Siemens
Industry
Online
Support

APPLICATION EXAMPLE

PCS 7 Cyber Security Blueprint for Water Plants

PCS 7 / Guideline for Secure Configuration

SIEMENS

Legal information

Use of application examples

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

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

Disclaimer of liability

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

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

Other information

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

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

Security information

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

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

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

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

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

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

Table of contents

1 Introduction

1.1 Preface

As a distinctly open system, SIMATIC PCS 7 can be flexibly adapted to a wide range of customer needs. The system software provides the configuration engineer with a great deal of freedom in terms of project configuration, as well as in the design of the program and visualization.

Experience has shown that subsequent modernization or plant expansion work is made much easier if the project is configured "in conformance with PCS 7" as far as possible right from the start. This means users must adhere to certain basic rules to ensure that the provided system functions will offer optimum usability in the future.

This manual serves as a compendium in addition to the product documentation for SIMATIC PCS 7. The basic steps for project creation and parameter assignment are described in the form of instructions. Please refer also to the SIOS portal (section 17.2)

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

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

This document supports operators of critical infrastructures to fulfill the recommendations mentioned in the BSI ICS Security Compendium ("Best Practice Guide for Operators") and to map the "state of the art" required according to BSIG 8a "Information Technology Security for Critical Infrastructures" as well as related B3S WA (water) catalogs by implementing the concepts presented.

1.2 Abbreviations

Table 1-1: Abbreviations

Abbreviations	Explanation
ADSL	Asymmetric Digital Subscriber Line
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol
EPS	Endpoint Security
GSM	Global System for mobile network
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAD	Industrial Anomaly Detection
IPSec	Internet Protocol Security
IWLAN	Industrial Wireless Local Area Network
PPTP	Point-To-Point Tunneling Protocol
KVM	Keybord Video Mouse
L2TP	Layer Two Tunneling Protocol
NMS	Network Management System
NAS	Network Attached Storage
RADIUS	Remote Access Dial In User Service
RDP	Remote Desktop Protocol
RTC	Real Time Clock
SIEM	Security Information Event Management
SPAN	Switched port analyzer – mirror port)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TPS	Threat Prevention Subscription
TRA	Threat and Risk Analysis
UMC	User Management Component
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WSUS	Windows Server Update Service
WWTP	Waste Water Treatment Plant

2 Security Strategies

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

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

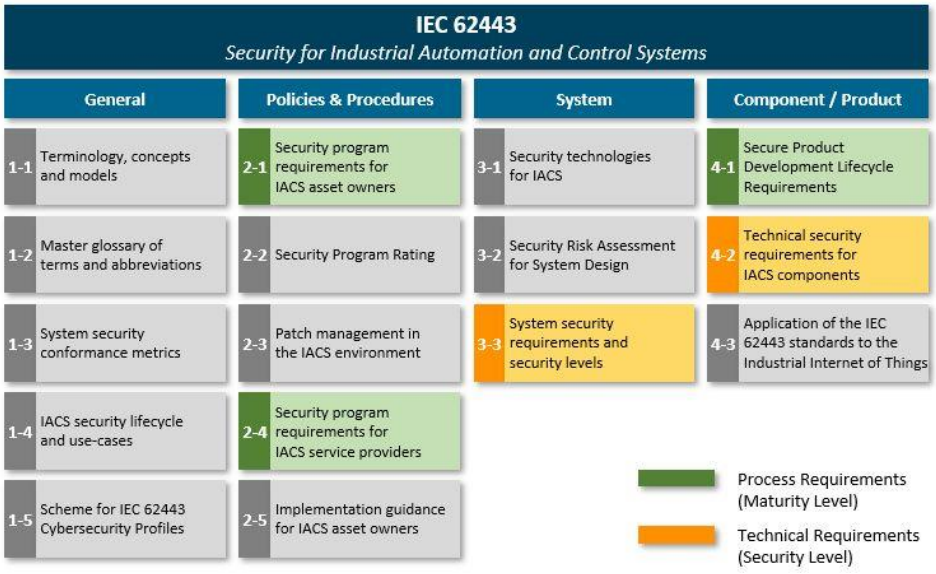
Due to the enormous variety of attacks and the complexity in the process industry, it is often not easy to identify relevant threats and resulting risks and to adapt to the right IT security strategy.

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

2.1 IEC 62443 Overview

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

Figure 2-1: Overview of IEC 62443

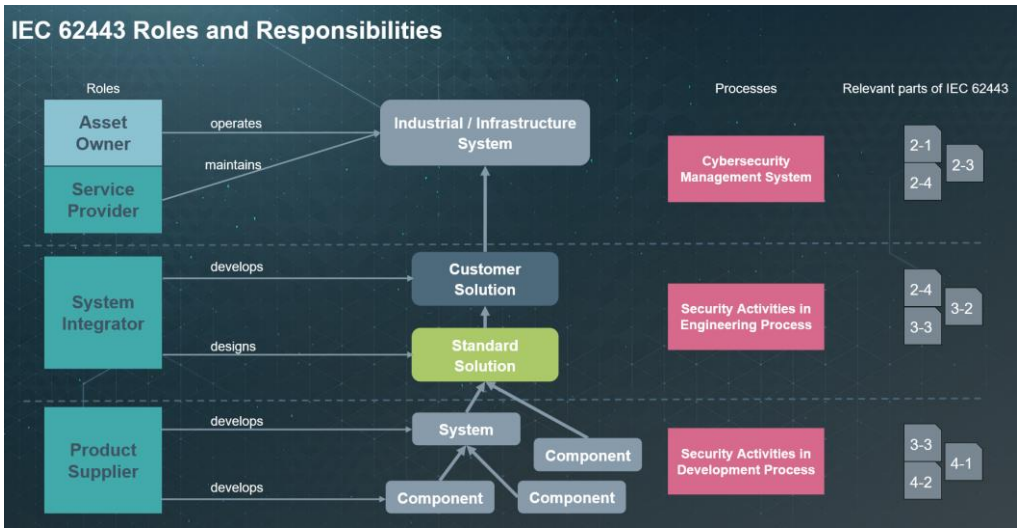


There is clear accountability and a primary objective associated with each of these phases. Security topics must be coordinated and communicated between different roles and stakeholders (Figure 2-2):

- Product suppliers implement security measures, such as authentication, secure communication capabilities, or robust communication stacks in the components, as part of a secure product development process (as per IEC62443 part 4-1)
- System integrators provide a secure design that matches the requirements resulting from exposure, threats, impacts, and the physical and technical operational environment as provided by the plant owner (asset owner). The system integrator manages and applies typical security activities like secure configuration and security verification and validation to ensure correct implementation in the resulting system (as per IEC 62443 part 2-4). System integrators need security information for the components from the product suppliers, e.g., documentation of security capabilities and recommended secure configuration settings.
- Plant owners are responsible for secure operation and maintenance (as per IEC 62443 part 2-1), for example dealing with operational user management, handling of security credentials, and regular security patching.

These roles need to work together to obtain adequate security along the whole lifecycle of a system. Lack of adequate information, or different interpretation of security topics impedes an overall secure approach and finally secure operation as a joint effort of the various stakeholders.

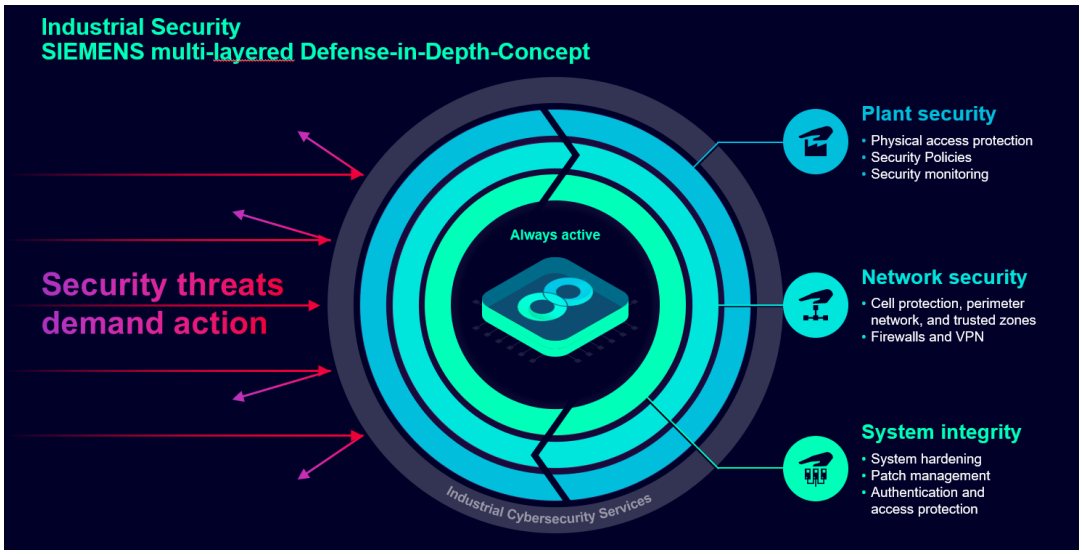
Figure 2-2: Roles according to IEC 62443



2.2 Defense-In-Depth Concept

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

Figure 2-3: Defense-In-Depth Concept



The distributed control system must be defended through multiple layers of security, meaning that plant owners and solution providers must address the complete range of technical, organizational and physical security aspects with appropriate measures.

