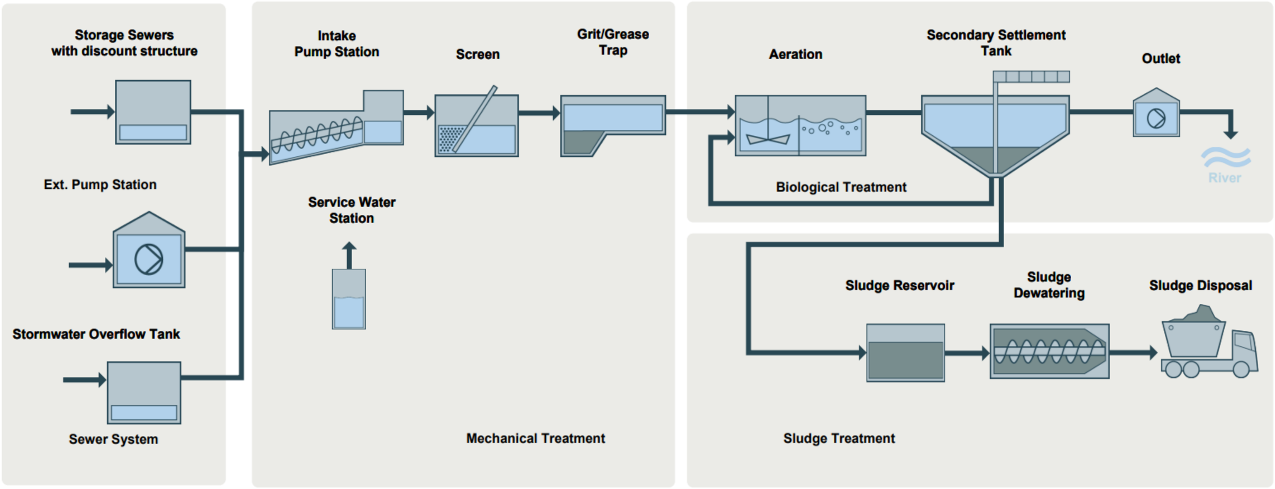


Figure 3-1: Wastewater Treatment Plant.

The blueprint's architecture can also be used as reference for a Water Treatment Plant (WTP), with the corresponding processes depicted in the table below.

Table 3-1: Processes in Wastewater and Water Treatment Plants.

Wastewater Treatment Plant	Water Treatment Plant
Sewer system	-
Mechanical treatment	Raw water feed
Biological treatment	Filtration, Wash-pure water
Sludge treatment	Sludge treatment, Neutralization

3.1. Process description

A small Wastewater Treatment Plant collects sewage from approximately 1,000 to 10,000 households and processes it to ensure that the treated water can be reused.

The wastewater treatment is performed in four main steps:

1. Sewer System
2. Mechanical treatment
3. Biological treatment
4. Sludge treatment

3.1.1. Sewer system

The sewer system is the intake station of the Wastewater Treatment Plant and feeds the plant through different 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 feeds the intake pump station of the Wastewater Treatment Plant.

The stormwater overflow tank is connected to a sewage channel via an inlet overflow wall. In case of heavy rain impact, the water/sewage mixture flows over the overflow wall into the storm water tank, 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.

3.1.2. Mechanical treatment

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

The intake pump station is used for lifting the sewage coming from the sewer system to the mechanical treatment area of the 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 fed 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 fed by a channel to the sand and grease trap.

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) settles on the tank’s floor and undissolved grease and oil, swimming on the water surface is moved by a grease blade into a grease hod.

3.1.3. Biological treatment

The biological wastewater treatment process is used to remove any contaminants that are 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 reduces the N-load of the sewage.
- Nitrification tank : In the nitrification tank the organic load of the sewage is reduced by the use of micro-organisms. Therefore dissolved oxygen 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 denser than water, settles at the button of the tank. A continuously rotating scraper moves the excess sludge to a receiving tank. From the receiving tank, return sludge pumps pump sludge back to the aeration tank. Excess sludge is transferred to the sludge treatment.

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

3.1.4. Sludge treatment

The last process consists of managing and disposing of the sludge. Sludge is mostly water with amounts of solid material removed from liquid sewage.

For dewatering, the sludge must be conditioned due to the strong adhesion of the water on the solid matters. A flocculation agent station doses a flocculation agent controlled by the turbidity and the flow rate in the inlet of the decanter.

3.2. System architecture

The WinCC Unified system architecture for the Wastewater Treatment Plant is shown in the image below.

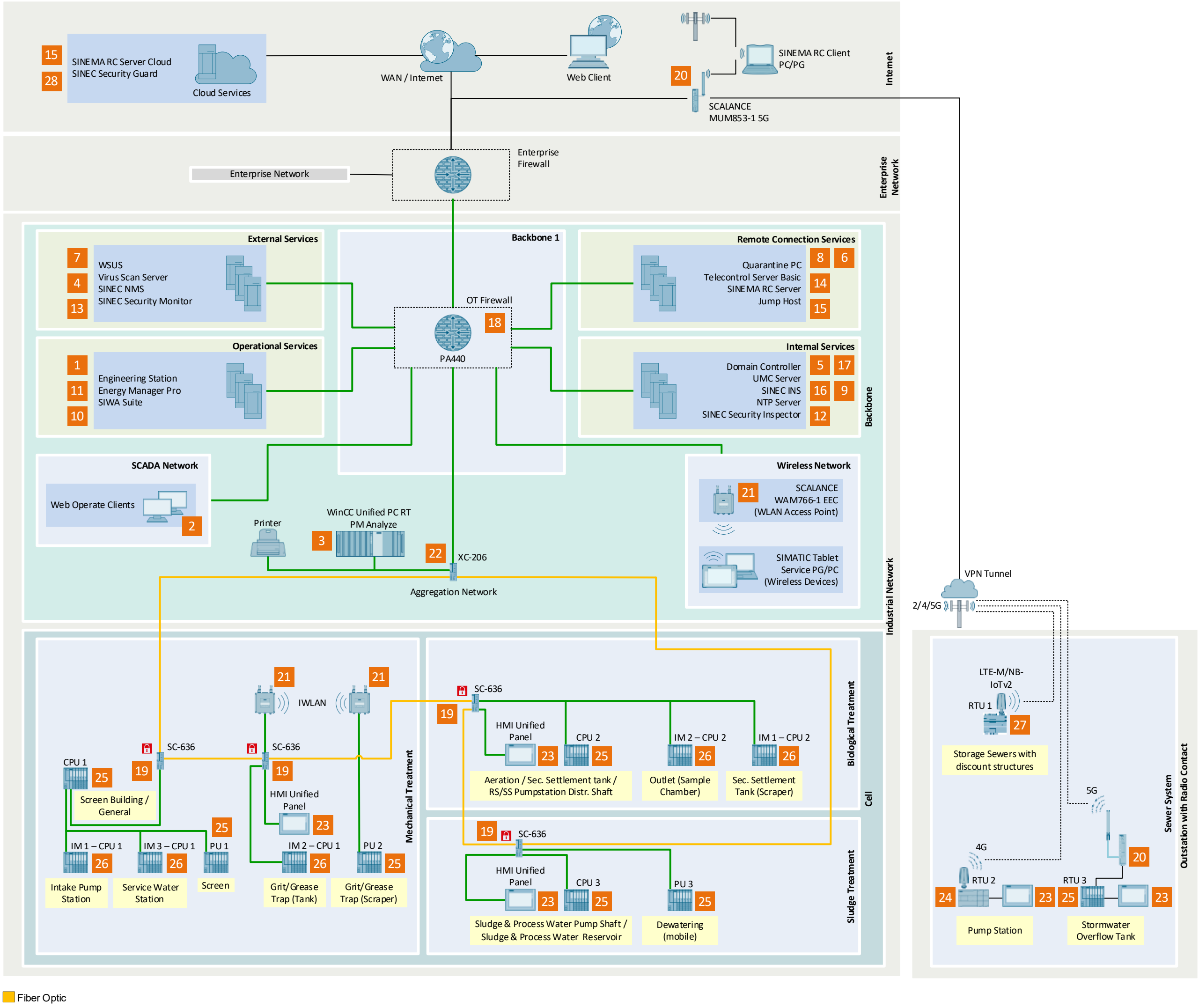


Figure 3-2: WinCC Unified system architecture.

3.2.1. System components of the blueprint's Wastewater Treatment Plant

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: Communication device that; facilitates data flow between devices in a network or restrict the flow of data in a network, i.e. Firewall, but do not directly interact with a control process.
- Embedded device: Special purpose device with embedded software, designed to monitor and control an industrial process, i.e. PLCs, sensors, actuators, remote I/O, etc.

The system components used in the blueprint are listed in the following tables. The System Component Identifier (SCI) corresponds with the number assigned on the system architecture, Figure 3-2.

Hosts/Applications on the OT Network

Table 3-2: Hosts/Applications components used in the blueprint.

SCI	Component	Function
1	Engineering Station	PC station for centralized plant-wide engineering: WinCC Unified devices and PLCs. • Configuration of the hardware. • Configuration of the communications networks. • Configuration of continuous and sequential process sequences. • Operator control and monitoring strategies. • Project compilation and download to automation devices.
2	Web Operate Clients	Used by operators, for control and monitoring. WinCC Unified clients access the data of the WinCC Unified PC RT to visualize and control the process.
3	WinCC Unified PC RT	PC-based visualization system for all types of applications – from single-user solutions directly on the machine to complex SCADA solutions. Can be configured in a redundant setup for high availability and reliability.
	PM ANALYZE	Add-On to prepare and create special reports to comply with water and wastewater regulations, such as DWA.
4	SINEC NMS	Network Management System for monitoring and managing industrial networks.
5	Domain Controller	Provides Active Directory Service and Time information.
6	Jump Host	Provides access to the plant via terminal or remote communication.
7	Infrastructure PC – WSUS, Virus Scan Server	Used for Windows Updates and antivirus applications.
8	Quarantine PC	Used to analyze, test, and contain potentially harmful files or software.
9	SINEC Security Inspector	Tool for asset management and to automate security testing. Scans and tests network components/systems for vulnerabilities and regularly checks the security status of the entire OT network.
10	SIWA Suite Server	Software for water and wastewater industries. Includes SIWA Optim, LeakControl, Sewer Wastewater control, and infrastructure simulation.
11	Energy Manager Pro	Energy data management system. Used to create the basis for economical energy operation management to increase energy efficiency and thus reduce energy costs.
12	SINEC INS	Infrastructure Network Services. Tool for central network services that are frequently required, especially in OT networks, such as RADIUS and syslog.
13	SINEC Security Monitor	Tool for anomaly detection. It monitors network traffic and assets for abnormal device behavior and network communication anomalies.
14	TeleControl Server Basic	For industrial remote communication and TeleControl applications. It facilitates the connection and management of up to 5000 SIMATIC RTUs to a control center using mobile wireless standards, such as GSM/GPRS, and Ethernet/Internet connections.
15	SINEMA RC Server	Provides secure remote access from the Internet to underlying networks for maintenance, control and diagnostics purposes.
16	UMC Server	For managing users and user groups across software and devices. It can be connected to the Active Directory hosted in the domain controller.

SCI	Component	Function
17	NTP Server	Ensures accurate and synchronized timekeeping across all networked devices and systems.

Hosts/Applications on the Internet and Enterprise Network

Table 3-3: Hosts/Applications on the Internet and Enterprise Network.

SCI	Component	Function
15	SINEMA RC Server Cloud	Cloud-based alternative to the on-premises SINEMA RC Server hosted in the Remote Connection Services Network.
28	SINEC Security Guard	Cloud-based vulnerability management solution to gain insight of vulnerabilities in automation assets.

Network components

Table 3-4: Network components used in the blueprint.

SCI	Component	Function
18	OT Firewall	Protects the OT processes from external zones, such as the Enterprise Network and the Internet, enabling access through certificate-based, encrypted and signed communication.
19	SCALANCE SC-636	Industrial-grade firewall to secure the automation cells. If PROFINET communication is required between automation cells, managed switches such as the SCALANCE XC-206 2SPF must be used instead.
20	SCALANCE MUM853-1 5G	Wireless routers for high-performance and secure connection of Ethernet-based subnets via mobile networks – 5G, 4G (LTE) and 3G (UMTS) – or in private 5G networks.
21	SCALANCE WAM766-1 ECC	IWLAN - Access Point for wireless communication based on IEEE 802.11ax.
22	SCALANCE XC-206 – 2 SPF	Managed layer 2 IE switch operating as the ring manager in the Aggregation Network.
-	SCALANCE XC-200 Series	Family of managed industrial switches deployed in process cells for the Sewer System, Mechanical, Biological, and Sludge Treatment areas. • XC-208 : Intake Pump Station, Stormwater overflow tank, External pump station, Screen, Grit/Grease Trap, Secondary settlement tank, Outlet, Dewatering. • XC-216 : Screen Building/General, Sludge & Process water reservoir. • XC-224 : Aeration.

Embedded devices

Table 3-5: Embedded devices used in the blueprint.

SCI	Component	Function
23	MTP1000 Unified Comfort	HMI Panels installed in the cells for process control and monitoring.
24	S7-1200 PLC	S7-1200 controller deployed at the External Pump Station: • CPU 1214C It is equipped with additional hardware: • CP 1243-7 LTE UE: Communication processor for connection of SIMATIC S7-1200 to LTE networks in European frequency range.
25	ET 200SP CPU	ET 200SP Distributed Controller family, employed throughout the blueprint's cells: • CPU 1510SP-1 PN • CPU 1514SP-2 PN It is equipped with additional hardware: • CP 1542SP-1 : Communication processor for connection of SIMATIC ET 200SP to Industrial Ethernet. • CP 1542SP-1 IRC : Communication processor for connection of SIMATIC ET 200SP to TeleControl Server Basic with IEC 60870-5-104 or DNP3. • CM DP : Communication module for connection of SIMATIC ET 200SP over PROFIBUS DP.
26	IM 155-6	IM 155-6PN BA distributed I/O. It can be deployed alongside additional hardware to connect to PROFIBUS networks. • IE/PB LINK PN IO: Gateway between Industrial Ethernet and PROFIBUS.
27	RTU 3051C	Compact, low-power Remote Terminal Unit, powered by battery or solar energy. Installed in the Storage Sewers to monitor water levels in the sewer and the overflow curb.

3.3. Zones and intended operational environment

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

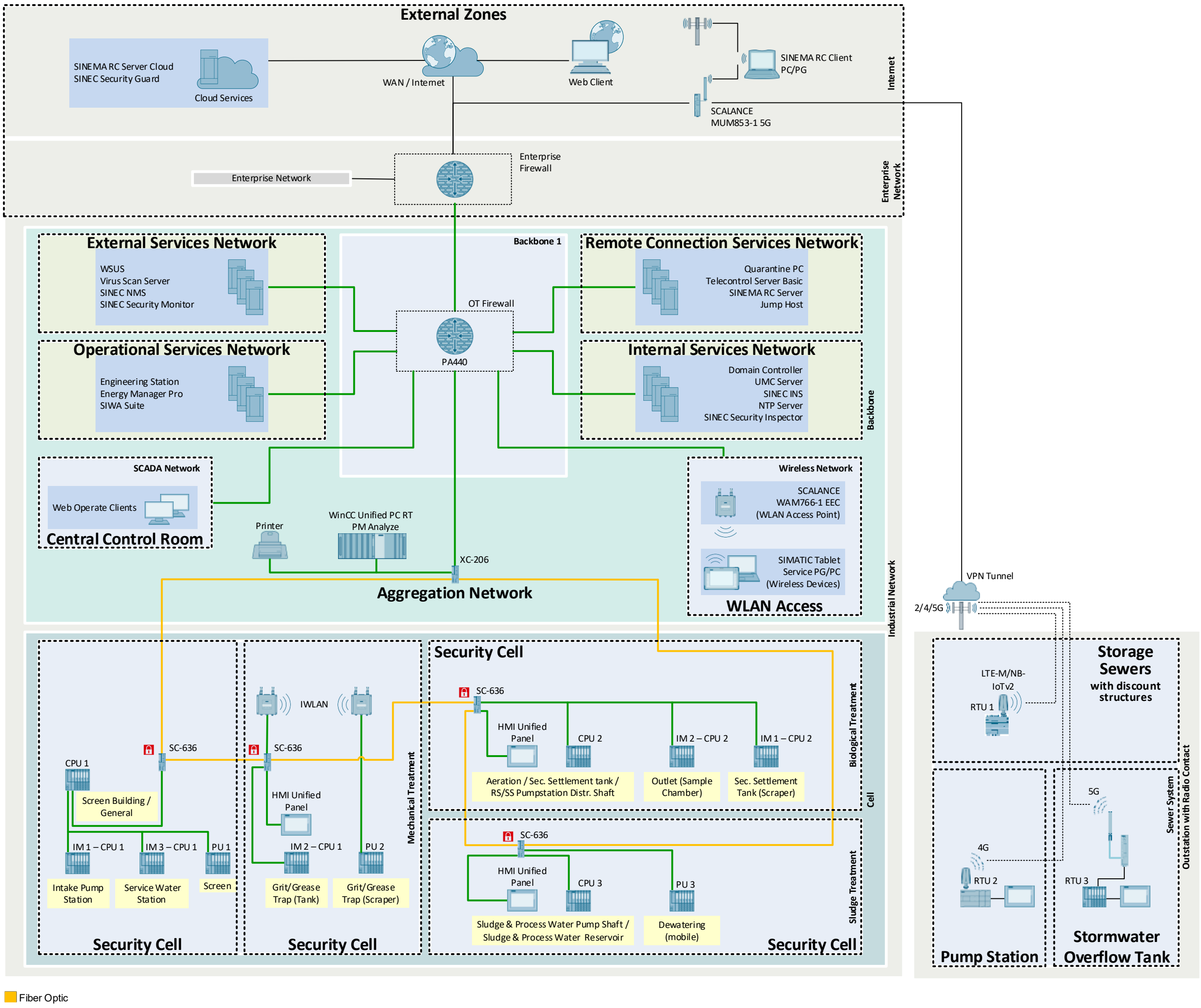


Figure 3-3: Zones of the blueprint's Wastewater Treatment Plant.