The following subsections briefly list important aspects for each of the three above mentioned categories of measures (see figure 2-3).

2.2.1 Plant Security

- Physical security measures
  Control of physical access to spaces like the plant area, special buildings, individual rooms or remote locations, cabinets, devices, equipment, cables and wires. The physical security measures must match the identified risk of the defined security zones or cells and the responsible persons. For water processing, this is especially important for physical protection at remote single station systems.
- Organizational security measures
  Secure workflows, security guidelines, security concepts, set of security rules, security checks, risk analyses, assessments and audits, awareness measures and training.

2.2.2 Network Security

- Division into security zones
  A comprehensively secured network architecture subdivides the control network into different security zones.
  Perimeter zone techniques should be employed for this. This means that systems set up in the perimeter network (DMZ – Demilitarized Zone) are shielded by one or more firewalls (front firewall and back firewall or three-homed firewall) from other networks (e.g., Internet, office network). This separation enables access to data in the perimeter network without having to simultaneously allow access to the internal network to be protected (e.g., automation network). As a result, risks of access violations can be significantly reduced.
- Securing access points to the security zone
  A single access point to each security zone (should be Implemented by a firewall) for authentication of users, employed devices and applications, for direction-based access control, for assignment of access authorizations, and for detection of intrusion attempts.
  The single access point functions as the main access point to the network of a security zone and serves as the first point of control of access rights at the network level. I.e., the external pump station or storm water tank as indicated in the blueprint are dedicated security zones.
- Securing the communication between two security zones over an "insecure" network
  Authenticated and secure communication, e.g., based on certificates, should always be used where communication between security zones needs to traverse potentially untrusted networks. Common standardized technologies for this include IPSec (IPSecurity) and OpenSSL (Open Transport Layer Security (TLS) as common VPN tunneling solutions. At individual application level, secure communication utilizes protocols like TLS (Transport Layer Security) to secure HTTPS based Web access, or OPC-UA. Such communication, when originating from external endpoints, terminates in the perimeter network for an additional level of control.

2.2.3 System Integrity

- System hardening
  Recommended secure configuration and system hardening settings to make the overall solution and its individual components more resistant to cybersecurity attacks.
- User/Account management and role-based access control with centralized management capabilities. An example is authorization for plant operators to perform allowed tasks.
  Patch management
  Systematic procedures and workflows for the management of vulnerabilities and security patches, including monitoring, classification, and installing necessary updates on affected components in the plant.
- Malware detection & prevention
  Use of suitable and correctly configured malware scanners, application whitelisting solutions, or security monitoring solutions.

2.3 Blueprints for Solutions

With all these requirements in mind, it is obvious that the burden to find and implement appropriate and secure realizations should not be on the individual project team. Secure design and its deployment in engineering projects should instead be supported as much as possible by prepared secure designs and recommended measures that suit the specific type of automation system in its intended operational environment.

For each topic mentioned in section 2.2, there are plenty of technical solutions, tools, and best practices available. On the one hand, project teams lack the time and should not be required to build up full expertise to develop a suitable solution for each security topic. On the other hand, it is a common pitfall to focus on only selected security aspects in depth, while overlooking others.

To facilitate secure engineering and helping to avoid this pitfall, Siemens has developed several blueprints for automation and control systems that are certified according to IEC 62443 by the German TÜV Süd. These blueprints provide guidance in the form of secure reference designs (secure blueprints), including specific resources to support that the engineering project produces all security documents prescribed by IEC 62443-2-4. Based on a standard control solution using the SIMATIC PCS 7 process control system, the blueprints are designed to meet the requirements of a specific yet typical industry application.

The blueprints described in this **Secure Configuration Guideline** cover water treatment plants, including different plant types for freshwater, wastewater, and desalination. Besides the PCS7 based process control system, additional products that are typical in such plants but whose use is not documented in the default PCS 7 system description, are addressed.

3 Blueprint Water Plant

The following blueprint represents the typical system architecture for a Water plant based on SIMATIC PCS 7.

The blueprint architecture can be used as a basis for the configuration of Water Treatment plants, Wastewater Treatment plants or Desalination plants, since the general facilities, zones and threats considered from a cybersecurity perspective are very similar.

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

Table 3-1: Overview about different Water plant types

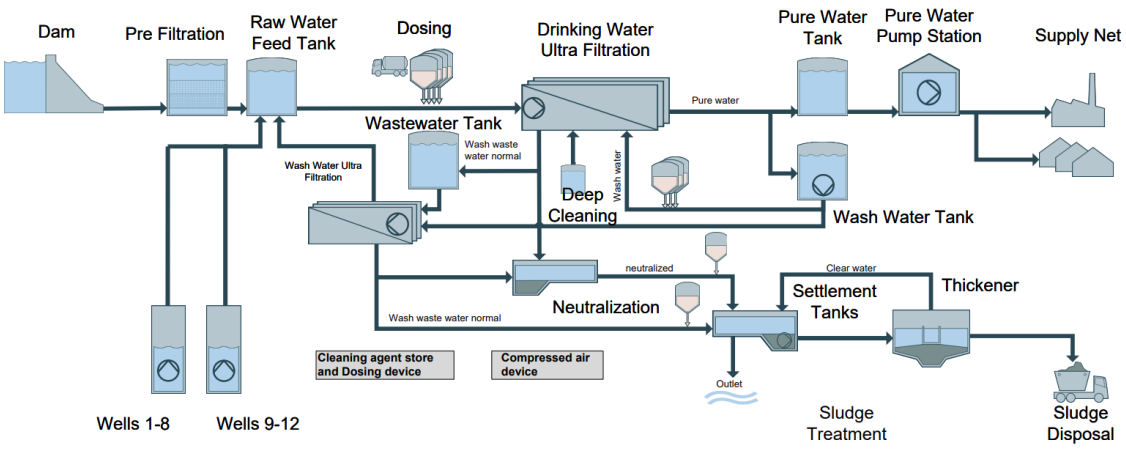
Water Treatment plant	Wastewater Treatment plant	Desalination plant
Raw water feed	Mechanical treatment	Seawater intake/pretreatment
Filtration, wash- pure water	Biological treatment	DAF / DMF / Chemicals
Sludge treatment, Neutralization	Sludge treatment	Reverse osmosis / Post treatment

3.1 Process Descriptions

A Water Treatment plant is typically a locally operated facility to generate fresh water and distribute this to the attached households or industrial consumers. The raw water catchment can be based on e.g., surface water collection or wells. The central water treatment plant cleans and processes the water to the desired quality, and finally feeds into the fresh water supply network.

The central water treatment plant is often fully automated and enclosed. The wells, and facilities of the supply network are remotely operated small stations, for example pump stations using Telecontrol technologies.

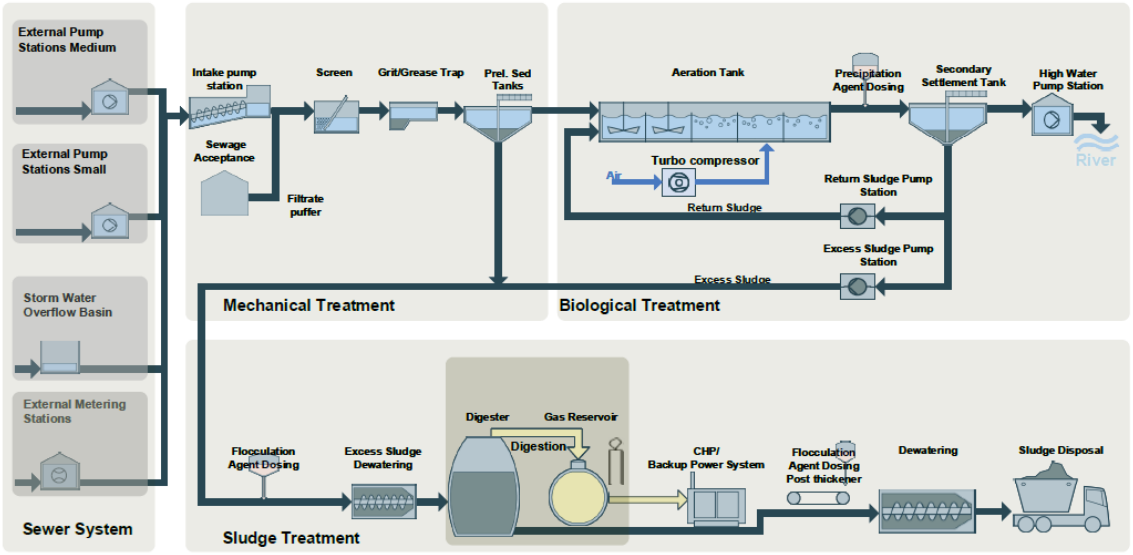
Figure 3-1: Process Overview



A Wastewater Treatment plant treats the polluted water of households and industrial facilities to minimize the impact on the environment. The wastewater arrives from the sewer system carried by external pumps, and undergoes mechanical-, biological- and chemical- or further treatment processes in the central plant. The treated water is transported by means of high-water pumps to rivers or the sea. The sludge produced by the treatment processes is either used locally for energy generation or requires full disposal logistics.