3.3.1. Rooms and cabinets

Central Control Room

The central control room contains the operator Workstations (Web Operate Clients) to supervise, control and acquire data from the wastewater treatment plant operations. Access to the central control room is restricted to authorized personnel only.

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 (Keyboard, Video, and Mouse) that serves as a local console for servers that do not have KVM screens located in the central control room. Access to the server room is restricted to authorized personnel only.

Engineering Room

The engineering room houses the TIA Portal Engineering Station, which is used to manage and configure the WinCC Unified and SIMATIC automation devices. Access to the engineering room is restricted to authorized personnel only.

Field PGs can also be used to manage and commission automation devices through the Wireless Access Zone connected to the OT Firewall. Refer to Section 3.3.2 – WLAN Access.

Controller Cabinets

Controller cabinets contain the ET 200SP Distributed Controllers located at various physical locations inside the central plant area. These cabinets are interconnected through the Aggregation Network.

3.3.2. Networks

Operational Services Network

The Operational Services Network contains all systems necessary to run, monitor or administer the production process.

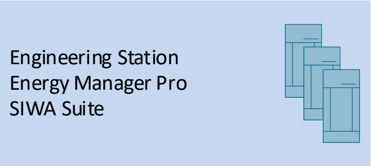


Figure 3-4: Blueprint's Operational Services Network.

Internal Services Network

The Internal Services Network contains all secondary systems which are required in the IACS network. These systems provide important services like the Active Directory, NTP server etc. The systems in this perimeter network do not need a direct connection to non-OT/external networks.

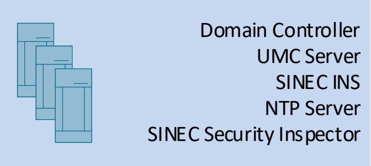


Figure 3-5: Blueprint's Internal Services Network.

External Services Network

The External Services Network is comparable to the Internal Services network. It supports all secondary systems which require a connection to non-OT/external networks:

- Windows Update Server (WSUS) – Retrieves the latest Windows updates.
- Virus Scan Server – Downloads the most recent virus patterns.
- SINEC NMS – Enables web server access from the Enterprise Network to NMS Control. If SINEC NMS shall not be accessible from overlying networks, NMS Control shall be placed in the Internal Services Network.
- SINEC Security Monitor – Retrives updates for the SINEC Security Monitor Intelligence Database.

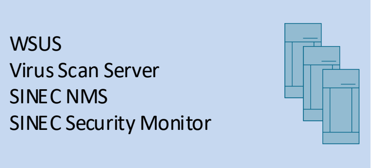


Figure 3-6: Blueprint's External Services Network.

Remote Connection Services Network

The Remote Connection Services is the network with the highest criticality of potential intrusion, as it contains the remote connection server, the jump hosts for each vendor and the quarantine station. To facilitate the connection and management of the remote stations, the TeleControl Server Basic is deployed in this network.

Quarantine PC
Telecontrol Server Basic
SINEMA RC Server
Jump Host

Figure 3-7: Blueprint’s Remote Connection Services Network.

WLAN Access

The Wireless Access zone is connected to the OT Firewall and provides restricted access to devices in the blueprint’s Wastewater Treatment Plant – 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 SIMATIC Tablets or Service Field PG/PCs. Connection to the Wireless Access Points must be encrypted, and require wireless clients to have knowledge of the specific wireless ‘key’ or to be authenticated via 802.1x protocol (RADIUS – network access restriction).

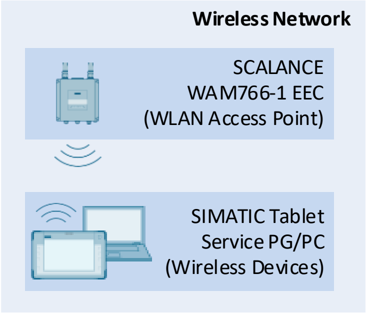


Figure 3-8: Blueprint's Wireless Network.

Aggregation Network

The Aggregation Network brings all the underlying production machine networks together, interconnecting the security cells with the WinCC Unified PC RT. This layer enables both vertical communication (machine to datacenter) and horizontal communication (machine to machine). It is configured in a ring topology for redundancy, ensuring high availability.

Each automation cell is separated by an industrial firewall from the overlying Aggregation Network. The automation devices within the cells control the following main process areas.

- Mechanical treatment
- Biological treatment
- Sludge treatment

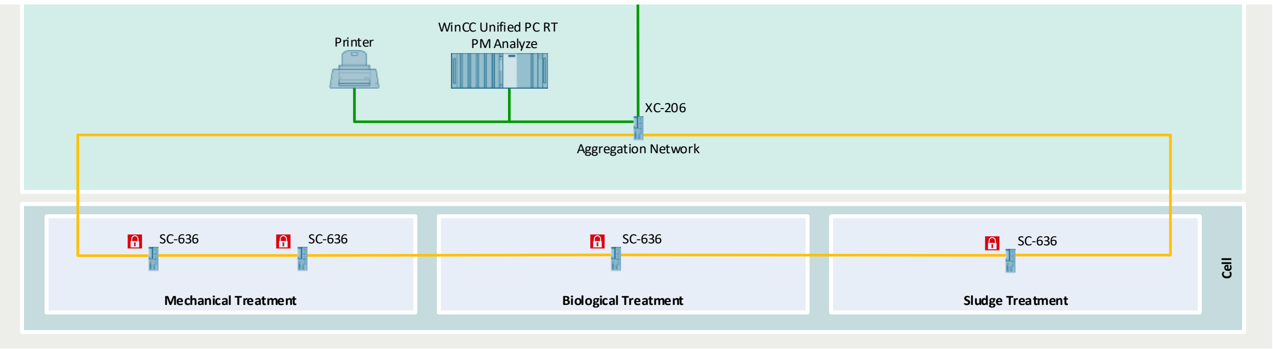


Figure 3-9: Blueprint's Aggregation Network.

External Zones

The blueprint's Wastewater Treatment Plant has two external zones: Enterprise Network and Internet.

These zones conventionally provide update services to the applications running in the External Services Network. The associated network connections for these services are, by convention, initiated – sourced – from the External Services Network 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 External Services Network, such as Windows updates or virus patterns.

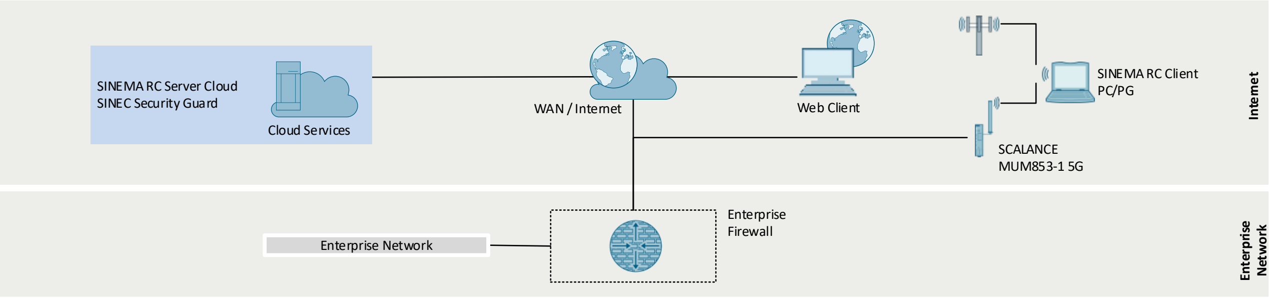


Figure 3-10: External Zones.

3.3.3. Remote stations

The blueprint's Wastewater Treatment Plant has three remote stations: the storage sewers with discount structure, the external pump station and the stormwater overflow tank.

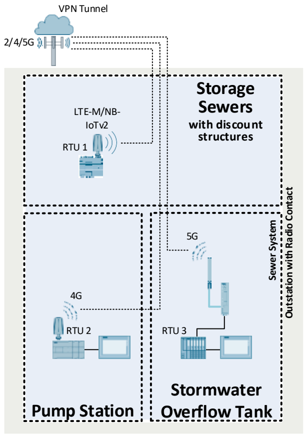


Figure 3-11: Remote stations.

Stormwater overflow tank

The remote station is used to absorb the first surge of wastewater from a rainstorm and limit the load on the water treatment's infeed by sending the excess water directly to the discharge.

To ensure secure and encapsulated communication between the remote station and the central plant area, the router SCALANCE MUM 853-1 and the CP 1542SP-1 IRC are used. For hardening measures and configuration guidelines, see Sections 6.3 and 6.5.

- \31\ – Product catalog: CP 1542SP-1 IRC
- \33\ – Product catalog: SCALANCE MUM853-1

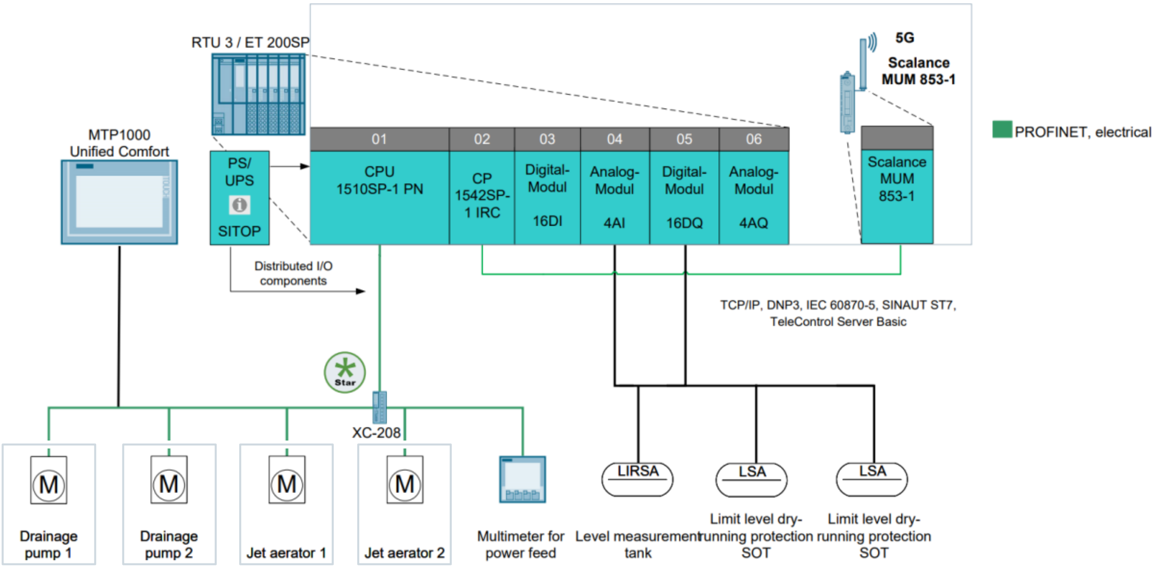


Figure 3-12: Components and network architecture of the stormwater overflow tank.

External pump station

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

To ensure the encapsulation of the communication between the remote station and the central plant area, the CP 1243-7 LTE-EU, with TC-SRC (telecontrol communication via SINEMA Remote Connect) is employed. Refer to Section 6.6 for hardening measures.

- \29\ – Product catalog: CP 1243-7 LTE EU

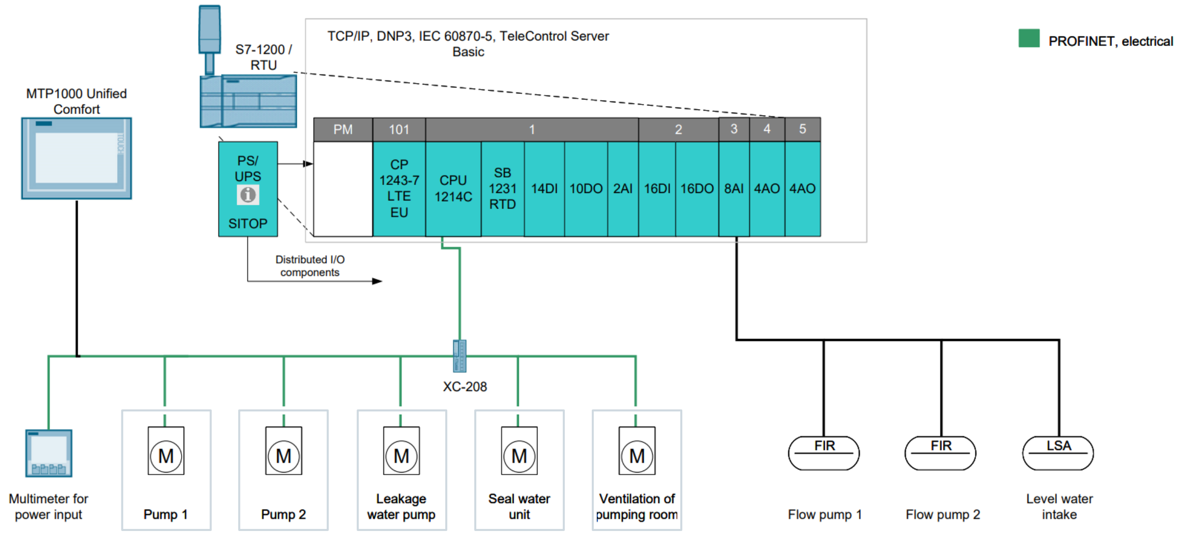


Figure 3-13: Components and network architecture of the external pump station.

Storage sewers with discount structure

The remote station is used to manage and regulate wastewater flow in the disposal area. Wastewater is collected, buffered, and temporarily stored within the sewer system, where a throttling mechanism – discount structure – controls the discharge rate to the treatment plant.

To ensure secure and encapsulated communication between the remote station and the central plant area, the SIMATIC RTU 3051C is used. For hardening measures and configuration guidelines, see Section 6.7.

- \27\ – Product catalog: SIMATIC RTU 3051C

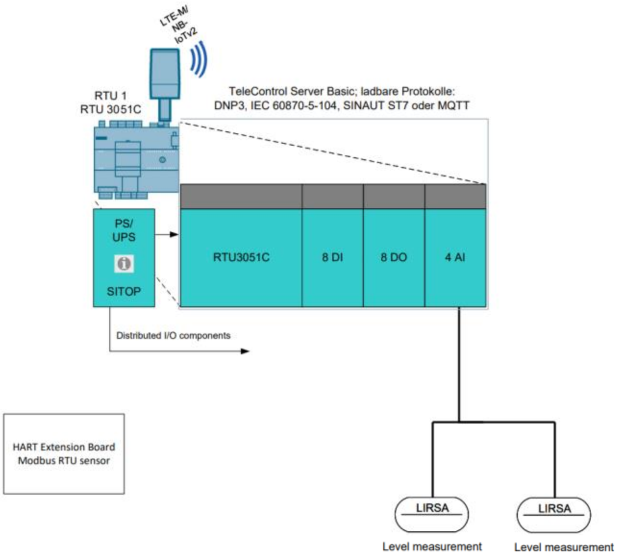


Figure 3-14: Components and network architecture of the storage sewers with discount structure.

3.4. Data exchange between zones

Data traffic and connections between the servers and applications in the respective zones are shown as a generic overview in Figure 3-15.