Wastewater treatment plants consists of mechanical treatment, biological treatment, sludge treatment, sewer system and sometimes CHP units.

Figure 3-2: Process Overview



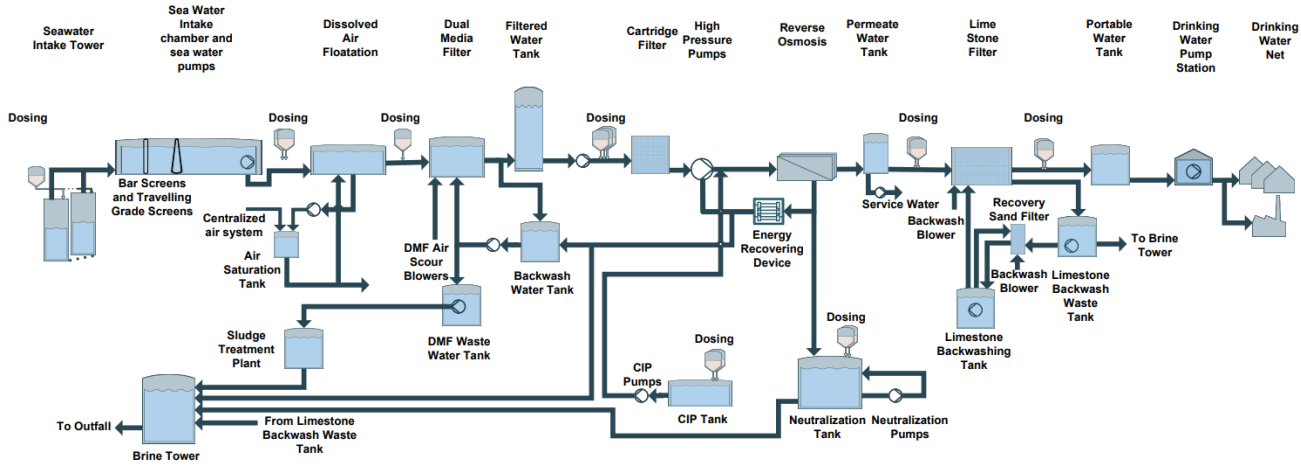
Desalination plants convert salty sea or brackish water into sweet water. Among the various available technologies Reverse Osmosis currently is the most economical and easy to operate technology which can be implemented from very small 25 m^3/d capacity to mega capacity plants as 100 MGD.

Reverse osmosis consumes relatively low energy and consists of a very modular design. In recent years energy consumption has dropped to ~3 kWh/m3, with the development of more efficient energy recovery devices and improved membrane materials.

The typical single-pass SWRO system consists of the following components:

Intake, Pretreatment, High pressure pumps, RO Membrane Banks, Remineralization, pH adjustment, Disinfection.

Figure 3-3: Process Overview



3.2 System Architecture

The following chapters give an overview of the facilities and functions mentioned in this document. These facilities differ between the different water plant types and sizes.

The exposure to threats, security requirements and system redundancy differs due to the location, relevance in the process, exposure to public and needed functions.

3.2.1 Facilities

Central Control Center

The central control center supervises several treatment plants, especially in setups where several prior self-sufficient and distributed plants were transformed to a single operating company. It locates the main control systems which includes the DMZ and Firewall.

Main plant

Location containing the main treatment facilities, automation equipment and supervisory and control solution. The control room for operating and monitoring the process and control system is also often located here.

If there is a central control center, this location may be (temporarily) unmanned and managed remotely.

External Stations

There are external stations in different locations like the Wells, Pump Stations, and Water Tanks and Rain overflow facilities.

External Stations work mostly stand-alone and automatically. They can be connected by a private network, VPN over public internet or a private radio system.

3.2.2 Zones

The cell protection concept divides the plant facilities and remote locations in security zones. This maps the physically existing parts of the automation system in smaller cells with different security requirements. Security gaps of very different kind (physical access, inside jobs, misuse or intrusion...) maybe contained and isolated in the zone where they appear.

1 – Control

The management servers in this zone provide the data exchange to any other internal network, for example energy data for higher level processing.

Also contains the infrastructure servers for the internal network, for example SINEC Network Management, Domain Controller and Time Server.

2 – DMZ

The demilitarized Zone for data exchange between trusted and untrusted networks. Here, the systems need access to internal and external networks and are therefore most exposed to attacks. The firewall restricts the allowed connections to the required minimum.

3 – Plant Operation / Process

Central operation and process zones. The most important and critical systems are located here and therefore this is the most protected zone (physically, organizational and technically).

The process zone contains the field level devices like S7 PLCs, sensors and actuators like drives, valves, instrumentation etc.

4 – Service WLAN

Wireless access is needed for service and maintenance when mobile SCADA clients are used in the plant area. As wireless connection may be exposed to the public, devices in this zone are considered untrusted like the internet.

5 – Internet / IT

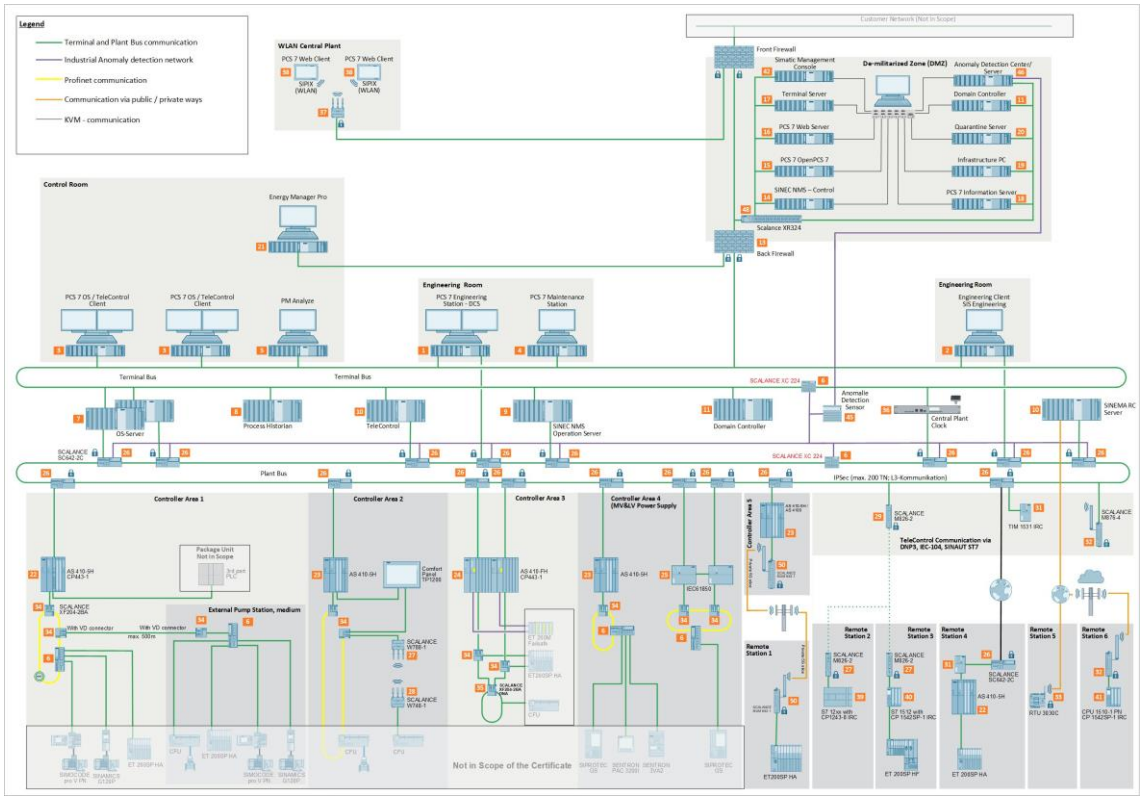
External Zones, not under control of the operator of the automation system.
Lowest security level exposed to the internet and most likely to be attacked. Untrusted, and therefore limited by the firewall (only connections in the DMZ are allowed).