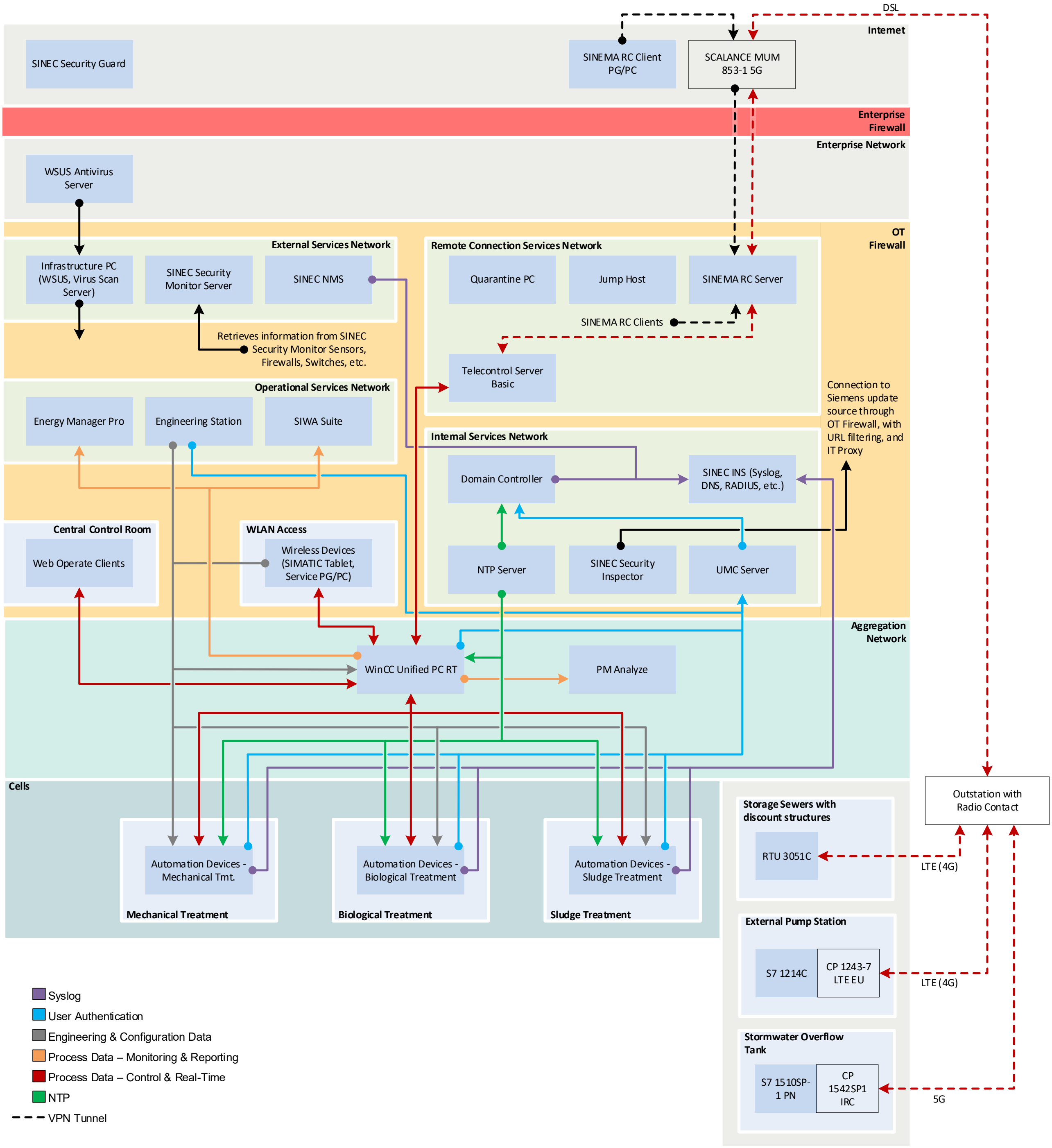

DSL
Internet
SINEC Security Guard
SINEMA RC Client PG/PC
SCALANCE MUM 853-1 5G
Enterprise Firewall
Enterprise Network
WSUS Antivirus Server
OT Firewall
External Services Network
Infrastructure PC (WSUS, Virus Scan Server)
SINEC Security Monitor Server
SINEC NMS
Retrieves information from SINEC Security Monitor Sensors, Firewalls, Switches, etc.
Remote Connection Services Network
Quarantine PC
Jump Host
SINEMA RC Server
SINEMA RC Clients
Telecontrol Server Basic
Operational Services Network
Energy Manager Pro
Engineering Station
SIWA Suite
Connection to Siemens update source through OT Firewall, with URL filtering, and IT Proxy
Internal Services Network
Domain Controller
SINEC INS (Syslog, DNS, RADIUS, etc.)
Central Control Room
Web Operate Clients
WLAN Access
Wireless Devices (SIMATIC Tablet, Service PG/PC)
NTP Server
SINEC Security Inspector
UMC Server
Aggregation Network
WinCC Unified PC RT
PM Analyze
Cells
Automation Devices - Mechanical Tmt.
Mechanical Treatment
Automation Devices - Biological Treatment
Biological Treatment
Automation Devices - Sludge Treatment
Sludge Treatment
Storage Sewers with discount structures
RTU 3051C
Outstation with Radio Contact
LTE (4G)
External Pump Station
S7 1214C
CP 1243-7 LTE EU
LTE (4G)
Stormwater Overflow Tank
S7 1510SP-1 PN
CP 1542SP1 IRC
5G
🟪 Syslog
🟦 User Authentication
⬜ Engineering & Configuration Data
🟧 Process Data – Monitoring & Reporting
🟥 Process Data – Control & Real-Time
🟩 NTP
- - - - VPN Tunnel

Figure 3-15: Data exchange in the blueprint’s Wastewater Treatment Plant.

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) must 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 presented in this section.

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

Table 4-1: Protection goals.

Protection goals	Description of the protection goals	Associated main components/assets
Confidentiality	Ensuring that sensitive information remains protected from unauthorized access or disclosure. • User passwords. • Customer asset information. • Process data, i.e. measurements of the effectiveness of the cleaning processes. • Project engineering data, i.e. WinCC Unified scripts, PLC user program, etc.	• Domain Controller, UMC Server. • Engineering Station. • SCADA – WinCC Unified PC RT. • PLCs and Unified Comfort Panels. • Firewalls and switches. • SINEC NMS, SINEC INS.
Integrity	Guaranteeing the accuracy, consistency, and trustworthiness of data and processes, preventing unauthorized alterations, corruption, or tampering. • Historian data. • Security logs. • Measurement data, i.e. correct chemical dosing. • Project configuration and engineering data.	• Engineering Station. • SCADA – WinCC Unified PC RT. • PLCs and Unified Comfort Panels (Audit Trail System). • Firewalls and switches. • SINEC NMS, SINEC INS (Syslog Server). • PM ANALYZE.
Availability	Ensuring uninterrupted access to critical systems, data, and resources, minimizing downtime and disruptions in manufacturing operations.	• SCADA – WinCC Unified PC RT and Web Operate Clients. • PLCs and Unified Comfort Panels. • Firewalls and switches.

Protection goals for zones

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

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

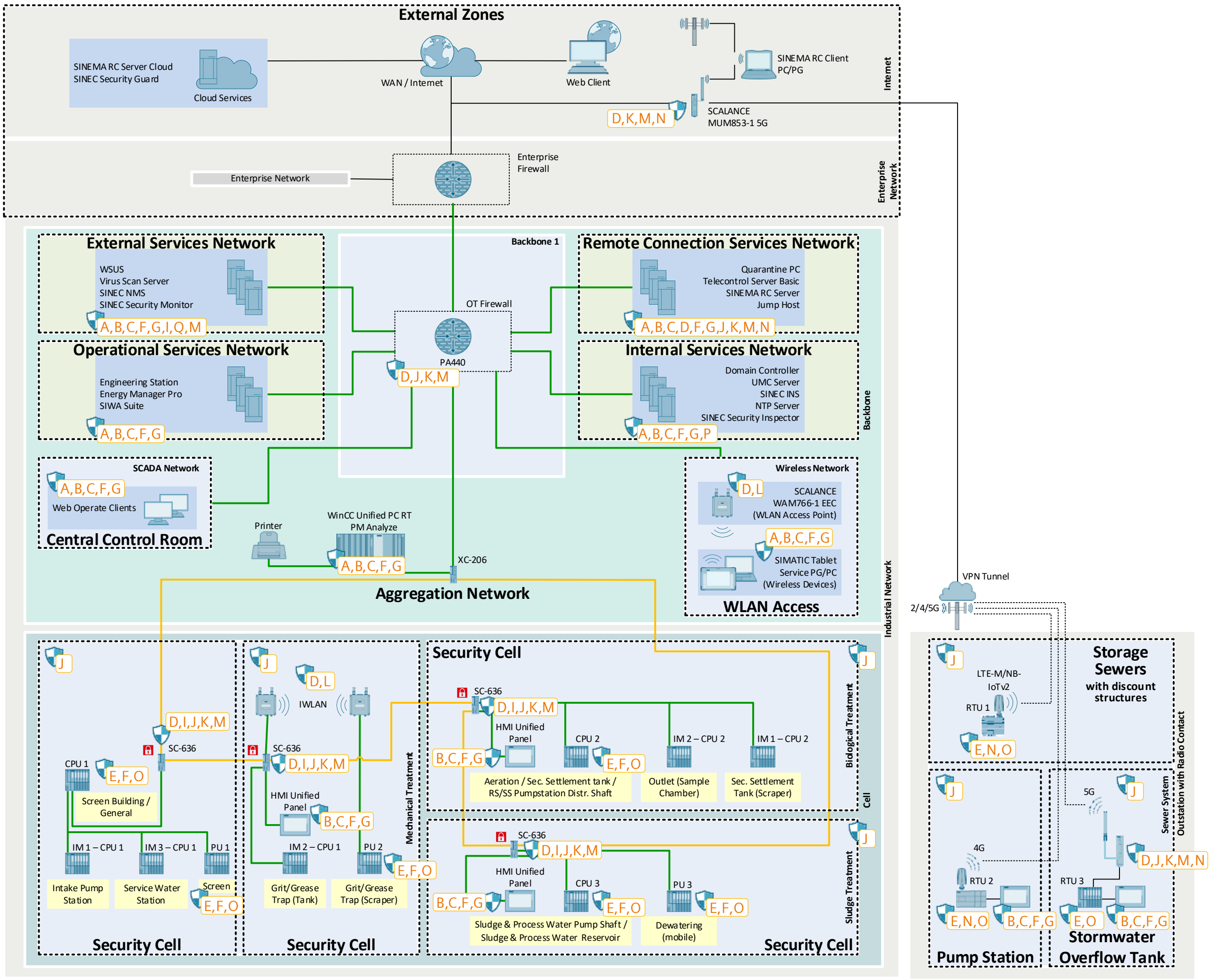


Figure 4-1: Protection goals for zones.

Threat and Risk Analysis

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.

The generic Threat and Risk Analysis conducted in this blueprint – Sections 4.1 through 4.5 – provides guidance on potential threats and risks relevant to wastewater treatment plants. However, a dedicated TRA must be carried out for each individual facility to ensure that site-specific conditions, configurations, and operational contexts are considered.

4.1. Physical access

Perimeter security

Table 4-2: Threat, risks and countermeasures regarding perimeter security.

Threat and risk	Countermeasures
Access to the facility to sabotage operations/processes.	Fencing and barriers, surveillance cameras and lighting, security personnel.
Physical disruption/manipulation of remote stations.	Fencing, surveillance cameras and lighting.
Damage/Manipulation to critical infrastructure, such as backup power supply systems.	Tamper evident seals to detect unauthorized access attempts.

Secured devices, systems and buildings

Table 4-3: Threat, risks and countermeasures regarding secured parts and buildings.

Threat and risk	Countermeasures
Access to central site/buildings.	Access control, 2-factor authentication.
Physical access to perform data theft.	Monitoring 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.

Exposed devices, systems, buildings and remote stations (valves, reservoirs, pumps, metering stations, etc.)

Table 4-4: Threat, risks and countermeasures regarding exposed devices, systems, buildings and remote stations.

Threat and risk	Countermeasures
Easy access to less secured systems and networks.	System and communication monitoring in SCADA.
Destroy/Disable systems in remote stations.	Redundant external systems, i.e. wells, pumps, etc.
Modify/Tamper the data sent and received by these stations.	Secure communication, access control, minimize the amount of information shared to the minimum required.

Network and Windows PCs

Table 4-5: Threat, risks and countermeasures regarding physical access to networks and Windows PCs.

Threat and risk	Countermeasures
Access to the OT network.	Monitoring of network components, 802.1x, Industrial Anomaly Detection.
Unpatched vulnerabilities in Windows PCs.	Updates and/or application whitelisting.

4.2. Power supply system

Table 4-6: Threat, risks and countermeasures regarding the power supply systems.

Threat and risk	Countermeasures
Loss of power supply from the public grid.	Real-time monitoring, backup system.
Malfunction of internal UPS.	Monitoring and maintenance of backup systems.

4.3. WinCC Unified PC RT and panels

For the WinCC Unified devices, two separate risk analyses are conducted – for the engineering and commissioning phases, and for the operational phase.

Threats and risks during the engineering and commissioning phases

Table 4-7: Threat, risks and countermeasures regarding the engineering and commissioning phases of WinCC Unified devices.

Threat and risk	Countermeasures
Unauthorized access to the TIA Portal project.	Protect the TIA Portal project with a project administrator.
Interception and manipulation of project transfer during commissioning.	Activate encrypted transfer on Unified Comfort Panels, enable secure download on the WinCC Unified PC RT.
Theft, loss, or removal of external storage devices, i.e. SD Cards, USB drives, etc. from Unified Comfort Panels containing sensitive data.	Store external storage devices in secure locations, protect panel interfaces from unauthorized access, i.e. lockable control cabinet, regularly export archived data to an access-protected location.
Theft or unauthorized access to sensitive data from WinCC Unified PC runtime.	• File-based archiving – SQLite: Use access-protected storage, regularly export data to a secure location. • Database archiving – Microsoft SQL: Protect databases using Windows Groups: 'Simatic HMI' (read/write) and 'Simatic HMI Viewer' (read only).

Threats and risks during operation

Table 4-8: Threat, risks and countermeasures regarding the operational phase of WinCC Unified devices.

Threat and risk	Countermeasures
Intended or unintended process disruptions or equipment damage by operators.	Restrict operation to authorized personnel. Configure access level protection for devices, screens, and UI elements. Assign users and roles with the minimum required access rights.
Unauthorized access to tags in the controller.	Enable PLC access control, configure access passwords for HMI connections.
Unauthorized access to Windows system functions on the IPC running WinCC Unified PC RT.	Use Windows Kiosk mode.
Theft or manipulation of sensitive data, and malware transfer via SD/USB ports.	Disable unnecessary interfaces, use physical safeguards, i.e. USB port locks, install panels in lockable cabinets, supervise access to the Central Control Room.
Theft or manipulation of sensitive data, and malware transfer via network interfaces.	Disable unused network interfaces, implement physical safeguards.
Interception or manipulation of data transmitted over the network, and impersonation of communication partners.	Use encrypted, certificate-based, communication protocols for server/client communication, runtime collaboration, and OPC UA connections.

4.4. Firewalls

Table 4-9: Threat, risks and countermeasures regarding the network and firewall configuration.

Threat and risk	Countermeasures
Network or devices publicly exposed to the Internet, highest visibility even for script kiddies.	Secure configuration, vulnerability patching.
Network intrusion.	Permanent central monitoring of firewall log data/Anomaly Detection.

4.5. Internal and organizational measures

Table 4-10: Threat, risks and countermeasures regarding internal and organizational measures.

Threat and risk	Countermeasures
Internal personnel with access to infrastructure PCs can tamper with them, either intentionally or unintentionally.	Personnel training, organizational procedures.
Internal personnel with access to operation PCs can tamper with them, either intentionally or unintentionally.	Personnel training, organizational procedures.
Unsecured USB ports.	System hardening, deactivation of USB ports.
Software updates can have an impact on proper OS functionality.	Application whitelisting (can be an option as an alternative to software/OS updates).

5. Security measures

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

The security measures described in the following sections are only valid 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 automation control systems and networks is network security. Networks of automation control systems must be protected from unauthorized access. Moreover, interfaces to other networks, such as the Enterprise Network or the Internet, must be controlled, monitored and limited to only allow necessary communication, using suitable technologies like 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

Network segmentation is key to minimize security threats and maximize system availability. The network shall be separated into different segments to isolate critical systems from non-critical parts. To achieve this, firewalls are the current state-of-the-art technique for network segmentation.

To segment an OT network, the following criteria must be considered.

- Risk and criticality : Systems identified as critical – based on the risk analysis from the planning phase – need to be separated from systems of lower criticality, aiming to increase the availability of those critical systems.
- Automation real-time communication : The communication protocols exchanged between controller and device may have real-time requirements. Therefore, devices belonging to the same automation application must be in the same network segment to provide the required deterministic communication.

Based on these requirements, and as part of implementing the Defense-in-Depth concept, the automation system is segmented into distinct security zones outlined in Section 3.3. These zones are strategically split up by the OT Firewall and the SCALANCE SC-636 firewalls deployed within each security cell, ensuring that system components with similar communication and protection requirements are grouped together within each zone. The boundaries between these zones, known as trust boundaries, require monitoring and controlling of the communication between them, as detailed in Section 5.1.2.

NOTE

In addition to physical separation via firewalls, networks can also be logically segmented through VLANs configured in managed switches. This logical segmentation prevents direct communication between VLANs, requiring all inter-segment traffic to pass through a firewall – which enforces communication restrictions according to the configured firewall rules.

Nevertheless, VLAN-based segmentation alone can only fulfil Security Level 1 as defined in the IEC 62443-3-3, while physical segmentation using firewalls can achieve Security Level 3. This results from:

- Network overloads or Denial-of-Service (DoS) attacks in one VLAN can impact other VLANs of the same physical segment (same physical switch).
- VLANs are easier to bypass – for example, the reset of a switch typically leads to the switch allowing all traffic, whereas a firewall reset leads to the firewall denying all traffic by default.

To reach Security Level 4, complete isolation of critical network segments is required.

The network segmentation realized as part of this blueprint is in line with the recommendations provided by the Secure Reference Architecture.

- \35\ – Secure Reference Architecture, Section 4.1 (Network segmentation)

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 security zones must be closely monitored and controlled. To enforce the necessary communication rules and ensure secure exchanges between different zones, firewalls with VPN functionality are deployed as a key security measure. Within the central plant network, only allowed traffic can traverse zone boundaries, in line with firewall policies that adhere strictly to the 'deny-by-default, allow-by-exception' principle.

To protect the central plant network boundary, the perimeter networks – Demilitarized Zone (DMZ) – provide additional application-level control. Communications from external zones are directed to the DMZ, preventing direct access to internal components such as direct engineering access. Instead, proxies or hosts within the DMZ facilitate necessary interactions, including 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 with the remote stations is secured through SCALANCE S firewall appliances, as well as the enterprise and OT firewalls. Data exchanged between these remote stations and the WinCC Unified PC RT in the Aggregation Network is routed through the OT Firewall, ensuring a single, controlled connection point between the OT network and the external networks. This connection, secured using VPN tunnels, is established via the SINEMA RC Server and the TeleControl Server Basic hosted in the DMZ, as detailed in Section 5.2.4.

The Industrial WLAN (IWLAN) access area enables secure wireless connectivity via SCALANCE W wireless access points. Wireless access is safeguarded by the wireless security features and secure configuration of the access points, coupled with the additional restriction to grant access solely to designated wireless clients. Moreover, all wireless access is subject to the limitations imposed by the boundary protection devices between the different plant areas.

Besides the network-based firewalls, PC-based host firewalls are also employed to provide an additional layer of protection.

These boundary protection measures are further enhanced by adaptable security logging and monitoring mechanisms, elaborated 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 play a crucial role in protecting network zones at their perimeters, it's equally important to implement appropriate measures for restricting local network access. This helps mitigate the risk of local attacks on the networks within individual secure plant zones, considering their respective criticality and exposure levels. In the context of the blueprint's Wastewater Treatment Plant, the following measures are recommended for secure configuration and operation.