6…10 – Remote Stations

The external stations are widely distributed and connected through mobile radio connections and public or private wide area networks. As the stations are typically in unsupervised and public exposed areas, the security requirements are higher and include physical access protection, tamper monitoring and the capability to work temporarily without network connection to the main plant by using Telecontrol systems.

The SIMATIC PCS 7 system architecture for the Blueprint Water plant is shown in Figure 3-2.

Figure 3-2: SIMATIC PCS 7 system architecture



System Components of the Blueprint Water plant

In alignment with IEC 62443 the system components are classified into three device types:

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

The system components used in the Blueprint for the water industry are listed in the following tables. Section 16 contains a detailed list about the installed application on the host components.

The System Component Identifier (SCI) in the tables is corresponding with the numbers given on the system architecture (e.g., 23).

Hosts

Table 3-2

SCI	Component	Function
1	PCS 7 Engineering Station - DCS	PC station for centralized plant-wide engineering for non-SIS plant parts only Configuration of the hardware Configuration of the communications networks Configuration of continuous and sequential process sequences Operator control and monitoring strategies Compilation and downloading of all configuration data to all target automation system (AS), operator station (OS),
2	PCS 7 Engineering Station - SIS	PC station for centralized plant-wide engineering for SIS plant parts only Configuration of the hardware Configuration of the communications networks Configuration of continuous and sequential process sequences Operator control and monitoring strategies Compilation and downloading of all configuration data to all target automation system (AS), operator station (OS),
3	PCS 7 OS / TeleControl Client	Used in process mode for operator control and monitoring. OS clients access the data of the OS and TeleControl server, visualize this data and allow operators to control the process.
4	PCS 7 Maintenance Station	Manages assets used for production equipment and provides diagnostic messages and maintenance requests for both process control system components and mechanical assets.
5	PM ANALYZE	Add-On to prepare and create special reports to be conformed with ATV regulations
7	PCS 7 OS Server, redundant	Contains all the data of the operating and monitoring systems and the interrupt and measured-value archive. It establishes the communication connection to the automation systems. The OS servers provide the process data to the OS clients.
8	PCS 7 Historian Server, redundant	A central archiving system for storing process data, such as process values and messages.
9	SINEC NMS - Operation	A network management system for monitoring and managing industrial networks. Operation is used displays detailed information about its monitored devices and displays the devices in network topologies.
10	PCS 7 TeleControl-/SINEMA RC Server	Integrate remote monitoring and control of widely distributed units into the SIMATIC PCS 7 process control system
11	Domain Controller (Terminal Bus & DMZ)	Provides Active Directory Service and Time information.
14	PCS 7 Management Console / SINEC NMS Control Server	SIMATIC PCS 7 Management Console enables:

SCI	Component	Function
		Centralized, standardized administration of SIMATIC PCS 7 software Inventory of all installed hardware and software components SINEC NMS - Control: A network management system for monitoring and managing industrial networks. Control is used for monitoring and administration of the entire network.
15	PCS 7 OpenPCS 7 Station	Provides data distributed from different SIMATIC PCS 7 stations (OS server, Process Historian) to higher level data evaluation and management systems.
16	PCS 7 Web Server	Provides the possibility to operate and monitor a plant via Internet / Intranet. All pictures and required scripts are stored on the Web server to enable them to be displayed or run on the Web client.
17	Terminal Server	Server for remote access.
18	PCS 7 Information Server	Takes out the raw data from the historian server and provides visualization and reports
19	Infrastructure PC	Used for Windows Updates, antivirus application.
20	Quarantine Server	Quarantine Server possibility for manual data import/export of production.
21	Energy Manager Pro	Energy data management system to create the basis for economical energy operation management to increase energy efficiency and thus reduce energy costs.
38	SIPIX	The SIPIX handhelds are used for mobile monitoring & controlling the Plant as PCS 7 client.
42	PCS 7 Management Console	The SIMATIC PCS 7 Management Console enables: Centralized, standardized administration of SIMATIC PCS 7 Software Directory of all installed hardware and software components Showing malware-based events Supporting the updating of the SIMATIC PCS 7 software-based components (applications, Microsoft software)
46	Anomaly Detection Center/Server	Processing and display of the network traffic received from the sensors in the IAD Center.

Network Components

Table 3-3

SCI	Component	Function
6	SCALANCE XC Series	Router and switches to connect host systems and embedded devices to the Terminal and Plant Bus
12	Front Firewall (e.g., Palo Alto Firewall NG)	Protects the control system from external zones, like Corporate Lan and allows mainly certificate-based, encrypted and signed access to station in the DMZ
13	Back Firewall (e.g., Palo Alto Firewall NG)	Protects the Terminal Bus production network from the DMZ network and allows mainly certificate-based, encrypted and signed access of individual and trusted remote stations/networks.
26	SCALANCE SC642-2C	Network switch with firewall used to establish secure communication from Plant Bus to AS 410-5H and the remote station connect via GSM
27	SCALANCE M826-2	Router for SHDSL communication on private communication infrastructure. Used for secure communication with remote stations, e.g., Storm Water Tank 1. Possible communication protocols are PROFINET, DNP3, IEC 60870-5-104, SINAUT ST7 via TeleControl
28	SCALANCE W788-1	IWLAN - Access Point for PROFINET wireless communication based on IEEE 802.11a/b/g/n
29	SCALANCE W748-1	IWLAN - Client for PROFINET wireless communication based on IEEE 802.11a/b/g/n
30	SCALANCE M816-1	Router for ADSL2+ communication on public communication infrastructure. Used for secure communication with remote stations, e.g., External Pump station, small. Possible communication protocols are PROFINET, DNP3, IEC 60870-5-104, SINAUT ST7 via TeleControl
31	TIM 1531 IRC	Communication module for WAN remote communication via possible communication protocols are PROFINET, DNP3, IEC 60870-5-104, SINAUT ST7 via TeleControl
32	SCALANCE M876-4	Router for wireless GSM/UMTS/LTE communication on public communication infrastructure. Used for secure communication with remote stations, e.g., External Metering Station or Storm Water Tank 2 Possible communication protocols are DNP3, IEC 60870-5-104, SINAUT ST7 via TeleControl
34	SCALANCE XF204-2BA	PROFINET network switch (managed) with redundancy manager to connect a PROFINET-Ring / Line to AS 410-5H
35	SCALANCE XF204-2BA DNA	PROFINET network switch (managed) with redundancy manager to connect a PROFINET ring / line to AS 410-5H
37	SCALANCE W786-2IA	WLAN Access point support data rates of up to 450 Mbps according to IEEE 802.11n standard
45	Anomaly Detection Sensor	Detect anomalies in the network

Embedded Devices

Table 3-4

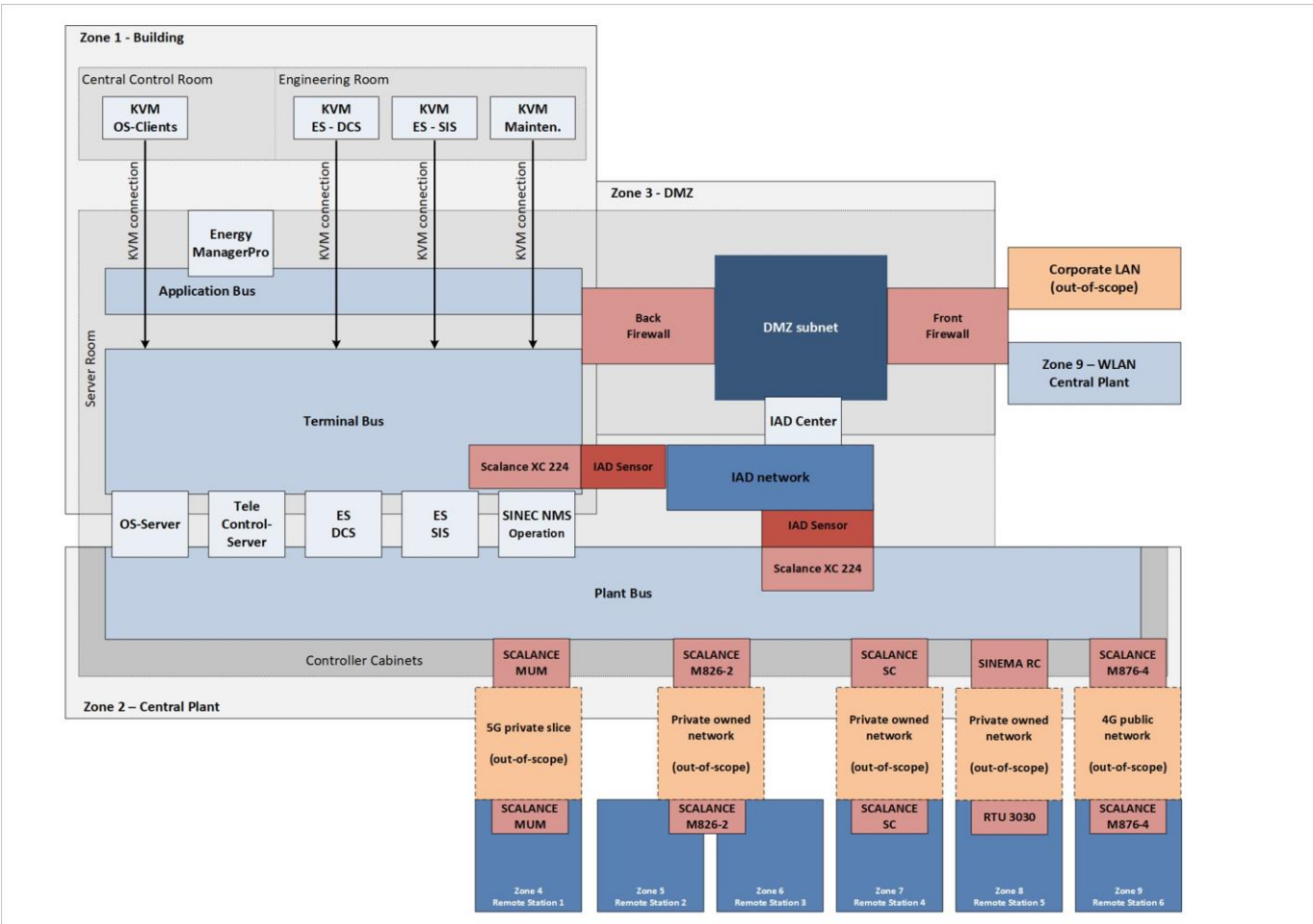
SCI	Component	Function
22	CPU410-5H, non-redundant	CPU with 2 integrated Interfaces, 1 used for Plant Bus communication,1 available for PROFINET or Profibus.
23	CPU410-5H, non-redundant	CPU with 2 integrated Interfaces, 1 used for Plant Bus communication via SCALANCE SC642-2C,1 available for PROFINET or Profibus
24	CPU410-FH, redundant and failsafe	Failsafe CPUs with 2 integrated Interfaces, 2 available for PROFINET or Profibus and
25	Station Gateway	Connect of up to 128 intelligent electrical devices (IED S) to SIMATIC PCS 7 automation systems using IEC 61850 MMS
33	RTU 3030C	Monitor and control small outstations without connection to an energy supply system. In telecontrol networks, the RTU is used to connect the remote stations to the control center via mobile communication.
36	Central Plant Clock (e.g., Bürk Mobatime)	Relevant for components equipped with an internal hardware clock or real time clock (RTC) to keep the process control system with a standard time
39	S7-1200	Monitor and control small outstations. In telecontrol networks, the RTU is used to connect the remote stations to the control center via cables.
40	S7-1512	Monitor and control outstations. In telecontrol networks, the RTU is used to connect the remote stations to the control center via cables
41	S7-1510	Monitor and control outstations. In telecontrol networks, the RTU is used to connect the remote stations to the control center via the mobile communication

3.3 Zones and Intended Operational Environment

The blueprint for Water Plants is structured into zones with similar security trust characteristics. Zones that are not in the blueprint scope but detail the characteristics of the intended operational environment are shown for completeness. The overview of the defined zones matches the detailed blueprint in section 3.2 and is shown in Figure 3-3.

The figure also shows assumed physical locations (server cabinets, controller cabinets, and central control room) and default networks (Terminal bus, Application bus, Perimeter network (DMZ) and Plant bus) of the internal zones.

Figure 3-3: Security Zones Overview



3.3.1 Zone 1 – Building

The building zone is located on the central plant (zone 2) and contains the central control room and the server room. The terminal bus and the application servers are installed only in this building.

Access to this zone is restricted to authorized personnel only.

3.3.2 Central Control Room

The central control room contains the Operator Workstations (OS-Client 1 - 2) The workstations are screens that are connected via KVM extender to the respective HMI Client CPU (physical machine). The workstations in the central control room are not connected to any IP network.

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

3.3.3 Engineering Room

The engineering room contains the Engineering Stations (ES) for DCS and SIS and the Maintenance Station (MS). The Workstations are screens that are connected via KVM extender to the respective ES and MS CPU (physical machine), as shown in the system overview. The workstations in the engineering room are not connected to any IP network.

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

3.3.4 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 rack mounted KVM switches that serve as local console for all the servers (DMZ and Terminal bus) that do not have KVM screens located in the central control room.

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

3.3.5 Terminal Bus

The Terminal bus contains the different servers and clients for the PCS 7 system.

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

3.3.6 Application Bus

The Application bus provides a separate zone to contain additional servers for special applications that are not standard PCS 7 applications. In the blueprint, this includes the Energy Manager Pro station.

3.3.7 Demilitarized Zone (DMZ) / Perimeter Network

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

- SIMATIC Management Console
- SINEC NMS Server – Control
- PCS 7 OpenPCS7
- PCS 7 Web Server
- Terminal Server
- PCS 7 Information Server
- Infrastructure PC
- Quarantine Server
- Domain Controller
- Anomaly Detection Center / Server

The DMZ physically exists only within the server cabinets located in the server room. A rack mounted KVM switch is used to serve as local console for all the servers of the DMZ.

3.3.8 IAD Zone

The IAD (Industrial Anomaly Detection) zone comprises one or more IAD sensors and an IAD center (server). These are connected by a separate LAN that is independent of the other plant networks. The IAD sensor devices are deployed with the regular network devices in the plant zones to be monitored, but only passively connect to SPAN ports for passive monitoring of network traffic. The IAD Center is physically located with the DMZ devices and is connected to the DMZ internal LAN.

3.3.9 Zone 2 – Central Plant

Central Plant is the main facility of the Plant. At the central plant, the building with the central control room and the server are located. The controller cabinets for the different plant areas are installed in locked control rooms at different locations in the Central Plant area. The SIMATIC AS 410 controllers in the controller cabinets are connected to the Plant Bus.

3.3.10 Plant Bus

The Plant Bus connects all Automation Systems (SIMATIC CPU410 controllers) and the remote stations to the Engineering Stations DCS / SIS and the PCS 7 servers (OS-Server and Tele-Control Server). The main process parts are controlled by our own Automation Systems in the respective Controller Area zones and the Power Supply (MV and LV).

There is no direct communication between the Terminal Bus or DMZ to the Plant Bus. The plant location itself is a physically protected environment where no open physical access is possible.

3.3.11 Controller Cabinets

Controller cabinets contain the automation systems (SIMATIC CPU410 controller) which are located at various physical locations inside the central plant area. These are connected to the plant bus.

3.3.12 Remote Stations (general)

The following sections describe different types of remote stations that are located outside the central plant area. These remote stations serve different purposes, depending on their respective functionality as part of outdoor water stations.

In general, remote stations are expected to be unstaffed and are not covered by the physical level of protection that applies to the central plant. It is therefore recommended (and assumed in the context of this blueprint) that all remote stations are equipped with respective physical protection measures, including locked door switches and physical hardening of the components in the remote stations (including locked physical ports like ETH and USB). In addition, depending on the specific deployment risk, the use of monitoring of the physical locks with alarming in case of tampering, and automatic lock of remote station functions in case of alarms, are recommended.

3.3.13 Zone 4 – Remote Station 1: Remote Data Transfer 5G

The remote data transfer is based on a PROFINET IO connection via VXLAN that runs over a private 5G network slice through the 5G router MUM853-1. This links the controller CPU410 with remote I/O-cards (ET 200 SP and ET 200 SP HA).
The 5G private radio network itself is not in scope of this blueprint. It is assumed that 5G private network slicing is used, where the asset owner uses a dedicated reserved network slice provided by a 3rd party provider that ensures state-of-the-art 5G security in the radio network.
In the context of this blueprint, it is assumed that the radio network is fully trusted and ensures that only authorized communication endpoints can participate in the secure 5G communication of the 5G network slice.
It is noted that the VXLAN communication itself is not cryptographically secured and therefore relies on the security provided by the 5G radio network.

3.3.14 Zone 5 – Remote Station 2: Remote data transfer via dedicated line (CPU S7-12XX)

The communication between the central plant and the remote station CPU S7-12XX is established by a privately owned infrastructure.

To ensure secure communication between the remote station and Plant Bus independent of the intermediate network infrastructure, the router SCALANCE M826-2 is used at both endpoints.