- Mobile devices : All accesses with mobile devices, such as service laptops, should undergo thorough review to assess their necessity and potential associated risks. If needed, only securely managed, and configured devices with clearly defined access paths and restrictions configured within the plant's access protection mechanisms should be utilized.
- Wireless access : Any users, software processes, or devices accessing the network via wireless communication must be identified and authenticated. A widely accepted security practice involves utilizing state-of-the-art security profiles with robust authentication and encryption protocols based on the current 802.11 wireless communication standard (Wi-Fi standard). This ensures the authentication, authorization, monitoring, and enforcement of usage restrictions for wireless connections.
- Hardening : To further minimize the risk of unauthorized access to any part of the central plant network, common measures such as hardening of deployed network devices and the disabling of all unused Ethernet ports and other physical interfaces, such as USB ports, must be implemented. Refer to Section 6 for recommended hardening practices and secure configuration settings.

The hardening measures realized as part of this blueprint are in line with the recommendations provided by the 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices'.

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 4.1.1 (Protect SD and USB ports) and Section 4.1.2 (Disable network interfaces)

5.1.4. Administration of network devices

Secure administration and configuration of network devices is of key importance given their central role in ensuring the availability of the plant's internal and external communication, as well as the implementation and enforcement of network segmentation.

All administrative access to network devices, including routers, switches, firewalls, and wireless network access points, used within the blueprint, is performed through communication protocols that use state-of-the-art cryptographic protection. This protection is achieved through either Web-based communication via HTTPS or SSH, ensuring mutual authentication and strong encryption of all data exchanged. Deprecated and vulnerable methods such as HTTP or Telnet – if supported at all – are disabled by default to mitigate security risks.

Human user access to these devices is managed through role-based access control, implementing the principle of least privilege to restrict administrative access to authorized personnel only. User management and access control for administrative purposes are integrated with Microsoft Active Directory via SINEC NMS – Siemens' Network Management System.

With SINEC NMS, network administrators can centrally deploy firmware updates across all managed SCALANCE network devices, as detailed in Section 6.9.4.

5.1.5. Protection measures against Denial-of-Service

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

To safeguard water and wastewater solutions from Denial-of-Service attacks, two critical aspects must be addressed.

Firstly, DoS attacks may aim to disrupt the overall availability of the central plant network or individual devices by overloading them with unnecessary network traffic. In response, the automation solution must maintain operational functionality even in a degraded state during such events.

Secondly, components safeguarding secure zones or being located within secure zones with critical roles in process control must exhibit proven robustness against malformed network packages and network-level attacks. They should either ignore such packets or switch to a predefined state to mitigate potential damage.

In the blueprint, key measures to ensure protection against DoS attacks across different networks include:

- OT Firewall – The deployment of Palo Alto’s Next-Generation Firewall provides general protection against common network level DoS attacks. Hardening measures and configurations for this firewall are outlined in Section 6.2.1.
- SCALANCE network devices, employed in the blueprint, undergo rigorous testing against various DoS or DDoS attacks through predefined test procedures.
- As part of Siemens' comprehensive approach to industrial security, the development process for all automation devices and software adheres to the IEC 62443-4-1 secure development process, incorporating security considerations and regular penetration testing.

For best practices on mitigating DoS attacks on Palo Alto’s Next-Generation Firewall, refer to the official documentation.

- \36\ – Palo Alto – DoS and Zone Protection Best Practices

For a complete list of certified Siemens devices, consult the following documentation.

- \4\ – Certification and standards ‘TÜV Süd certification based on IEC 62443’
- \5\ – ‘IEC 62443-4-1 Secure product development lifecycle' for Digital Industries (DI)

5.2. Identity and access management

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

- Operating system accounts.
- Engineering accounts, i.e. TIA Engineering Station.
- Accounts for administrative access to network devices, i.e. SCALANCE devices, SINEC NMS, SINEC INS, etc.
- Operator accounts for applications with user interfaces, i.e. Web Operate Clients, HMI Unified Comfort Panels, web interfaces, etc.
- User accounts for automation devices, i.e. ET 200SP Distributed Controller: online connection through TIA Portal, web server, 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	SR 1.1 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 in the DMZ and Aggregation Networks. See Section 7.1.

NOTICE

Exceptions to unique user accounts in OT environments

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 individuals, 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, user authentication and account management are 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

Users and groups to monitor and configure network devices can be centrally managed through UMC – which can be integrated with the Active Directory – or configured locally in 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 configured in 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

To ensure secure operation, operator device screens – WinCC Unified Panels and PC runtime – must be protected against unauthorized access that could result in process disruptions or equipment damage. WinCC Unified devices implement user-based access control, where each user is uniquely identified and assigned specific roles.

When an unauthorized individual attempts to interact with a protected WinCC Unified device or screen object, a login dialog is displayed requesting valid user credentials. User configuration in WinCC Unified is managed within the TIA Portal project. User management can be implemented either globally, via UMC, or locally, using TIA's 'User Management & Access Control'.

In the same way, access to SIMATIC controllers is user-based, ensuring that users attempting to connect are uniquely identified and authenticated. User management can be handled globally, via UMC (for S7-1500 and ET 200SP distributed controllers running FW 4.0 onwards), or locally, using TIA's 'User Management & Access Control'. Exceptions that require group-based authentication can be accomplished through the controller's access level-based control, that relies on passwords assigned to different access levels.

To gain further information regarding access control to automation devices, refer to Section 6.10. The information provided in the blueprint regarding user authentication is derived from the device manuals listed below.

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 2.6 (Creating user administration), Section 3.1 (Operation of configured plant screen) and Section 3.4.1 (Enable access protection for the Control Panel)
- \6\ – 'SIMATIC S7-1500 S7-1500R/H redundant system', Section 11.3 (Local user management) and Section 11.4 (Central user management)
- \7\ – 'Connecting WinCC Unified to User Management Component (UMC)', Section 2.4 (Configuring the WinCC Unified PC station) and Section 2.5 (Configuring the Unified Comfort Panel)

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 (i.e. username, host name) and passwords for the Windows domain accounts through the Windows AD domain controller. This includes mechanisms for password recovery and reset mechanisms.

Through centralized management and integration with the domain controller, 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 automation devices, user management can be handled globally, via UMC (for S7-1500 and ET 200SP distributed 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 TIA Portal project. Policies can be set to enforce password strength based on minimum length and variety of character types.

User management in this blueprint aligns with the recommendations provided by

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 2.6 (Creating user administration)
- \18\ – Central User Management with 'User Management Component (UMC)'
- \54\ – 'Configuring users and roles (RT Unified)'

5.2.3. Account management and configuration of access rights and privileges

Account management handling (users & groups) is done via the Active Directory. The least privilege approach is applied to grant users the minimum level of access or privileges required to fulfill their 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, systems or devices must be removed.

For centralized user authentication across Siemens' software, network and automation devices, UMC is employed. However, UMC does not support user authorization – that is, the assignment and management of user access rights and privileges. As a result, access rights must be configured locally within each software application (SINEC NMS, TIA Portal), SCALANCE routers and switches, WinCC Unified systems and automation devices. System administrators define these access rights directly in the software applications or within TIA Portal projects, running on the Engineering Station, from where they are downloaded to the automation devices during commissioning.

For the WinCC Unified PC RT and Web Operate Clients, additional security can be achieved with Windows Kiosk mode. This mode restricts users to a single application – such as Microsoft Edge for accessing the SCADA system – thereby preventing access to the Windows environment, system settings and other applications.

Access rights and privileges in this blueprint aligns with the recommendations provided by

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 3.5 (SIMATIC WinCC Unified PC RT – Windows Kiosk mode)

5.2.4. Control of access via untrusted networks (remote access)

As the blueprint's solution is protected by firewalls – enterprise and OT Firewall – and a DMZ, no direct access is possible for users connecting to the plant from external networks that are considered untrusted by default. Users connecting remotely can only access machines within the DMZ and the Aggregation Network that are specifically configured and secured to authorize further access at the application level.

Remote Access

In the Wastewater Treatment Plant blueprint, secure remote access is achieved through SINEMA Remote Connect, with the SINEMA RC Server installed in the Remote Connection Services Network. When combined with a jump host solution, this setup provides a highly secure remote access configuration, enabling restricted access for authorized users into the plant.

In the remote access scenario, users first log in to the SINEMA RC server to establish a secure VPN connection, allowing them to traverse unsecured networks like the Internet. This VPN connection is then used to establish an RDP connection to the jump host located in the DMZ. From there, authorized users can establish a connection through the OT Firewall to other systems such as the Engineering Station. It's worth noting that the Engineering Station undergoes scanning for malware and unauthorized file transmissions before granting access.

TeleControl Basic

In the context of telecontrol communication with the remote terminal units, SINEMA Remote Connect and TeleControl Server Basic work jointly to establish secure VPN connections between the central plant and the remote stations.

Once the VPN tunnels are established, TeleControl Server Basic – located within the plant's Remote Connection Services Network – can securely exchange process values, alarms and control commands with the remote stations using telecontrol protocols such as IEC 60870-5-104 or DNP3.

The SINEMA RC Server centrally manages these connections and enforces access control policies, ensuring that only authorized devices can communicate with each other.

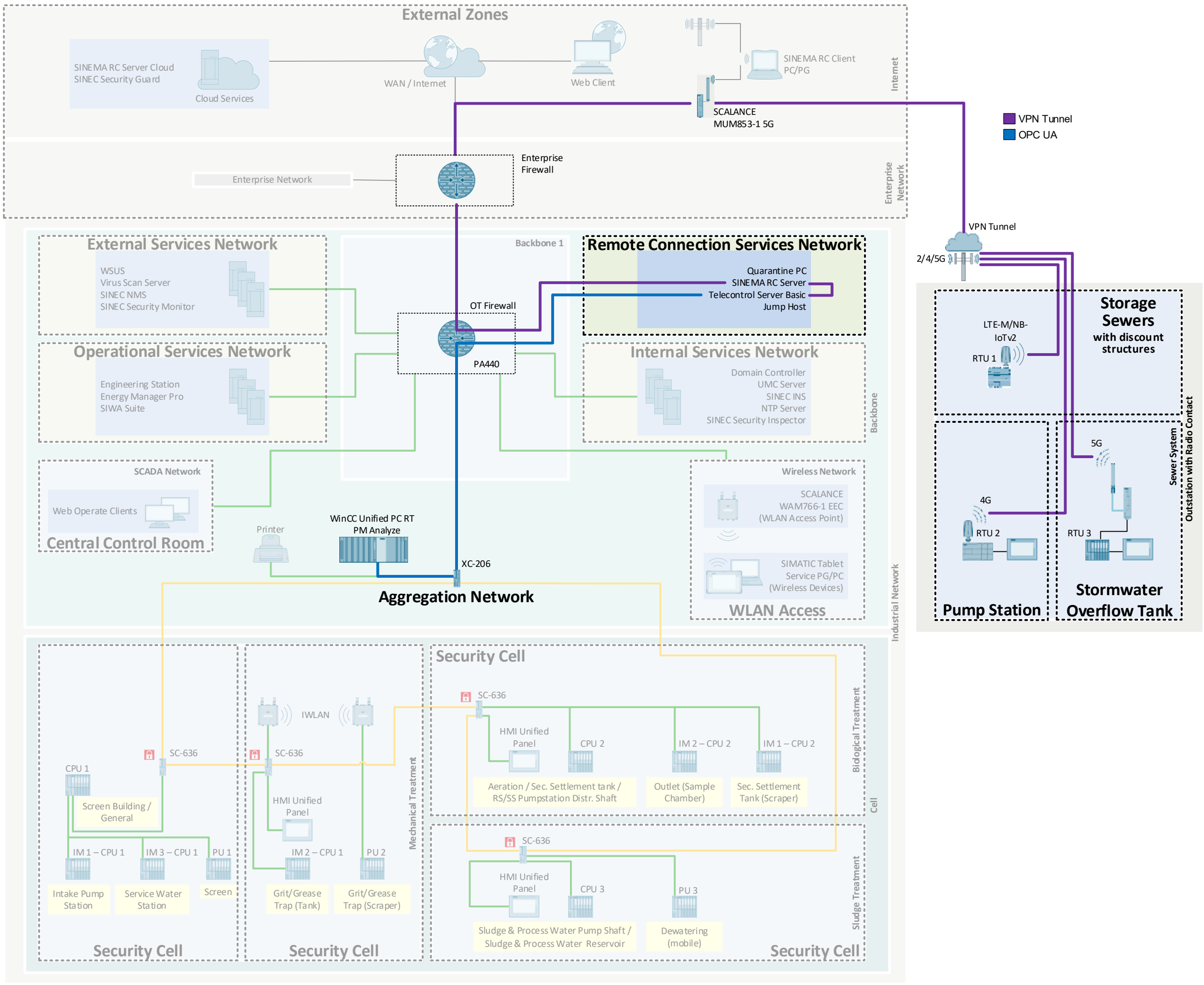


Figure 5-1: Remote connection between WinCC Unified PC RT and the remote stations.

5.3. Attack surface reduction

In an automation system, a considerable part of its vulnerabilities to cyber threats arises from its interfaces.

5.3.1. Least functionality

To reduce the attack surface, the principle of least functionality is implemented. This involves two security measures, referred to as 'hardening'.

- Disabling all unnecessary interfaces.
- Securing necessary interfaces with appropriate configurations.

Typical measures applied in the blueprint to protect such interfaces include:

- Disabling physical communication interfaces like USB ports, Ethernet ports, diagnostics interfaces, and wireless communication.
- Safeguarding system-level functionality, particularly with external component interfaces, by eliminating unnecessary functions, removing unused software applications, and disabling communication ports, protocols, and/or services.

These measures are implemented across various levels of components, including applications, operating systems, and low-level interfaces in the BIOS.

Recommended hardening measures to reduce the attack surface of the above-described areas, are listed in Section 6.9. Additionally, physical protection measures such as locks or access-protected rooms, detailed as part of the intended operational environment of the zones in Section 3.3, are of utmost importance.

Finally, it is essential to ensure the removal of all temporarily enabled functions post-commissioning, such as debug and test interfaces, and to minimize the attack surface during plant operation by limiting accounts to only those strictly necessary.

For further information regarding the principle of least functionality in WinCC Unified systems, refer to the security guide.

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 4.1.1 (Protect SD and USB ports) and Section 4.1.2 (Disable network interfaces)

5.4. Secure channels and encryption

Secure communication ensures the integrity and confidentiality of messages transmitted over networks, as well as providing endpoint authentication.

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 VPN protected channels between the main plant and all remote stations, to achieve independence from the security capabilities of the communication infrastructure, i.e. WWAN or WLAN radio.
- Secure communication within trusted zones for sensitive data transmission, i.e. HTTPS, SSL, OPC UA, secure OUC, etc. Real-time communication requirements must be considered.
- Encryption of the PLC's confidential data, i.e. private keys, through password protection.

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, locking down components, or establishing remote control of a client or server by an attacker. Targeted malware could also manipulate the system's behavior.

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

5.5.1. Software and information integrity

Besides technical support for securing workflows related to software updates and configurations, and additional measures like digitally signed software updates, system protection against malware and unauthorized changes can be implemented using virus scanner software and whitelisting technologies.

Virus scanner software

Virus scanner software detects, blocks and removes malware – if necessary and configured.

For the operational environment of the blueprint, 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 does not interfere with the process. 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.
- 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 or unapproved tools, will be blocked from execution.
- Whitelisting, rule-based : 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 in the External Services Network. Whitelisting software is also installed on the stations and servers of the blueprint. Section 8 describes these protection measures in detail.

It is important to identify new malware exploit vulnerabilities present in the installed software components and services. Therefore, virus scanners and whitelisting solutions must be complemented by maintaining an up-to-date security patch level. The patch management procedures for the blueprint are described in Section 9.

5.5.2. Security functionality verification

It is important to ensure the correct functioning of the implemented security measures. Verification of their intended operation is recommended during the Factory Acceptance Test (FAT) and Site Acceptance Test (SAT), incorporating appropriate security tests. Regular verification, i.e. during scheduled maintenance, is also advised to uphold the integrity of the security infrastructure.

5.5.3. Input validation and output and error message sanitization

The Wastewater Treatment Plant blueprint is founded on the WinCC Unified SCADA solution. WinCC Unified guarantees features such as input validation and controlled output through an overall secure development process. This secure development process is certified in accordance with the IEC 62443 framework for security in industrial control systems, specifically part 4-1, which outlines the Secure Development Lifecycle Requirements.

- \5\ – 'IEC 62443-4-1 Secure product development lifecycle' for Digital Industries (DI)

5.5.4. Support for control system backup and recovery

The objective of backup and recovery procedures is to enable the operator or asset owner to restore the system to a known state following a disruption or failure. Additional information can be found in Section 10.

5.5.5. Time distribution and synchronization

Time synchronization within the blueprint is achieved via an NTP Server hosted in the Internal Services Network. The Domain Controller retrieves time signals from the NTP Server and distributes them across all domain members, including OS clients, OS servers, OPC UA servers, etc. The SCADA – WinCC Unified PC RT – system, WinCC Unified Comfort Panels, and automation devices connected to the Aggregation Network receive the time signal directly from the NTP Server.

Recommended measures and further details about the time distribution and synchronization are 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 previous sections are complemented by security logging and monitoring of security-related actions and events across essential system components. In addition to the logging and monitoring focused on the process, that is thoroughly covered by the capabilities of regular automation control systems, information from security logs and monitored events are important to discover or perform forensics in case of cybersecurity incidents.

Apart from security logging and monitoring, additional industrial anomaly detection capabilities can be added with SINEC Security Monitor. For more details, refer to Section 5.7.3.

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 is performed by the OT Firewall and by the PC-based systems within the DMZ. Hence, all user or system-level access, as well as communication sessions at network (TCP/IP) level, are covered.

5.6.2. Logging of security-related events

PC-based systems maintain security logs for both application level and operating system level events. Security logs can be exported through standardized communication protocols, such as Syslog or SNMP, to central servers. These central servers collect security log information from the system components and provide interfaces that can be integrated with the asset owner's SIEM solutions (Security Information Event Management). Further details on SIEM functionalities are described in Section 5.7.4.

Monitoring of Palo Alto's OT Firewall is done with Panorama Management Software. 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.

For the protected zones in the blueprint, such as buildings and central plant zones, security logging is performed for the WinCC Unified PC RT, WinCC Unified Comfort Panels, SCALANCE network devices and SIMATIC PLCs.

To forward security-relevant events, Syslog clients are configured on PLCs, network devices, and the SINEC NMS network management system. SIMATIC PLCs use a dedicated message memory to record user logins, configuration changes, or operating state changes. SINEC NMS and SCALANCE network devices log system events, network events, Audit Trail events, and system alarm messages. The configurable forwarding to external Syslog servers or SIEM systems allows these devices and software applications to be integrated into existing security monitoring solutions.

SINEC INS, deployed in the Internal Services Network, hosts the Syslog server to centrally collect and store security-related events.

NOTICE

Avoid local access to devices during operation

Physical access to devices – WinCC Unified PCs and Panels, PLCs or SCALANCE network components – should be strictly limited to the initial commissioning phase and avoided during regular operation, including maintenance activities.

Therefore, administrative tasks such as updates or configuration changes shall not be performed directly at the device. Instead, they must be executed via the designated infrastructure to ensure that all changes are systematically tracked and managed through centralized platforms, enhancing accountability, traceability, and minimizing the risk of unauthorized modifications.

To prevent direct physical access, devices must be housed in locked cabinets or secure enclosures. While cabinets may remain open during commissioning for practical reasons, they must be secured once the system enters operation.

- \40\ – 'SIMATIC NET Network management SINEC INS'

- \41\ – ‘SIMATIC NET Industrial Ethernet Security SCALANCE SC-600’, Section 4.4.13 (Syslog client)
- \42\ – ‘SIMATIC NET Industrial Ethernet Switches SCALANCE Layer 2 Switches’, Section 6.4.14 (Syslog client)
- \43\ – Network management SINEC NMS, Section 6.2.18 (Operation parameter profiles (Control) – Syslog settings), Section 6.7.5 (Control administration – Syslog settings), and Annex 7 (Syslog messages)
- \38\ – ‘Sending SIMATIC S7-1200/S7-1500 CPU Security Messages via Syslog to SINEC INS’
- \39\ – ‘SIMATIC S7-1500/ET 200MP, S7-1500R/H, Drive Controller, S7-1500 Software Controller, ET 200SP, ET 200pro Syslog Messages’

5.6.3. Audit trail

To fulfill the requirements regarding change management, all changes shall be centrally executed either via the WinCC Unified Audit Trail System, 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 performed which changes.

- \37\ – ‘WinCC Audit (RT Unified)’
- \43\ – Network management SINEC NMS, Section 5.3 (Audit Trail)

5.7. Additional security measures

The security measures described in Section 5, together with the configuration and hardening measures described in Section 6, 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 the measures Siemens is providing.

5.7.1. Threat Prevention Subscription for Palo Alto's OT Firewall

Palo Alto Next Generation Firewalls, as described in Section 6.2.1, can be enhanced with the Threat Prevention Subscription (TPS) option. TPS is highly recommended if remote access is implemented and must be ordered for each Next Generation Firewall. The TPS includes an Intrusion Prevention and Detection System (IPS/IDS), providing integrated protection against network-borne threats, i.e. exploits, malware, command and control traffic, various hacking tools, etc. through the IPS functionality and stream-based blocking of millions of known malware samples.

5.7.2. Industrial Vulnerability Manager

Software and hardware components embedded in Automation Control Systems are regularly affected by security flaws that need to be mitigated to reduce the risk of cyber-attacks on plants and factories. As part of a global patch management strategy, it is necessary to continuously monitor hardware and software components to identify and address any vulnerabilities. The Industrial Vulnerability Manager offers the following features:

- Accessible via a secured web interface.
- Hosting a list of components embedded in the ICS that shall be monitored over 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.
  - SINEC Security Inspector.
- 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.
  - Common Vulnerability Scoring System (CVSS) 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').

SINEC Security Inspector

SINEC Security Inspector is a security framework designed to automate security testing processes across IT/OT environments. It conducts automated scans, tests, and vulnerability assessments to deliver consistent, reproducible and reliable security test results. Detailed reports are generated to summarize the test results, facilitating Factory Acceptance Tests, Site Acceptance Tests, and compliance checks. SINEC Security Inspector can also be used to support penetration testing and manual testing for security-critical products and environments.

In the blueprint's Wastewater Treatment Plant, SINEC Security Inspector is hosted within the Internal Services Network in the DMZ.

- \45\ – Industrial Ethernet Security SINEC Security Inspector, Section 7 (Asset discovery and vulnerability detection in factories)

SINEC Security Guard

SINEC Security Guard is a cloud-based security platform that enables operators managing Siemens OT assets to centralize risk and security management within a single tool. SINEC Security Guard continuously analyzes vendor security advisories to match known vulnerabilities with assets in the production environment. Operators can evaluate the security risks under consideration, prioritize recommended security measures, and integrate vulnerability management tasks into a task management system.

- \46\ – SINEC Security Guard

5.7.3. Industrial Anomaly Detection

SINEC Security Monitor

SINEC Security Monitor is a modular, non-intrusive, security monitoring software 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 – if required – can be started with low impact. The detected assets are compared with an extensive database of known vulnerabilities to identify affected devices. Furthermore, the software understands what normal communication in the network looks like and can detect anomalies using AI-based analysis.

- \34\ – 'Industrial Ethernet Security SINEC Security Monitor Operating Instructions'

5.7.4. Security Information Event Manager (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 can be used.

A SIEM system continuously collects data from network and security devices, correlates and analyzes this information, and presents it through a centralized interface. Based on this analysis, appropriate security measures can be derived. As a result, safety-relevant incidents can be detected earlier, plant operators can be promptly informed, and countermeasures can be initiated as soon as possible.

5.7.5. Industrial Cybersecurity Services

While many SIMATIC products offer built-in configurations to enhance cybersecurity, these features are rarely found in real-world deployments due to limited in-house expertise.

Siemens addresses this gap with a suite of Industrial Cybersecurity Services designed around SIMATIC automation systems and aligned with international standards such as IEC 62443 and the NIS 2 European Directive. These services are conceived to:

- Provide transparency regarding the current security status and compliance with security standards.
- Ensure state-of-the-art implementation and configuration of security features.
- Long-term support to maintain and improve the security level throughout the entire lifecycle of the system/plant.

Siemens' Industrial Cybersecurity Services portfolio is grouped in three main categories, following the Defense-in-Depth concept.

1. Plant Security Services
    - Security Assessments – Identifying security gaps and defining countermeasures according to IEC 62443 and NIS 2-based evalutaions.
    - Scanning Services – Transparency over assets and vulnerabilities.
    - Industrial Security Consulting – Support with policies, secure network design, implementation and incident analysis.
    - Cybersecurity Trainings – Provision of knowledge to secure the 'weakest link'.

- Remote Industrial Operations Services (RiOPS) – 24/7 remote monitoring and management of IT/OT infrastructures.

2. Network Security Services
   - Industrial Next Generation Firewall – Continuous network protection with Next Generation Firewalls.
   - Industrial DMZ Infrastructure – Secure data exchange between IT and OT.
   - Remote Platform Software as a Service – Secure remote access to industry devices.
3. System Integrity Services
   - Endpoint Protection – Continuous endpoint protection with Antivirus and Application Control.
   - Vulnerability Services – Vulnerability intelligence and vulnerability management.
   - Patch Management – Management of critical updates in Microsoft products.
   - Backup and Restore – Pre-configured IT infrastructre for disaster recovery.

Siemens' Industrial Cybersecurity Services can be ordered through the local Siemens contact person.

- \8\ – 'Siemens Industrial Cybersecurity Services'

6. Hardening and configuration of system components

For the components used in the blueprint's Wastewater Treatment Plant, various hardening measures must be considered according to the Threat and Risk Analysis and the defined protection goals presented in Section 4.

The recommended hardening measures and configurations described in the following sections are only valid for the blueprint's Wastewater Treatment Plant. Any deviations from the blueprint require a new Threat and Risk Analysis. The corresponding hardening measures and configurations must be reviewed and adjusted 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-in-Depth concept recommends physical and organizational security measures which fall under the responsibility of the plant owner.

After evaluating the possible security risks for the blueprint's Wastewater Treatment Plant, the following physical security measures are assumed:

- Unauthorize access to the central plant and buildings is prevented with physical measures. Only authorized personnel have access.
- Unauthorize access to the remote stations is prevented with physical measures. Access to the remote stations is monitored, i.e. using door switches, and only authorized personnel have access.
- All cabinets have a locking system with semi-cylinders.
- All cabinets, both in the main part of Wastewater Treatment Plant and in the remote stations, are installed in lockable control or server rooms. Access to control or server rooms is limited to authorized personnel – maintenance – only.
- The Aggregation Network is installed in one building with high physical protection as shown in Figure 3-3. If the Aggregation Network is not limited to one building, it needs to be physically protected to prevent eavesdropping.

For all components used in the blueprint, the following general hardening measures shall be considered to ensure a secure configuration during plant operation:

- The latest released firmware versions shall be installed. Firmware versions for all Siemens components are available on the Siemens Industry Online Support \1\.
- For all components, the latest released patches shall be installed. The patches for Siemens components are available on the Siemens Industry Online Support \1\. Further information regarding patch management given in Section 9.
- All Operating Systems should have the latest released security patches installed. For more information see Section 9.1.
- The virus scanner installed on the workstation and server must have the latest virus pattern installed.
- For the Endpoint protection software, that is installed on the workstations and servers, the latest updates regarding software updates, patterns, etc. must always be installed. Changing configuration, uninstalling, or deactivating the Endpoint protection software must be password protected. Further information about Endpoint protection software is available at 'Continuous endpoint protection against malware' \9\.
- The standard user and password on all devices must be changed before the first installation. The same password shall not be 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 described in the 'Checklist for setting up SCALANCE devices' \10\ shall be considered and centrally executed by SINEC NMS.

6.2. Firewalls for secure communication between zones

Communication between security zones must be monitored and controlled as described in Section 5.1.2.

The plant network boundary is protected using the OT Firewall, creating a Demilitarized Zone. The hardening measures and configuration of the firewall are described in Section 6.2.1.

Communication between security cells within the Aggregation Network is secured using SCALANCE network security devices. The hardening measures and configuration of these devices are described in Section 6.2.2.

6.2.1. Palo Alto 440 NGFW

OT Firewall

Protects the networks in the DMZ – External Services Network, Remote Connection Services Network, Operational Services Network, Internal Services Network – and the internal networks – WLAN Access Network, SCADA Network, Aggregation Network – from untrusted external networks such as the Enterprise Network and the Internet.

In addition, it allows servers in the DMZ to securely communicate with public servers on the Internet and the remote stations of the wastewater treatment plan. Both outgoing and incoming data is screened utilizing Deep Packet Inspection (DPI).

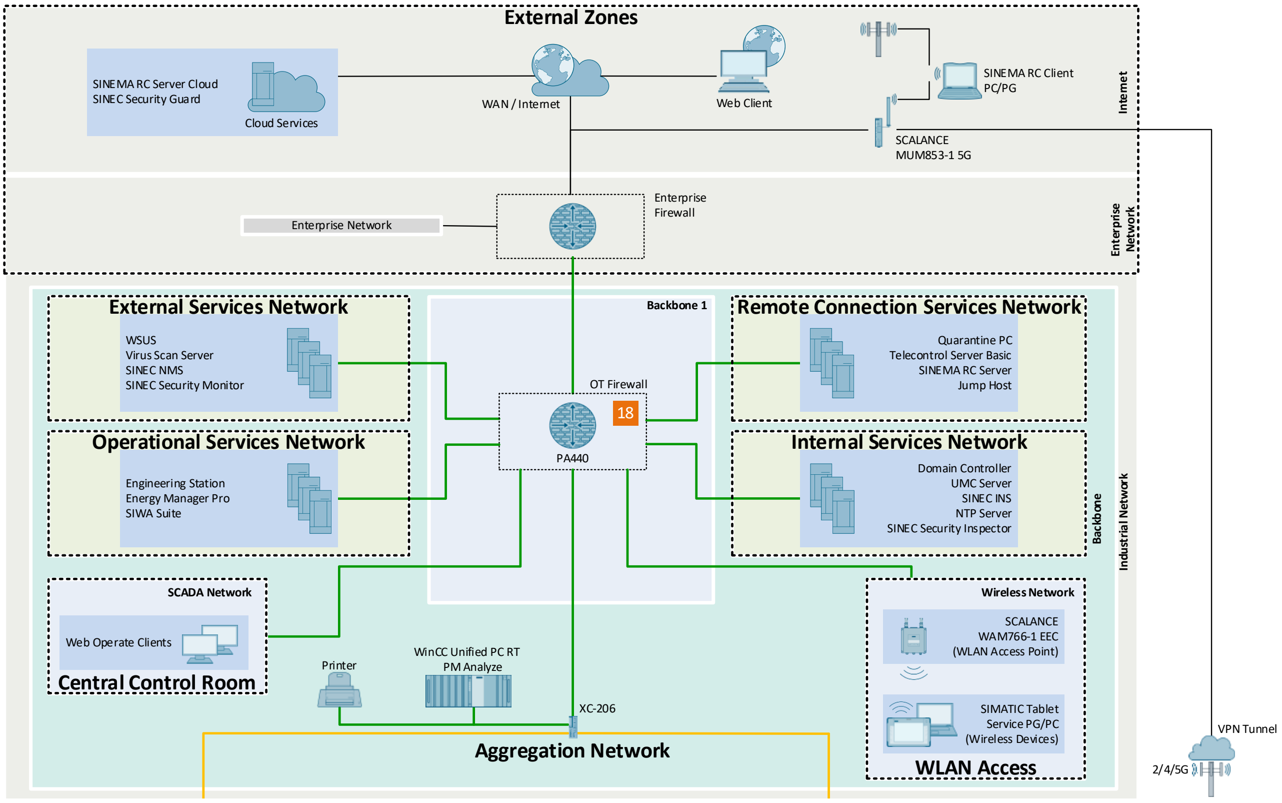


Figure 6-1: OT Firewall.

The recommended hardening measures and the configuration of the OT Firewall are listed below.

Table 6-1: OT Firewall.

SCI	Supplier	Type	MLFB	Function
18	Palo Alto	440 NGFW	9LA1110-6SY12-1AB1	OT Firewall

Table 6-2: Hardening measures for the OT Firewall.

No.	Security topic	Hardening measure
1	Restrict IP addresses	Restrict access to only those IP addresses that are required.
2	Restrict services	Block access over unsecure protocols, HTTP or Telnet. Require SSH and/or HTTPS.
3	Change admin credentials/user management	• Change the default username and password. • Configure an account for each user that needs access and assign only the minimum required access rights. • Employ multi-factor authentication (RADIUS or SAML). • Configure a strict password policy.
4	Dedicated management interface	Use the dedicated management interface in a separate management LAN or VLAN.
5	Security policy rules and profiles	• Scan all traffic destinated to the management interface for threats. • Create a security profile, enable extended packet capture. • Configure inbound inspection and SSL Forward Proxy.
6	Logging	• Set up logging for configuration changes. • Set up logging for unauthorized login attempts.
7	SNMP	• Use SNMP v3. • Set an SNMP string that is not easy to guess. • Only enable SNMP on internal interfaces.
8	Certificates	Replace the default certificate with a certificate signed by the organization's enterprise CA.
9	Updates	Keep the PAN-OS and all software packages up to date.

Further information regarding the secure configuration of Palo Alto's Next-Generation Firewall.

- \11\ – PAN-OS Administrator's Guide
- \12\ – Palo Alto – PAN-OS
- \13\ – Palo Alto – Best Practices for Securing Administrative Access

6.2.2. SCALANCE network security devices

Secure communication between the cells on the Aggregation Network and between the central plant building and the remote stations is implemented using SCALANCE network security devices as shown in Figure 3-2.

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

Table 6-3: SCALANCE security network devices.

SCI	Supplier	Type	MLFB	Function
19	Siemens	SCALANCE SC-636	6GK5636-2GS00-2AC2	Secure communication between security cells and other networks.
20	Siemens	SCALANCE MUM 853-1 5G	6GK5853-2EA00-2DA1	High-performance and secure connectivity over 5G networks.
21	Siemens	SCALANCE WAM766-1 EEC	6GK5766-1GE00-7TX0	Access point for secure wireless communication with mobile devices.

For the SCALANCE devices listed in Table 6-3, the following general hardening measures must be considered:

Table 6-4: Hardening measures for SCALANCE network security devices.

No.	Security topic	Hardening measure	Documentation
1	Secure network	• Set quality of service (QOS) priority is to 'DSCP'. • Deactivate Spanning Tree if not required. • Deactivate Passive listing.	\10\ – Section 3.10. \10\ – Section 3.11.2. \10\ – Section 3.11.3.
2	Identity and access management	• Use central authentication via RADIUS/UMC/AD. • Establish password policy (complexity and change frequency). • Deploy changes centrally and regularly via SINEC NMS.	\10\ – Section 3.6. \14\ – User administration for SCALANCE devices with RADIUS protocol.
3	Reduction of the surface of attack	• Disable unencrypted and non-required protocols. • Disable the PROFINET interface. • Disable unused ports. • Disable all non-required services, like DHCP or DNS.	\10\ – Section 3.3 \10\ – Section 3.7. \10\ – Section 3.9.1. \10\ – Section 3.14.1.
4	Secure channels and encryption	No action required.	
5	System integrity	Use of NTP for time synchronization. If available, use the secure NTP variant.	\10\ – Section 3.2.
6	Logging and monitoring	Activate Syslog client.	Section 5.6.2. Section 5.7.4.