3.3.15 Zone 6 – Remote Station 3: Remote data transfer via dedicated line (CPU S7-15XX)

The communication between the central plant and the remote station CPU S7-15XX is established by a privately owned infrastructure.

To ensure secure communication between the remote station and Plant Bus independent of the intermediate network infrastructure, the router SCALANCE M826-2 is used at both endpoints.

3.3.16 Zone 7 – Remote Station 4: Remote data transfer via DSL

The communication between the central plant and the remote station CPU410 incl. TIM (telecontrol protocol & buffering) is established via public networks DSL,

To ensure secure communication between the remote station and Plant Bus, SCALANCE SC firewalls with IPsec VPN tunnels are used.
The intermediate network infrastructure connecting the remote station in this case is not in scope of this blueprint but is assumed to be in the responsibility of the asset owner. It is assumed that the intermediate network is trusted and prevents any unauthorized access to the SCALANCE SC devices.

3.3.17 Zone 8 – Remote Station 5: Remote data transfer via 4G

The communication between the central plant and the remote station RTU 30XX is established either via public networks with 4G radio, or via intermediate fixed line network infrastructure owned by the asset owner. In the latter case, the security assumptions for the remote station 4 setup apply.

To ensure secure communication between the remote station and Plant Bus, the switch SCALANCE M876-4 is used in the 4G radio case. An intermediate fixed line network infrastructure is not in scope of the blueprint, see also the remote station 4 case.

In all cases, the communication between the plant bus and the remote stations is protected by secure VPN tunnels between the SINEMA RC server and the RTU devices.

3.3.18 Zone 9 – Remote Station 6: Remote data transfer via 4G

The communication between the central plant and the remote station CPU S7 15XX incl. CP 1542 is established via public networks with 4G radio.

To ensure secure communication between the remote station and Plant Bus, the switch SCALANCE M876-4 is used at both endpoints.

3.3.19 Zone 10 - WLAN Access

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

The Wireless Access Points are located where required throughout the site and provide wireless access for tablet PCs. The tablet PCs are Siemens SIPIX clients and were used for the monitoring and controlling of the plant.

Connection to the Wireless Access Points will be encrypted and require wireless clients to have knowledge of the specific wireless “key”. The user authentication for the SIMATIC PCS 7 applications is realized with SIMATIC Logon.

3.3.20 External Zones

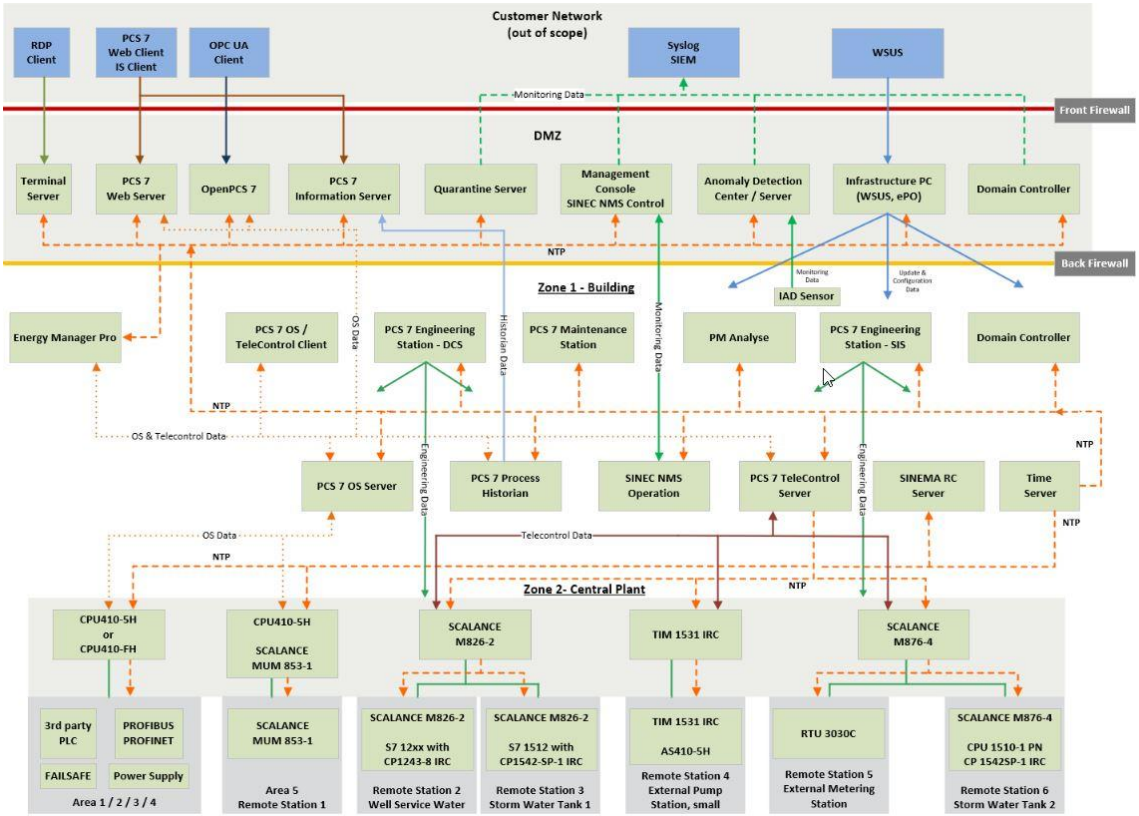
This Blueprint has only one external zone: The Corporate LAN.

This zone conventionally provides update services to the applications running in the DMZ. The associated network connections for these services are, by convention, initiated (sourced) from the DMZ to the appropriate provider (destination) in the company network. A few, limited services are initiated from the company network to the DMZ.

3.4 Data Exchange between Zones

The overview of the connections and data traffic between the previously defined zones and the applications provides the following Figure 3-4.

Figure 3-4: Overview of Data Exchange



The figure depicts selected data flows for different types of communication within and between zones. Different types are grouped by different colors:

- Telecontrol data is shown by brown arrows.
- SIMATIC PCS 7 process control data is shown by light orange dotted arrows.
- Monitoring and Engineering data is shown by light and dark green arrows.
- Microsoft Update and ePO communication is shown by blue arrows.

4 Protection goals

Protection goals for a solution in terms of confidentially, integrity and availability can differ from plant to plant. Due to this, an individual threat and risk analysis (TRA) must be conducted for each plant and automation control system solution. The blueprint described in this document is verified by detailed technical threat and risk analysis efforts for each of the three plant types of water treatment, wastewater treatment, and desalination.

The following data and functionalities have been identified as most relevant with respect to confidentiality, integrity and availability.

Table 4-1: Protection Goals

Protection Goals	Description of the Protection Goals	Associated Main Components / Assets
Confidentiality	User Passwords Process data Customer assets, e.g., employee data Internal process data become public, e.g., measurement data of the effectivity of cleaning processes	Domain Controller PCS 7 OS-Server, CPU410 5H-Controller
Integrity	Historian data Measurement data Integrity of the water treatment process (e.g., use of correct chemical dosing) Project Configuration & Engineering data Integrity of Gas process (Methane)	PCS 7 Process Historian / PM Analyze PCS 7 OS-Server, PCS Engineering Stations DCS / SIS PCS 7 Engineering Stations DCS / SIS, CPU410 5H-Controller SINEC NMS, PCS 7 Engineering Stations DCS /SIS CPU410 5FH-Controller, PCS7 Engineering Station SIS
Availability	Wastewater Treatment Plant availability Measurement data for report generation	CPU410 5H-Controller, OS Server

Note: The protection goals shown above apply to all three types of Water Plants, except where the specific plant type is indicated in brackets.

The above protection goals should be used as input to solution projects based on the blueprint.

- to assess the impact on the plant in the event of potential violations of the protection goals in terms of confidentiality, integrity and availability
- for project specific threat and risk analysis.

5 Security measures

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

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

5.1 Secure Network Design

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

5.1.1 Network Segmentation

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

For the Blueprint, segmentation is enforced between the central plant zone and the building zone. Segmentation is implemented through the dual-homed terminal bus PCs as these are also connected to the plant bus network.

The central plant zone, including the plant bus network, spans over the whole plant area with a lower level of physical protection compared to the building zone. It connects the subordinate subsystem zones (Zone 4 to zone 8 in Figure 3-3) with the SIMATIC PCS 7 system (TeleControl server) in the central plant zone, where communication between these zones is implemented through encrypted VPNs.

Subsystems in the physically protected remote locations outside the area itself are their own zones connected by encrypted VPNs to the central telecontrol server. This is to ensure an appropriate level of protection of the communication through the plant bus network.

All communication between external zones and the Water Plant like an operator's office network or remote access, must pass through the DMZ. This is also implemented as a separate zone located within the building zone.

The overview of the zones for the blueprint are shown in section 3.3.

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

- \1\ – Security concept PCS 7 & WinCC (Basic), section 6.2 and 6.3
- \2\ – PCS 7 Compendium Part F - Industrial Security, section 5.3.

5.1.2 Zone Boundary Protection

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

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

Communication across the plant bus network between the TeleControl Server and the remote stations is secured by SCALANCE SC network devices. These also implement strict firewall rules to reduce the attack surface for the plant bus network and allows it to configure encrypted communication via VPN to the connected remote locations.

Besides the network-based firewalls, also the PC-based host firewalls are capable to provide an additional layer of protection. The configuration of the host firewall is done during the SIMATIC PCS 7 installation / setup (by Security Controller application)

Recommended configurations (rule sets) for the front and back firewalls as well as for the SCALANCE SC network devices connecting the remote stations for the Water Plant Blueprint are described in the sections 6.3, 6.4 and 0.

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

5.1.3 Network Access Protection

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

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

Users, software processes or devices accessing via wireless communication must be identified and authenticated. A commonly accepted security practice is to use the WPA2 or WPA3 security profile with strong authentication and 802.11i based encryption of the wireless communication. This is to authenticate and authorize access as well as monitor and enforce usage restrictions for wireless connections.

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

The hardening measures and the configuration of the wireless devices of the blueprint are described in section 6.4.

5.1.4 Administration of Network Devices

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

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

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

Furthermore, user management and access control for administrative access is integrated with Active Directory based centralized account management through the SINEC NMS network management system that also allows central administration and updating the firmware of all managed SCALANCE network devices, see section 6.10.3.

5.1.5 Protection Measures Against Denial-of-Service

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

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

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

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

- The Palo Alto Front- and Back Firewalls NG provide a general protection against common network level DoS attacks. The hardening measures and the configuration of the Palo Alto Firewalls NG are described in section 6.3.1.
- As part of the overall approach to industrial security in SIMATIC PCS 7 systems, many industrial network devices are certified to meet robustness criteria with the Achilles certification. This includes especially the CPU410-5H devices. For the used network components Siemens internal tests take place to check the robustness criteria.

The complete list of certified SIEMENS devices is given in:

\3\ – SIEMENS Devices with Achilles certificate

5.2 Identity and Access Management

Human user identification and authentication is provided and enforced on all interfaces which provide human user access. The human user interfaces include:

- Operator accounts for applications with user interfaces (e.g., OS client, web interfaces, engineering system)
- Operating system accounts
- Accounts for administrative access to network devices
- Access to web interfaces of embedded devices

Centralization of account management across the Blueprint is supported using Microsoft Active Directory (Windows Domain) where personalized accounts for the Windows based machines, operators and engineers are covered. Network devices and embedded devices with RADIUS support can also be integrated into the centralized account management.

The user management and the authentication of the blueprint is described in section 7.

5.2.1 Authentication Mechanisms for Users and Components

For application-level access (e.g., PCS 7 Graphical Runtime), user authentication is handled by SIMATIC Logon which gets all Windows domain group memberships of this user account managed by the Active Directory. The Windows domain group membership of the user account is used to determine the rights within the process control applications.

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

Exceptions to personalized (unique) accounts depend on configuration and operational procedures. These typically include accounts for machines that must be permanently operational. In this case the recommendation is to use a machine-based Windows user system account. An example could be an OS client, for operator control and monitoring, see section 7.2.

Secure access to network devices is described in section 5.1.4 and can be integrated with the Active Directory managed groups and users through RADIUS. This covers administrative access to SCALANCE network devices.

For centralizing authenticated user access to SCALANCE network devices SINEC NMS is used. SINEC NMS supports UMC (User Management Component) feature for user management with the capability to integrate it into the Active Directory service. For SINEC NMS see section 6.10.3.

SIMATIC PCS 7-specific software processes on the different components communicating with each other typically run as machine-based accounts (non-interactive) that are integrated into the Active Directory. This way, it is ensured that software processes are identified and authenticated, see section 7.2.

Critical communication between devices and processes can also be protected by using secure channels. Examples include IPsec-, OpenVPN- or TLS-based communication between network devices or PC based systems, e.g., with remote stations. Furthermore, it is possible to use an application integrated encrypted communication possibility, e.g., configured via SIMATIC Shell.

5.2.2 Management of Identifiers and Credentials

The Blueprint supports the management of identifiers (e.g., username, host name) and passwords for the Windows domain accounts through the Active Directory. This includes mechanisms for password recovery and reset mechanisms.

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

Management of further security credentials, e.g., for setting up secure communication, is described in detail in the respective product security manuals of SIMATIC PCS 7, and is supported by several tools and management consoles, including SIMATIC Shell or SINEC NMS for the SCALANCE network devices.

5.2.3 Account Management and Configuration of Access Rights and Privileges

The account management handling (users & groups) will be done inside the Active Directory.

5.2.4 Control of Access via Untrusted Networks (Remote Access)

As the Blueprint solution is protected by firewalls and a de-militarized zone, no direct access is possible for users connecting to the plant from external networks that are considered untrusted by default. Access is just possible to machines in the DMZ that are specifically configured and secured to allow access at application level. Remote users therefore require user accounts with specific privileges and all such accounts are also controlled by Active Directory. The recommended tools for Remote Access are the SIEMENS Remote Service Platform (cRSP) or SINEMA Remote Connect (SINEMA RC). For both tools the Terminal Server (Jump Host) will be the secured entry point to the plant.

cRSP

Optimal proactive, secure and system-specific support for the automation system from remote locations: This is the idea behind the SIMATIC Remote Services (SRS) platform. Thanks to its modular design, SIMATIC Remote Services can be optimally adapted to actual requirements. The available modules not only provide the remote infrastructure but also include support and maintenance.

Since the SIMATIC Remote Services are based on the common Remote Services Platform (cRSP) from Siemens, plant operators work on a secure, high-performance, and high availability platform for remote access to their SIMATIC automation systems. The cRSP functionalities are certified under ISO 27001.

SINEMA RC

With SINEMA Remote Connect installed in the DMZ, remote access can be realized. In combination with a Terminal Server solution, it is possible to get a high secure remote access setup, enabling the access to the engineering station or the PCS 7 webserver. In the remote access use case, the user will login to SINEMA RC server and establish a secure VPN connection to pass the unsecure networks, like the internet. This connection can then be used to establish a RDP connection to the Terminal Server station. Furthermore, the user establishes a connection from the Terminal Server to the PCS 7 webserver in the DMZ or through the back-firewall to the engineering station, which must be scanned for malware and unauthorized file transmissions. Finally, the combination of SINEMA RC, Terminal Server and the back-firewall results in a high security and state-of-the-art remote access solution.

5.3 Attack Surface Reduction

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

Least Functionality

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

- Disable all unnecessary interfaces and applications using them, and
- Protect those interfaces with secure configuration that are either necessary or cannot be disabled.

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

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

All the above is applied to different levels of components:

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

Recommended hardening measures for the Blueprint to reduce the attack surface of the above-described areas, are listed in chapter 6.7.

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

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

Further information regarding least functionality for PCS 7 systems is provided by:

- \1\ – Security concept PCS 7 & WinCC (Basic), section 7.3
- \2\ – PCS 7 Compendium Part F - Industrial Security, section 6

5.4 Secure Channels and Encryption

Encrypted communication 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 analyzed for typical Blueprint, balancing threats and costs.

The data considered sensitive are identified by the protection goals in section 4. For such data both access restrictions and 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 context:

- Secure communication for all traffic to and from the plant, i.e., between the servers in the DMZ and external communication end points.
- By default, critical communication across the plant bus receives additional protection through VPNs (e.g., between OS Server and CPU410-5H controller, or telecontrol server and network devices connecting power supply, or remote stations), see section 6.3.2 and 0.
- Dedicated VPN protected communication channels between the main plant and all remote stations, to achieve independence from the security capabilities of utilized communication infrastructure (e.g., WWAN or WLAN radio)

The unauthorized access to CPU410-5H controller can be prevented by protection level, e.g., level 2 against unauthorized writing or level 3 against unauthorized reading. The latter provides cryptographic protection with encryption. The protection level can also be set by an external key switch, see section 6.11.

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 media, other mobile devices, or through users browsing infected Web pages or opening infected email-attachments.

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

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

5.5.1 Software and Information Integrity

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

Virus scanner software

Virus Scanner software detects, blocks and removes malware (if necessary and configured).
For the actual operational environment of the Blueprint Water based on SIMATIC PCS 7, specific configuration recommendations apply, see section 8. These are important to ensure that the use of virus scanning software on the computers of an automation plant do not interfere with the process mode of a plant. Examples include:

Configuration is aligned with availability requirements and e.g., generates alarms but does not proactively disable or shut down parts of the system functionality that may result in loss of control of the production system (e.g., for an OS server).