Protocol settings

The following table outlines the settings for the protocols used by the SCALANCE devices in the blueprint.

Table 6-5: Protocol settings.

No.	Protocol	Settings
1	Telnet server	Disabled.
2	SSH server	Disabled. Use SINEC NMS to configure 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

IPSec VPN and firewall configuration

Secure communication with external zones is established using IPsec VPN and the internal firewall. Table 6-6 and Table 6-7 display the IPSec and firewall settings respectively.

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	CA signed certificates.
4	Phase 1	Use default ciphers. Minimum: • Encryption: AES128 GCM 16 • Authentication: SHA256 • Key derivation: DH group 14
5	Phase 2	Use default ciphers and auto firewall rules. Minimum: • Encryption: AES128 GCM 16 • Authentication: SHA256 • Key derivation: DH group 14

Table 6-7: Firewall settings.

No.	Topic	Settings
1	Predefined IPv4	Disable all services for VLANs that are not required.

Further information about the configuration of the SCALANCE security network devices is provided in

- \10\ – 'Checklist for setting up SCALANCE devices'
- \14\ – '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 provide wireless access for SIMATIC Tablets and Service Field PG/PCs to the devices and systems in the DMZ and Aggregation Network. Additionally, wireless links are established between automation devices located within the Mechanical Treatment area, as well as between the Radio Outstation that connects the central plant building with the remote stations.

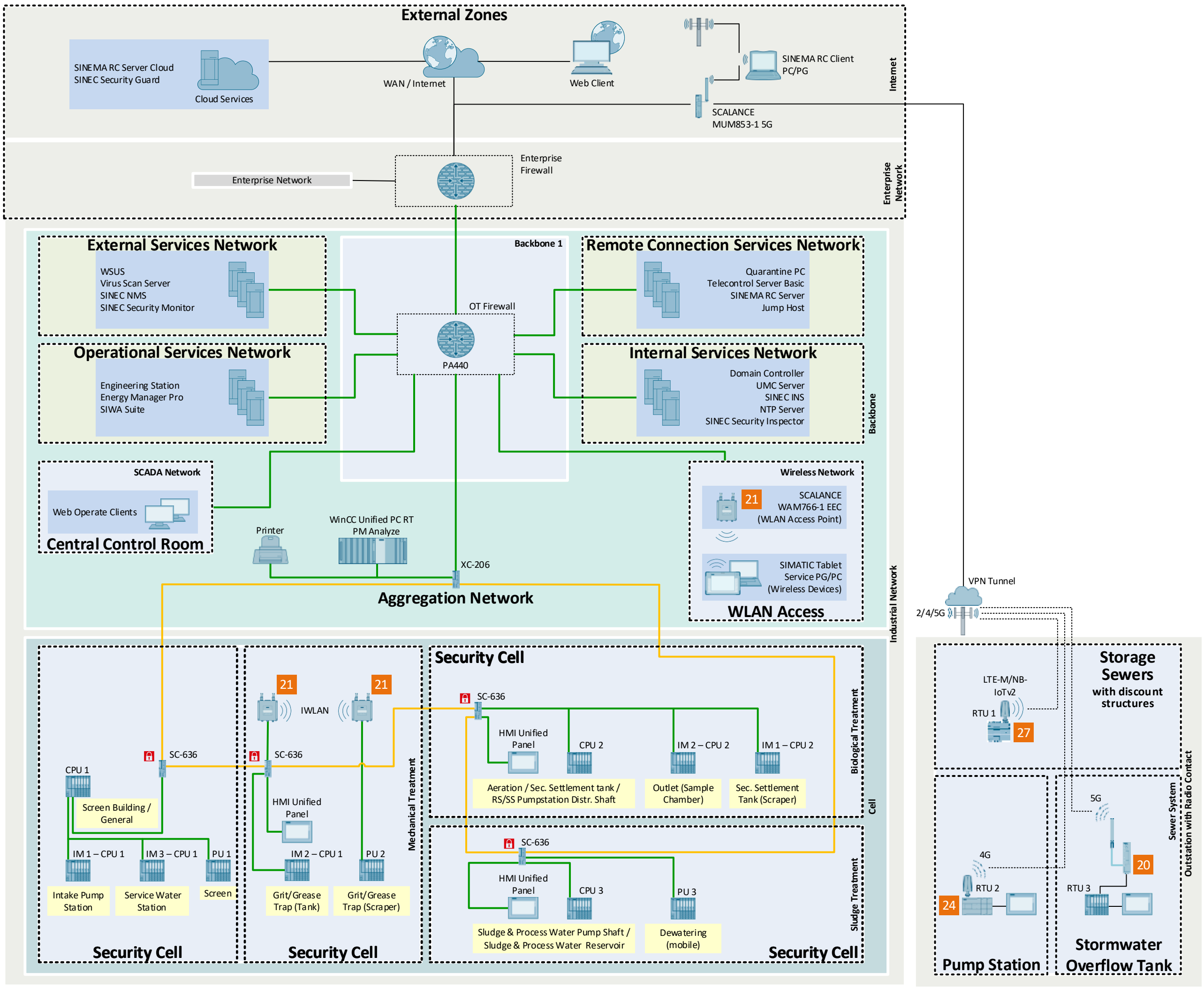


Figure 6-2: Wireless communication.

Table 6-8: Wireless devices.

SCI	Supplier	Type	MLFB	Function
20	Siemens	SCALANCE MUM 853-1 5G	6GK5853-2EA00-2DA1	High-performance and secure connectivity over 5G networks.
21	Siemens	SCALANCE WAM766-1 EEC	6GK5766-1GE00-7TX0	Access point for secure wireless communication.
24	Siemens	CPU 1214C with CP 1243-7 LTE EU	6GK7243-7KX30-0XE0	Secure connection between the SIMATIC S7-1200 CPU in the external pump station and the central plant area.

SCI	Supplier	Type	MLFB	Function
27	Siemens	RTU 3051C with integrated modem for LTE-M/NB-IoTv2	6NH3112-5BB00-0XX0	Secure connection between the RTU in the storage sewers and the central plant building.

The hardening measures for the SCALANCE devices are listed in Table 6-4 and Table 6-5.

In addition to these general hardening measures and configuration, the following hardening measures must be considered for wireless SCALANCE appliances.

Table 6-9: Additional HW measured for SCALANCE W.

No.	Security topic	Hardening measure	Documentation
1	WLAN encryption	Enable AES encryption for iPCF.	\10\ – Section 3.12.1
2	WLAN layer 2 tunnel	Set Mac mode to 'Layer 2 tunnel'. This setting is only supported when exclusively using SCALANCE devices.	\10\ – Section 3.12.2
3	WLAN iPCF	Use iPCF if time-critical data, i.e. PROFINET, is being transferred via the radio link.	\10\ – Section 3.12.3

Hardening measures for the wireless TeleControl CP 1243-7 LTE EU are detailed in Section 6.6.

6.4. Network components – SCALANCE XC

The SCALANCE XC-200 series of managed Layer 2 switches provide connectivity between automation devices within the process cells.

Table 6-10: SCALANCE XC switches.

SCI	Supplier	Type	MLFB	Function
22	Siemens	SCALANCE XC-206 – 2SFP	6GK5206-2BS00-2AC2	Ring manager in the Aggregation Network.
-	Siemens	SCALANCE XC-208	6GK5208-0BA00-2AC2	Switch to provide Layer 2 network connectivity for devices in the: Intake Pump Station, Stormwater overflow tank, External pump station, Screen, Grit/Grease Trap, Secondary settlement tank, Outlet, Dewatering.
-	Siemens	SCALANCE XC-216	6GK5216-0BA00-2AC2	Switch to provide Layer 2 network connectivity for devices in the: Screen Building/General, Sludge & Process water reservoir.
-	Siemens	SCALANCE XC-224	6GK5224-0BA00-2AC2	Switch to provide Layer 2 network connectivity for devices in the: Aeration process.

The hardening measures for the SCALANCE switches are listed in Table 6-4 and Table 6-5.

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

Table 6-11: Additional hardening measures for SCALANCE XC-200.

No.	Security topic	Hardening measure	Documentation
1	Ring redundancy	Disable ring redundancy, if the device is not operated in a ring topology.	\10\ – Section 3.11.1
2	PROFINET	If the SCALANCE device is used in a PROFINET network, the PROFINET interface functionality must be enabled.	\10\ – Section 3.7

6.5. TeleControl CP 1542SP-1 IRC

The communication processor CP 1542SP-1 IRC connects ET 200SP CPUs to control centers using telecontrol protocols such as TeleControl Basic, DNP3, and IEC 60870-5-104.

In the blueprint, the CP 1542SP-1 IRC operates in conjunction with the wireless SCALANCE MUM 853-1 to establish secure telecontrol communication between the stormwater overflow tank and the TeleControl Server Basic in the central plant building. Refer to Figure 3-12.

The hardening measures for the CP 1542SP-1 IRC are listed below.

Table 6-12: Hardening measures for CP 1542SP-1 IRC.

No.	Security topic	Hardening measure	Documentation
1	VPN	Use SINEMA RC (OpenVPN).	\32\ – Section 1.6 \32\ – Section 1.7
2	SNMP	Disable SNMP or use SNMP v3.	\32\ – Section 1.7

6.6. TeleControl CP 1243-7 LTE

The CP 1243-7 LTE EU communication processor is employed to connect SIMATIC S7-1200 CPUs with LTE networks operating in European frequency bands.

For the wastewater treatment plant, the communication module is configured with TC-SRC (telecontrol communication via SINEMA Remote Connect) to secure the connection between the external pump station and the central plant area. Refer to Figure 3-13.

The following hardening measures are recommended.

Table 6-13: Hardening measures for CP 1243-7 LTE.

No.	Security topic	Hardening measure	Documentation
1	VPN	Use VPN tunnels: • IPsec • SINEMA RC (OpenVPN)	\30\ – Section 1.5
2	Firewall	Activate firewall: • IP firewall with stateful packet inspection – layer 3 and 4. • Firewall for ‘non-IP’ Ethernet frames according to IEEE 802.3 – layer 2. • Limitation of the transmission speed to restrict flooding and DoS attacks. • Global firewall rules.	\30\ – Section 1.5
3	Web server access to the CPU	Use HTTPS only.	\30\ – Section 1.5
4	NTP	Use secure NTP for secure transfer during time-of-day synchronization with telecontrol communication disabled.	\30\ – Section 1.5

6.7. TeleControl RTU 3051C

The compact SIMATIC RTU 3051C is used to monitor the storage sewers with discount structures. This remote station is geographically distributed and operates without a connection to the power supply network.

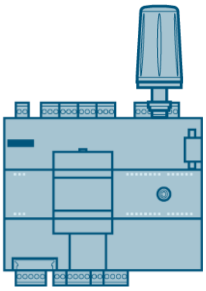


Figure 6-3: RTU 3051C.

The remote terminal unit can store process data and transfer it via mobile wireless communication to a master station. To ensure secure communication between the RTU 3051C in the remote station and the TeleControl Server Basic in the central plant building, encrypted communication is established through the SINEMA RC server. Refer to Figure 3-14.

The hardening measures for the RTU 3051C are listed below.

Table 6-14: Hardening measures for RTU 3051C.

No.	Security topic	Hardening measure	Documentation
1	VPN	Use OpenVPN: configure the RTU as an OpenVPN client.	\28\ – Section 3.8 \28\ – Section 6.15.1
2	HTTPS for WAN	• Enable HTTPS for WAN. • Block receipt of SMS messages.	\28\ – Section 6.13
3	Web server access	Use HTTPS only.	\28\ – Section 6.15.3

6.8. NTP Server

The NTP Server centrally manages time synchronization across the entire plant, and it is located within the Internal Services Network.

The Domain Controller receives the time signal from the NTP Server and distributes it to the workstations and servers located in the DMZ. Embedded devices, such as the WinCC Unified PC RT, Unified Comfort Panels, or the ET 200SP distributed controllers, receive the time signal directly from NTP Server.

The recommended security measures are:

- Use of secure NTP, i.e. Network Time Security – NTS.
- Use of SNMPv3.

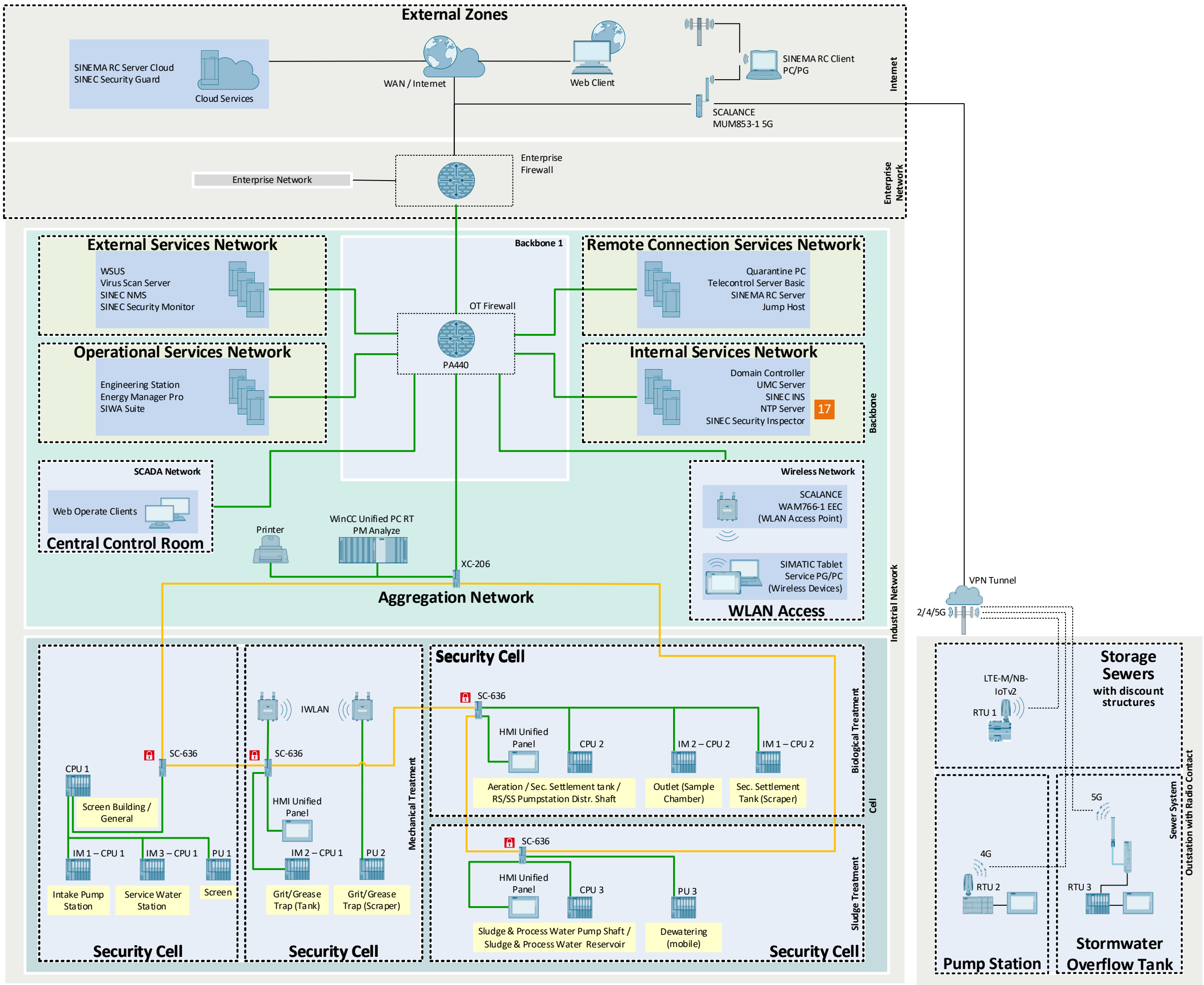


Figure 6-4: NTP Server.

6.9. Workstations and servers

In the blueprint's Wastewater Treatment Plant, the software applications and WinCC Unified PC RT are installed on Siemens' Industrial Workstations – IPCs.

6.9.1. Workstations and servers

The following hardening measures must be implemented for both the WinCC Unified PC RT workstation and the servers running in the DMZ.

Table 6-15: General hardening measures for workstations and servers.

No.	Security topic	Hardening measure	Documentation
1	Secure Network	Use of the Window's firewall.	\47\ – Section 2.1 \47\ – Section 5.1
2	Identity and Access Management	• Set up BIOS settings. • Configure user administration with Active Directory.	-
3	Reduction of Surface Attack	• Remove unnecessary Windows components. • Disable unused Windows services. • Diasable the Automation License Manager (ALM) server funtionality if the plant is in operation. • Enable SMB signing. • Disable SMVv1. • Block USB storage media: - Lock or disable through mechanical means. - Restrict access via Windows group policy. • USB-Ports – Disable autorun and autoplay.	\47\ – Section 2.1 \47\ – Section 4.8 \47\ – Section 4.10 \47\ – Section 4.11
4	Secure Channels and Encryption	Enble encrypted communication in the SIMATIC Shell.	-
5	System Integrity	• Use of whitelisting Technologies. • Installation of a virus scanner. • Use digital signatures to verify that applications, binaries and libraries have not been altered. • Patching the Operating System. • Backup of engineering and system data.	-
6	Logging and Monitoring	• Use Event Viewer to monitor security logs, system logs and application logs. • Forward logs to central server using Windows Event Forwarding (WEF) or Syslog.	-

Some of the aforementioned hardening measures can be configured in the Group Policy Objects (GPOs) of Windows. In the blueprint, the GPOs are managed centrally on the Domain Controller. Refer to Section 7.1.

For further security settings regarding Windows and Linux based IPCs, refer to the following documentation.

- \47\ – Recommended Security Settings for IPCs in the Industrial Environment (Windows)
- \48\ – SIMATIC IPC - Security Guidelines for Linux systems

6.9.2. WinCC Unified PC RT

For the WinCC Unified PC RT and Web Operate Clients, additional security can be achieved with Windows Kiosk mode. This mode restricts users to a single application – such as Microsoft Edge for accessing the SCADA system – thereby preventing access to the Windows environment, system settings and other applications.

Table 6-16: Hardening measures for WinCC Unified PC Runtime.

No.	Security topic	Hardening measure	Documentation
1	Windows Kiosk mode	Use Windows Kiosk mode to prohibit access to default Windows functions.	\3\ – Section 3.5

Additional hardening measures regarding the use of services and applications in WinCC Unified can be found in the security guideline.

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 5 (Risk analysis when using services and apps)

6.9.3. PM ANALYZE

PM ANALYZE is a WinCC Add-on that offers a powerful toolset for archiving, analysis, and reporting, extending the functionality of the SCADA system. It is employed in the blueprint to prepare and create special reports to conform with the DWA – German Association for Water, Wastewater and Waste Management – and it consists of the following modules.

- PM-SERVER : Central platform for data archiving and management.
- PM-AGENT : Manages the data transfer from the WinCC Unified PC RT to the PM-SERVER. All incoming alarms and process values are forwarded to the server where they are recorded in the configured alarm or process value archives.
- PM-CLIENT : Delivers the user interface component, providing visualization and analysis capabilities for operators and analysts.

In the Wastewater Treatment Plant, both the PM-SERVER and PM-AGENT are hosted on the same workstation as the WinCC Unified PC RT. The PM-CLIENT is deployed in the Central Control Room, enabling operators to access and visualize archived data and reports.

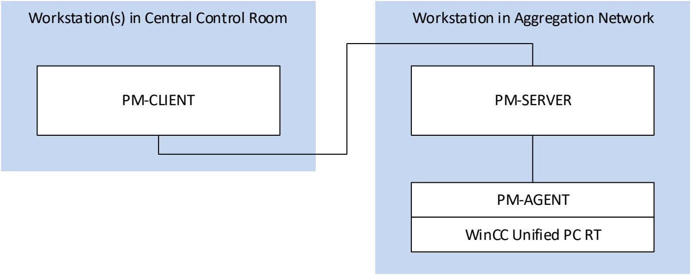

Workstation(s) in Central Control Room
PM-CLIENT
Workstation in Aggregation Network
PM-SERVER
PM-AGENT
WinCC Unified PC RT

Figure 6-5: PM-ANALYZE implementation.

All hardening measures mentioned in Section 6.9.1 apply; however, the use of whitelisting on the PM ANALYZE station is not recommended.

Further information on PM-ANALYZE can be found in the following document.

- \49\ – PM-ANALYZE System description

6.9.4. SINEC NMS

SINEC NMS is a Network Management System deployed to monitor and administer networks and their devices. It supports a distributed system architecture that consists of one central 'Control' component and one or more distributed 'Operation' instances located in different network segments, such as the Aggregation Network or the WLAN Access Network.

- NMS Control : Manages configuration policies, analyzes diagnostic data and provides an overview of the entire OT network infrastructure. NMS Control also provides northbound interfaces for the integration into overlying systems and services; that include Syslog forwarding, URL access, inventory list and email notifications.
- NMS Operation : Automatically monitors and collects device information to compile performance statistics and periodically sends reports to the central NMS Control. Events can be detected directly by NMS Operation components or devices can send notifications and alarms. Changes like device configuration or firmware updates will be triggered by NMS Control and performed by NMS Operation.

SINEC NMS supports both local and central user management through UMC. In the blueprint, user authentication is performed with UMC, enabling centralized user administration, the integration of UMC user groups into SINEC NMS, and support for Web Single Sign-On (Web SSO) – allowing users to switch between the web interfaces of NMS Control and NMS Operation without needing to log in multiple times.

Although the UMC server can be installed together with SINEC NMS on the same PC, this blueprint splits them up to comply with network segmentation requirements. NMS Control is deployed in the External Services Network, to enable web server access from the enterprise level, while the UMC server runs in the Internal Services Network of the DMZ.

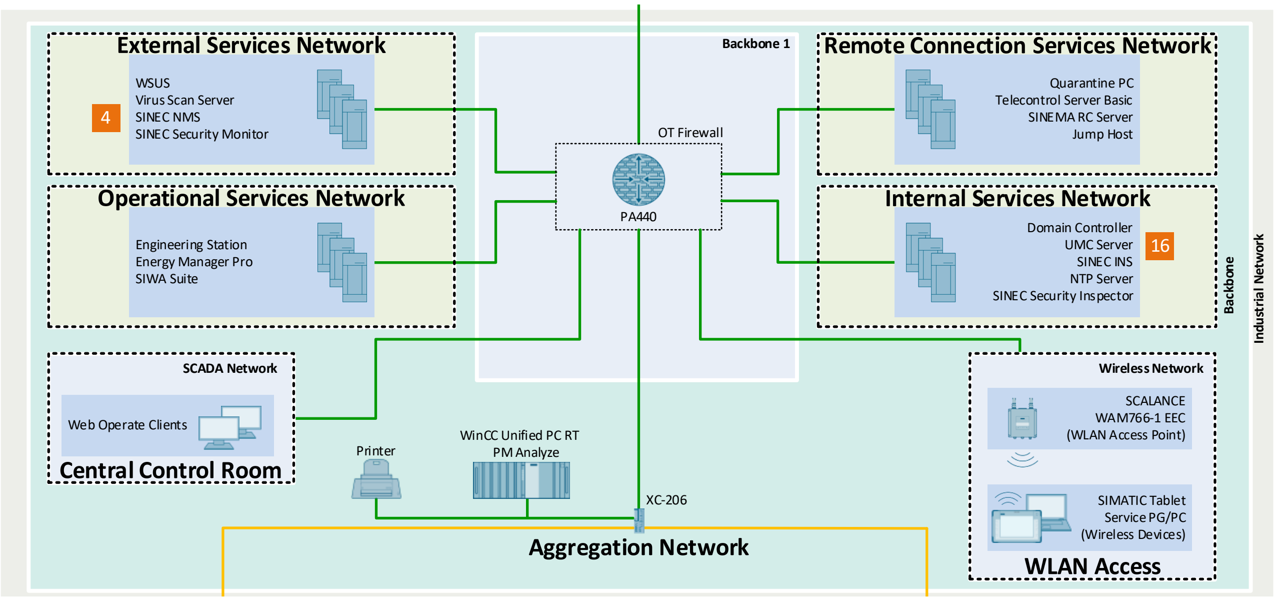


Figure 6-6: SINEC NMS and UMC Server.

NOTICE

Deployment of NMS Control

In the Wastewater Treatment Plant blueprint, NMS Control is hosted in the External Services Network to enable web server access from the enterprise level. If SINEC NMS shall not be accessible from overlying networks, NMS Control shall be placed in the Internal Services Network.

In addition to the hardening measures stated 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, as it may negatively impact the functionality of SINEC NMS.

Further information on SINEC NMS can be found in the following documents.

- \43\ – Network management SINEC NMS
- \44\ – Getting Started with SINEC NMS

6.9.5. SIMATIC Energy Manager Pro

SIMATIC Energy Manager Pro is an industrial energy management system – certified in accordance with ISO 50001 – that provides detailed visualizations of energy flows and consumption values within processes. These values are assigned to the relevant consumers or cost centers, allowing businesses to monitor, manage and optimize energy consumption.

In addition to the hardening measures listed in Section 6.9.1, it is recommended to follow the guidelines provided in the installation manual.

- \50\ – 'SIMATIC Energy Manager V7.2 – Installation', Section 3 (Installing Energy Manager)

Further information about the SIMATIC Energy Manager Pro is provided in the following documentation.

- \51\ – 'SIMATIC Energy Manager PRO V7.5 – Operation'
- \52\ – 'SIMATIC Energy Manager V7.5 – Acquisition'
- \53\ – 'SIMATIC Energy Manager V7.5 – System description'

6.10. Automation devices

6.10.1. WinCC Unified Comfort Panels

WinCC Unified Comfort panels are deployed across various process cells within the wastewater treatment plant to monitor and control operations. Based on the Threat and Risk Analysis performed in Section 4.3, the following hardening measures are required to ensure secure commissioning and operation of the MTP1000 Unified Comfort Panels.

Table 6-17: Hardening measures for WinCC Unified Comfort Panels.

No.	Security topic	Hardening measure	Documentation
1	Access control	• Protect the TIA Portal project. • Assign roles to local and/or global users following the principle of least privilege. • Enable access protection on the HMI panel.	\3\ – Section 2.1 \3\ – Section 2.6 \3\ – Section 3.4.1
2	Expansion ports	Disable unused USB and SD card interfaces.	\3\ – Section 4.1.1
3	Network security	• Disable unused ports and network adapters. • Use encrypted communication to securely exchange data with controllers, engineering stations and other Unified devices.	\3\ – Section 2.5 \3\ – Section 2.9 \3\ – Section 4.1.2
4	Logging and monitoring	Use the Audit Trail System to prove which human user performed which changes.	\37\ – Audit Trail System
5	Secure commissioning	• Disable project transfer during operation. • Activate encrypted project transfer during commissioning.	\3\ – Section 2.7.3

Figure 6-7: MTP1000 Unified Comfort.

Additional hardening measures regarding the use of services and applications can be found in the security guideline for WinCC Unified.

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 5 (Risk analysis when using services and apps)

6.10.2. SIMATIC Controllers

SIMATIC S7-1200 basic controllers and SIMATIC ET 200SP distributed controllers are employed in the blueprint to control the processes of the sewer system, mechanical treatment, biological treatment and sludge treatment.

The following hardening measures apply to all SIMATIC controllers used in the blueprint.

Table 6-18: Hardening measures for SIMATIC controllers.

No.	Security topic	Hardening measure	Documentation
1	Access control	Enable access contol to restrict user access to specific PLC functionalities.	\56\ – Section 1.3
2	Secure communication	Use secure communication methods: • Only allow secure PG/PC and HMI communication. • Use Sign&Encrypt for OPC UA communication. • Employ Secure Open User Communication (OUC) with TLS v1.3.	\55\ – Section 2.2 \57\ – Section 2.4 \57\ – Section 2.6 \57\ – Section 2.7
3	Protection of the PLC's confidential configuration data.	Enable password-based protection to encrypt the PLC's confidential configuration data.	\55\ – Section 2.3

NOTICE

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.

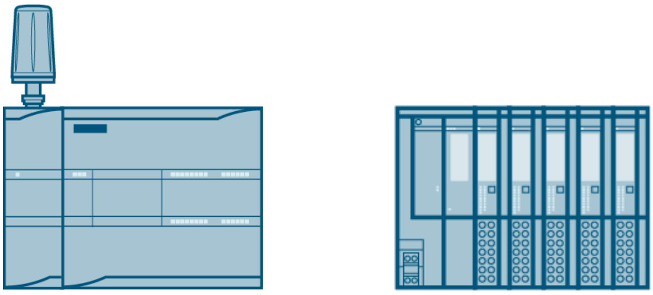


Figure 6-8: CPU 1214C with CP 1243-7 LTE and ET 200SP Distributed Controller.

6.10.3. Distributed IO Periphery

The Distributed IO Periphery is employed to connect field-level sensors and actuators to the controllers via PROFINET IO communication. The hardening measures for these devices align with the specifications defined by PROFINET Security Class 1.

No.	Security topic	Hardening measure	Documentation
1	GSD files	GSDX to ensure integrity and authenticity of GDS files during import.	\58\ – Security Class 1 for PROFINET Security, Section 4
2	SNMP	Disable SNMP.	\58\ – Security Class 1 for PROFINET Security, Section 5
3	DCP	Set DCP mode to read-only.	\58\ – Security Class 1 for PROFINET Security, Section 6

Figure 6-9: IM 155-6 PN BA.

6.10.4. Remote Terminal Units

Remote Terminal Units are employed to monitor and control outlying stations without a connection with the power supply network. RTUs support the following core functions.

- Energy saving operation.
- Process connection – through its equiped inputs and outputs, and via expansion card.
- Controller – for simple control tasks.
- Storing/Logging process data – when there is no connection to the communication partner.
- TeleControl communication protocols.
- Position determination and time synchronization via GPS.

Hardening measures for the blueprint’s remote terminal unit – RTU 3051C – are defined in Section 6.7.

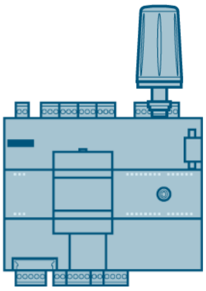


Figure 6-10: RTU 3051C.

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.

7.1. Domain controller

The Domain Controller in the blueprint is hosted within the Internal Services Network of the DMZ. This placement ensures secure and controlled access – through the OT Firewall – to authentication and directory services for devices, applications, servers, and workstations located in both the DMZ and Aggregation Networks.

By centralizing user management in the Internal Services Network of the DMZ, consistent policy enforcement can be achieved across the entire OT environment.

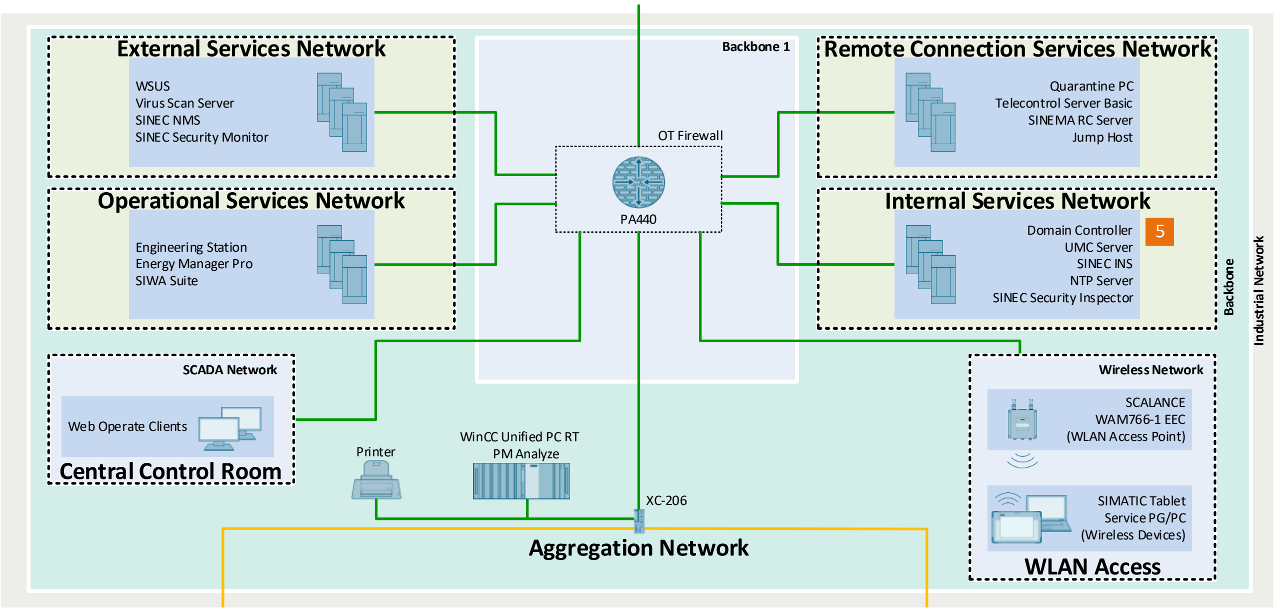


Figure 7-1: Domain Controller in the blueprint's Wastewater Treatment Plant.

7.2. User Management Component

The User Management Component is used to establish a centralized system for managing users and user groups across various Siemens' software and devices. It can be integrated with Microsoft Active Directory, allowing existing users and groups to be imported and synchronized.

7.2.1. UMC Ring Server

The UMC ring server serves as the central configuration platform for user management within the UMC domain and is located within the Internal Services Network. On this server, users are defined with the relevant group assignments for the UMC domain. To enable the transfer of users and groups from the Active Directory, the UMC ring server PC must be added to the AD Domain.

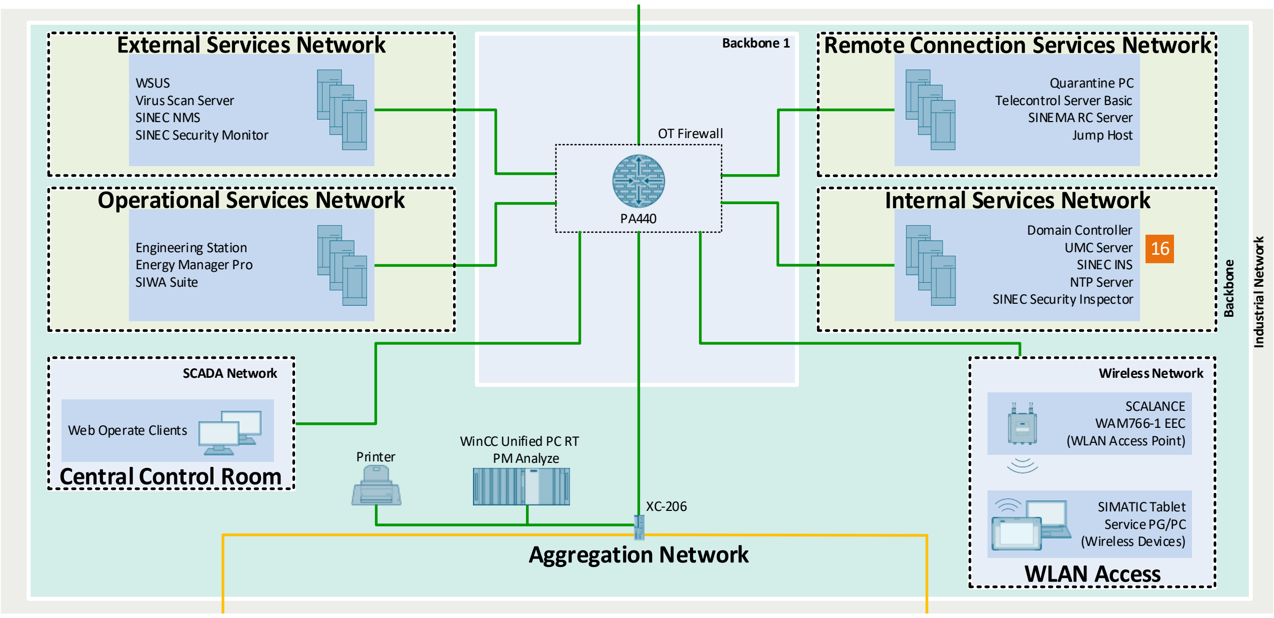


Figure 7-2: UMC Ring Server in the blueprint's Wastewater Treatment Plant.

For enhanced availability, the UMC ring server can be deployed in a redundant configuration.

- \18\ – Central User Management with 'User Management Component (UMC)'

7.3. User authentication and authorization for WinCC Unified

WinCC Unified provides secure mechanisms to ensure that only authenticated users can access the system and that their actions are restricted based on their assigned roles. Authentication, which verifies user identities, can be managed either locally or centrally via UMC. Authorization, which determines what authenticated users are permitted to do, is always enforced locally on the runtime device.

Role-based access control, aligned with the principle of least privilege, ensures users are only granted the necessary engineering/runtime rights to perform their specific tasks. Roles can be either predefined – HMI Operator, HMI Administrator, HMI Monitor, HMI Monitor Client – or custom-defined to meet specific operational requirements.

In the blueprint's Wastewater Treatment Plant, centralized authentication is implemented using UMC in conjunction with Microsoft Active Directory. In this setup, users log in with their domain credentials, and user and group information is synchronized from the AD domain to the UMC Ring Server.

- \54\ – 'Configuring users and roles (RT Unified)'

7.3.1. Benefits of using Active Directory and UMC for user authentication

An Active Directory system allows the enforcement of password policies through the Group Policy Editor. With enforced settings, all users must adhere to the defined security standards, thereby protecting the TIA Portal engineering project and WinCC Unified devices from vulnerabilities associated with weak passwords.

In addition to password enforcement, an Active Directory based user authentication mechanism allows the synchronization of users and groups inside a domain, simplifiying user maintenance and administration. With UMC, user authentication can be centrally managed, eliminating the need to perform individual TIA Portal downloads on each WinCC Unified panel or PC RT.

8. Malware protection and application control

The integrity of the system has to be protected against unauthorized changes of software and data, and these changes need to be detected, recorded and reported. In the blueprint, the protection against malware and unauthorized changes is implemented using anti-virus software and whitelisting technologies.

Anti-virus software

The latest version of the Trellix Endpoint Security (ENS) is installed on the workstations and servers of the blueprint. Trellix Endpoint Security is more than a traditional anti-virus software, as it employs additional advanced features detailed in the product's data sheet.

- \24\ – Trellix Endpoint Security data sheet

Whitelisting software

The latest version of Trellix Application and Change Control is installed on the workstations and servers of the blueprint.

- Trellix Application Control can be used to block the start of unauthorized or unknown applications. After the installation and activation of Trellix Application Control, all executable applications and files are protected against modification.

  Contrary to simple allowlisting concepts, Trellix Application Control uses a dynamic trustworthiness model. This eliminates the lengthy, manual updates of approved application lists. Updates of authorized applications in the list can be integrated through:

  - Trustworthy users.
  - Trustworthy manufacturers.
  - Trustworthy directories.
  - Binary files.
  - Updaters, like Windows Update or virus scanners.

  Furthermore, Trellix Application Control offers functions that monitor the main memory, protect files that are running in the main memory, and provide protection against buffer overflow.

- Trellix Change Control prevents unauthorized changes to critical system files, directories, and configurations, while simplifying the implementation of new policies and compliance measures. It features file integrity monitoring and change prevention, enforcing change policies and continuously monitoring critical systems. Additionally, it detects and blocks unwanted changes across distributed and remote locations.

Centralized security management

Both; Trellix Endpoint Security, and Trellix Application and Change Control, can be configured and managed centrally using Trellix ePolicy Orchestrator (ePO). This software is installed on the Infrastructure PC, located in the External Services Network of the DMZ, simplifying policy management and enforcement across the workstations and servers.

- \23\ – Trellix Endpoint Security
- \25\ – Trellix Application and Change Control
- \26\ – Trellix ePolicy Orchestrator

9. Patch management

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 key measure to protect the integrity of an automation control system is patch management, which forms part of the overall security strategy.

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

- Operating System Patches for Microsoft Windows : This category includes all types of updates, service packs, feature packs, and similar installations, regardless of whether they are related to security.
- Security Updates for Microsoft Windows : These updates specifically address security-related issues.
- Firmware and Software Patches : These patches address vulnerabilities in Siemens software and products, as well as third-party components.

For Siemens software and products, security vulnerabilities are managed by the responsible Siemens product unit. This also applies to vulnerabilities in third-party components within Siemens products. However, for third-party components not owned by Siemens, the responsibility falls on the plant owner to ensure that these components are kept up to date with the latest patches throughout their complete lifecycle.

Siemens publishes advisories for all products, including third-party components, on a monthly basis.

- \19\ – Siemens ProductCERT and Siemens CERT

9.1. Patch management for Microsoft Windows

The Infrastructure PC in the DMZ manages Windows patches for the automation control system. Some tools to manage Windows patches are listed below.

Windows Server Update Service (WSUS)

Installed on the Infrastructure PC, WSUS can receive Windows patches either from the Microsoft Update server or from a server in the enterprise network and distribute them to all Windows-based PCs in the automation control system.

NOTICE

WSUS deprecation announcement for 2025

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 is 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.

Windows Autopatch, Microsoft Intune and Azure Update Manager

While the WSUS service remains available in Windows Server 2025, Microsoft recommends organizations to transition to cloud tools, including Windows Autopatch and Microsoft Intune – for client update management – and Azure Update Manager – for server update management.

- \20\ – Microsoft Autopatch
- \21\ – Microsoft Intune
- \22\ – Azure Update Manager

9.2. Patch management of automation and network components

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

- \59\ – Updates for SIMATIC WinCC Unified PC Runtime V20
- \60\ – Image-Downloads for SIMATIC HMI Operator Panels: Unified Comfort Panels
- \61\ – Firmware update S7-1500 CPUs incl. Displays and ET 200 CPUs (ET 200SP, ET 200pro)
- \62\ – Firmware update for CPU 1214C, DC/DC/DC, 14DI/10DO/2AI

10. Backup and recovery

The ability to recover and restore an automation control system to a known, operational state following a disruption or failure is a critical aspect of the Defense-in-Depth strategy, as recommended in IEC 62443.

In a Backup and Restore strategy, it is important to identify all necessary data required to recover the IACS to a known state and its location in the system. 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.

System backup

A system backup refers to a complete system image, i.e. a snapshot of the current system at a specific point in time. This includes:

- Hardware-specific files, such as 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

Backup of the TIA Portal project(s) used to configure the WinCC Unified visualization systems and automation devices, such as the S7-1200 PLCs and ET 200SP Distributed Controllers.

Component-specific data

Component-specific backups include data such as databases or individual configurations of embedded and network devices.

For WinCC Unified panels, the following backup mechanisms are available.

- Backup & restore : Full backup of the panel's data, which can be restored to a device of the same model. The backup file is non-editable and includes all configuration data.
- Automatic backup: Continuous, automated backup of process-related data to a SIMATIC HMI SD memory card.

For SCALANCE network devices, backup and restore operations are managed using the SINEC NMS Configuration Repository.

- \3\ – 'Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices', Section 4.1.4 (Backup and restoration of panel data)
- \43\ – Network management SINEC NMS, Section 4.5 (Device configuration repository)
- \44\ – Getting Started: Understanding and Using SINEC NMS – Further documentation (backup)

NOTICE

System recovery readiness

Restoring systems is often more critical than creating backups. Recovery processes need to be tested in advanced and must be reproducible to ensure system availability during emergencies, minimizing downtime.

10.1. Disposal of components

Sensitive data, such as passwords, cryptographic material, and configurations, can be misused if disclosed to unauthorized individuals. Asset owners must securely purge all customer information on those devices that are no longer required.

This requirement applies to all devices, including removable media.

Table 10-1: Disposal of components that contain sensitive and confidential customer data.

Device	Customer/confidential information	Disposal of the component
Embedded devices	User program, scripts, cryptographic keys, etc.	Reset PLCs and HMI panels to factory settings and securely erase the flash memory.
Network devices	Firewall rules.	Reset SCALANCE components to the factory state. SINEC NMS can perform resets using specific device profiles.
Storage media	Depends on usage.	USB drives, CDs, DVDs and other media must be completely erased or handed over for secure disposal, i.e. shredding.
Hosts	Configuration, passwords, cryptographic keys, etc.	Entire systems, such as IPCs, must be handed over for secure disposal.

11. Appendix

11.1. 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

11.2. Links and literature

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109780322
\3\	Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices https://support.industry.siemens.com/cs/ww/en/view/109481300
\4\	Certification and standards 'TÜV Süd certification based on IEC 62443' https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity/certification-standards.html
\5\	IEC 62443-4-1 Secure product development lifecycle https://assets.new.siemens.com/siemens/assets/api/uuid:b78aadd6-2ec7-44e6-9fd1-e221f4c2a988/secure-product-development-lifecycle-iec62443-4-1-en.pdf
\6\	SIMATIC S7-1500 S7-1500R/H redundant system https://support.industry.siemens.com/cs/ww/en/view/109754833
\7\	Connecting WinCC Unified to User Management Component (UMC) https://support.industry.siemens.com/cs/ww/en/view/109780337
\8\	Siemens Industrial Cybersecurity Services https://www.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html
\9\	Continuous endpoint protection against malware https://www.siemens.com/in/en/products/services/digital-enterprise-services/industrial-security-services/endpoint-protection.html
\10\	Checklist for Setting Up SCALANCE Devices https://support.industry.siemens.com/cs/ww/en/view/109745536
\11\	PAN-OS Administrator's Guide https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/getting-started
\12\	Palo Alto – PAN-OS https://docs.paloaltonetworks.com/pan-os
\13\	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
\14\	User administration for SCALANCE devices with RADIUS protocol https://support.industry.siemens.com/cs/ww/en/view/98210507
\15\	All-round protection with Industrial Security - System Integrity https://support.industry.siemens.com/cs/de/en/view/92605897
\16\	All-round protection with Industrial Security - Network Security https://support.industry.siemens.com/cs/de/en/view/92651441
\17\	All-round protection with Industrial Security - Plant Security https://support.industry.siemens.com/cs/de/en/view/50203404
\18\	Central User Management with 'User Management Component (UMC)' https://support.industry.siemens.com/cs/ww/en/view/109780337

No.	Topic
\19\	Siemens ProductCERT and Siemens CERT https://www.siemens.com/global/en/products/services/cert.html
\20\	Windows Autopatch https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/overview/windows-autopatch-overview
\21\	Microsoft Intune https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/what-is-intune
\22\	Azure Update Manager https://azure.microsoft.com/en-us/products/azure-update-management-center
\23\	Trellix Endpoint Security https://www.trellix.com/products/endpoint-security
\24\	Trellix Endpoint Security data sheet https://www.trellix.com/assets/data-sheets/trellix-endpoint-security-datasheet.pdf
\25\	Trellix Application and Change Control https://www.trellix.com/products/trellix-application-control
\26\	Trellix ePolicy Orchestrator https://www.trellix.com/products/epo
\27\	SIMATIC RTU 3051C – 6NH3112-5BB00-0XX0 https://mall.industry.siemens.com/mall/en/ww/Catalog/Product/?mlfb=6NH3112-5BB00-0XX0&SiepCountryCode=WW
\28\	SIMATIC NET TeleControl - RTU SIMATIC RTU 3030C/RTU 30x1C https://support.industry.siemens.com/cs/ww/en/view/109986730
\29\	CP 1243-7 LTE EU – 6GK7243-7KX30-0XE0. Connection of SIMATIC S7-1200 to LTE network in European frequency range https://mall.industry.siemens.com/mall/en/ww/Catalog/Product/?mlfb=6GK7243-7KX30-0XE0&SiepCountryCode=WW
\30\	SIMATIC NET: S7-1200 - TeleControl CP 1243-7 LTE https://support.industry.siemens.com/cs/ww/en/view/109476704
\31\	CP 1542SP-1 IRC – 6GK7542-6VX00-0XE0. Connection of SIMATIC S7-ET 200SP to Industrial Ethernet, SINAUT ST7, TeleControl Server Basic, IEC 60870-5-104 or DNP3 protocol to a control center https://mall.industry.siemens.com/mall/en/ww/Catalog/Product/?mlfb=6GK7542-6VX00-0XE0&SiepCountryCode=WW
\32\	SIMATIC NET: ET 200SP - Industrial Ethernet CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1 https://support.industry.siemens.com/cs/ww/en/view/109977935
\33\	SCALANCE MUM853-1 – 6GK5853-2EA00-2DA1. 5G router for wireless communication via public 3/4/5G mobile radio networks and private 5G networks https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK5853-2EA00-2DA1
\34\	SIMATIC NET Industrial Ethernet Security SINEC Security Monitor Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109982510
\35\	Network concepts for industrial automation networks https://support.industry.siemens.com/cs/ww/en/view/109802750
\36\	Palo Alto – DoS and Zone Protection Best Practices https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices
\37\	SIMATIC WinCC Unified online documentation: WinCC Audit (RT Unified) https://docs.tia.siemens.cloud/r/en-us/v20/wincc-audit-rt-unified

No.	Topic
\38\	Sending SIMATIC S7-1200/S7-1500 CPU Security Messages via Syslog to SINEC INS https://support.industry.siemens.com/cs/ww/en/view/51929235
\39\	SIMATIC S7-1500/ET 200MP, S7-1500R/H, Drive Controller, S7-1500 Software Controller, ET 200SP, ET 200pro Syslog Messages https://support.industry.siemens.com/cs/ww/en/view/109823696
\40\	SIMATIC NET Network management SINEC INS https://support.industry.siemens.com/cs/ww/en/view/109978415
\41\	SIMATIC NET Industrial Ethernet Security SCALANCE SC-600 https://support.industry.siemens.com/cs/ww/en/view/109954186
\42\	SIMATIC NET Industrial Ethernet Switches SCALANCE Layer 2 Switches https://support.industry.siemens.com/cs/ww/en/view/109977339
\43\	SIMATIC NET Network management SINEC NMS https://support.industry.siemens.com/cs/ww/en/view/109973629
\44\	Getting Started: Understanding and Using SINEC NMS https://support.industry.siemens.com/cs/ww/en/view/109762792
\45\	SIMATIC NET Industrial Ethernet Security SINEC Security Inspector https://support.industry.siemens.com/cs/ww/en/view/109988448
\46\	SINEC Security Guard https://xcelerator.siemens.com/global/en/all-offerings/products/s/sinec-security-guard.html
\47\	Recommended Security Settings for IPCs in the Industrial Environment (Windows) https://support.industry.siemens.com/cs/ww/en/view/109475014
\48\	SIMATIC IPC - Security Guidelines for Linux systems https://support.industry.siemens.com/cs/ww/en/view/109768383
\49\	PM-ANALYZE System description https://cache.industry.siemens.com/dl/files/856/109782856/att_1036486/v2/PM-ANALYZE_Systemdescription.pdf
\50\	SIMATIC Energy Manager V7.2 – Installation https://support.industry.siemens.com/cs/ww/en/view/109742441
\51\	SIMATIC Energy Manager PRO V7.5 – Operation https://support.industry.siemens.com/cs/ww/en/view/109963217
\52\	SIMATIC Energy Manager V7.5 – Acquisition https://support.industry.siemens.com/cs/ww/en/view/109963216
\53\	SIMATIC Energy Manager V7.5 – System description https://support.industry.siemens.com/cs/ww/en/view/109811736
\54\	SIMATIC WinCC Unified online documentation: Configuring users and roles (RT Unified) https://docs.tia.siemens.cloud/r/en-us/v20/configuring-users-and-roles-rt-unified
\55\	Configuration of the security functions in TIA Portal V17 https://support.industry.siemens.com/cs/ww/en/view/109798583
\56\	User Management & Access Control with TIA Portal V19 https://support.industry.siemens.com/cs/ww/en/view/109973173

No.	Topic
\57\	Using Certificates with TIA Portal https://support.industry.siemens.com/cs/ww/en/view/109769068
\58\	PROFINET Security https://profinet.co.uk/profinet-security/
\59\	Updates for SIMATIC WinCC Unified PC Runtime V20 https://support.industry.siemens.com/cs/ww/en/view/109963700
\60\	Image-Downloads for SIMATIC HMI Operator Panels: Unified Comfort Panels https://support.industry.siemens.com/cs/ww/en/view/109825605
\61\	Firmware update S7-1500 CPUs incl. Displays and ET 200 CPUs (ET 200SP, ET 200pro) https://support.industry.siemens.com/cs/ww/en/view/109478459
\62\	Firmware update for CPU 1214C, DC/DC/DC, 14DI/10DO/2AI https://support.industry.siemens.com/cs/ec/en/view/107539750

11.3. Change documentation

Version	Date	Modification
V1.0	09/2025	First version