Configuration is adjusted to minimize potential impact on performance on the critical software applications during runtime.

Whitelisting technologies

Whitelisting either complements or is used as an alternative to virus scanning solutions. Basically, installed PC-based software components of the system that typically run in a stable known state will be "freezed". Software processes and services that are part of a managed whitelist and are classified as trustworthy are allowed to run, all others (like malware added into the whitelisted component, unapproved scripts, applications and tools) will be blocked from execution.

On the stations and servers of the Blueprint virus scanner software is installed with the capability to keep the virus patterns up to date using an infrastructure server for exchange of virus pattern files in the DMZ, e.g., WSUS. Whitelisting is installed on the stations and servers of the Blueprint. Section 8 describes these protection measures in detail.

It is important to note that typical malware exploits vulnerabilities in the installed software components and services, and both virus scanner and whitelisting solutions must be complemented by an up-to-date security patch level. The patch management procedures for the Blueprint are described in section 10.

5.5.2 Security Functionality Verification

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

5.5.3 Input Validation and Output and Error Message Sanitization

The SIMATIC PCS 7 Blueprint Water Plant is based on components developed and tested in the SIMATIC PCS 7 context. SIMATIC PCS 7 ensures aspects like input validation and controlled output through an overall secure development process. The secure development process is certified according to the IEC 62443 framework for security in industrial control systems (part 4-1, secure development).

5.5.4 Support for Control System Backup and Recovery

The goal of backup and recovery is, that the asset owner can recover and reconstitute to a known state after a disruption of failure. Further details are in section 13.

5.5.5 Time Distribution and Synchronization

In the Blueprint the central plant clock is connected to the Terminal and the Plant Bus. The domain controller on the Terminal Bus is using the time telegram from the central plant clock and provides the time to all domain members (e.g., OS clients and servers, MES systems, OPC server). The CPU410-5H controllers connected to the Plant Bus get the time signal directly from the central plant clock.

Recommended measures and further details about the time distribution and synchronization provides section 6.9.

5.6 Security Logging and Monitoring

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

In addition to security logging and monitoring, additional industrial anomaly detection or logging (e.g., SIEM) capabilities can be added.

5.6.1 Monitoring Access from Untrusted Zones

As described in section 5.1.2, the Blueprint Water Plant is protected by a DMZ that allows full control of all network communication and remote access from external, potentially untrusted, networks. Security logging and monitoring covers both firewalls realizing the DMZ as well as the PC based systems within the DMZ. Hence, all user or system-level access and all communication sessions at network (TCP/IP) level are covered.

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

5.6.2 Logging of Security-Related Events

For the protected zones of the Blueprint Water Plants including building and central plant zones, for both PC-based SIMATIC PCS 7 systems and SCALANCE network devices security logging is performed. The PC-based systems maintain security logs for both application levels (e.g., SIMATIC Logon) and operating system level events. Security logs can be exported through standardized communication protocols (syslog, SNMP) to central servers. These servers centrally collect security log information from the system components and provide interfaces that can be integrated with asset owner's superior SIEM solutions (Security Information and Event Management). Further information about optional SIEM functionalities is given in section 15.3.

Monitoring of Palo Alto Front & Back Firewall NG is done with Panorama Management Software.

In general, all access to security logs is secured and restricted to authorized users of the automation solution through the system capabilities described in section 5.2. Hence, all access to security log data is also covered by the security and logging capabilities.

5.6.3 Audit Trail

To fulfill the requirements for change management all changes shall be centrally executed either via the SIMATIC PCS 7 ES (concerning automation equipment like CPU) or via SINEC NMS (concerning network components). In this way, audit reports can be generated at any time to prove which human user has done which changes.

Direct local access to CPU or SCALANCE devices should be used only during first time commissioning, no more during operation incl. maintenance phase.

6 Hardening and Configuration of the System Components

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

The recommended hardening measures and configurations described in the following sections are only valid for the Blueprint Water Plants.

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

6.1 Assumptions

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

In evaluation of the possible security risks for the Blueprint Water Plants the following physical security measures are assumed:

- Unauthorized access to the central plant and buildings is prevented by physical measures. Only authorized personnel have access.
- Unauthorized access to the remote stations is prevented by physical measures. Access to the remote stations is monitored, e.g., using door switches. Only authorized personnel have access.
- All cabinets having a locking system with semi-cylinders.
- All cabinets, on the main part of Water Plants as well as on the remote stations, are installed in lockable control or server rooms. Access to control or server rooms are limited to authorized personnel (maintenance) only.
- The Terminal Bus is installed in one building with high physical protection as shown in figure 3.3.
- The Plant Bus is operated in the central plant of the Water Plant with physical access control as shown in figure 3.3.

6.2 General Security Measures

For all components used in the Blueprint Water Plants the following general security measures shall be considered to ensure the secure configuration during the plant operation

- The latest released firmware versions shall be installed. Firmware versions for all Siemens components are available on the Siemens Industry Online Support \4\.
- For all components the latest released patches shall be installed. The patches for Siemens components are available on the Siemens Industry Online Support \4\. Further information regarding patch management is given in section 10.
- For the virus scanner installed on the workstation and server always the latest virus pattern must be installed. Further information is available in the following documents: \34\, \35\, \36\
- The standard user and password on all devices must be changed before the first installation. The same password shall be not used for different users and systems and shall be protected and inaccessible to unauthorized persons.
- Further information is given in section 7.
- For SCALANCE components the hardening measures described in \5\ – Checklist for Setting Up SCALANCE Devices shall be considered and centrally executed by SINEC NMS.

6.3 Firewalls for Secure Communication Between the Zones

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

The plant network boundary is protected using a front- and back firewall, which built the Demilitarized Zone (DMZ) of the Blueprint. The hardening measures and the configuration of the firewalls are described in section 6.3.1.

The communication between the security zones within the automation control system is secured by SCALANCE network security devices. The hardening measures and the configuration of these devices are described in section 6.3.2.

6.3.1 Palo Alto 460 NGFW

The plant network boundary is protected using a Front- and Back-Firewall, which built the Demilitarized Zone (DMZ) of the Blueprint, see Figure 3-3.

Front firewall:

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

Back firewall:

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

The recommended hardening measures and the configuration of the Front – and the Back-Firewall are listed in 6.2.

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

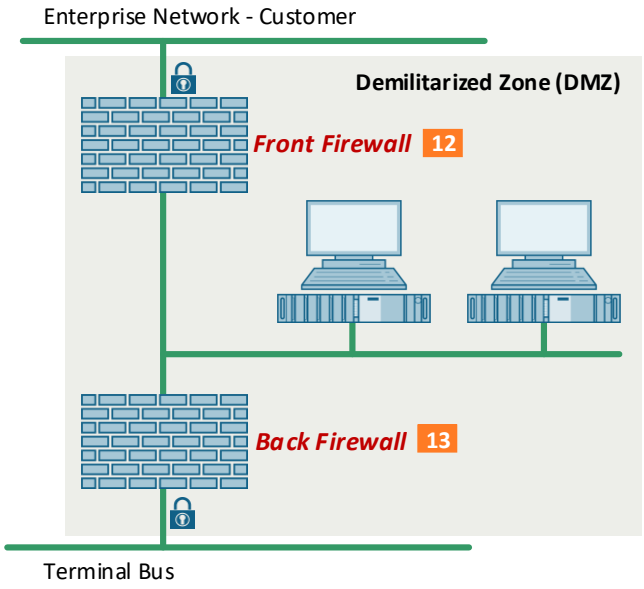


Table 6-1: Front- and Back-Firewall

Function	SCI	Supplier	Type	MLFB
Front-Firewall	12	Palo Alto	460 NGFW	TBD
Back-Firewall	13	Palo Alto	460 NGFW	TBD

For the firewalls listed in Table 6-1 the following general hardening measures must be considered at least:

Table 6-2: Hardening measure for the Firewalls

No.	Security Topic	Hardening Measure	Documents
1	Restrict IP addresses	Restrict the access only to those IP addresses that needed	\38\
2	Restrict services	Do not allow access over the unsecure protocol HTTP or Telnet, require SSH and/or HTTPS	\38\
		Set the encryption min. version to TLSv1.2	\38\
3	Change admin credentials / user management	Change the default username	\38\
		Change the default password	\38\
		Configure an account for each person who needs access and give them only the rights that they need	\38\
		Use multi-factor authentication (RADIUS or SAML)	\38\
		Configure a strict password policy	\38\
4	Dedicated management interface	Use the dedicated management interface in a separate management LAN or VLAN	\38\
5	Security policy rules and profiles	Scan all traffic destinated to the management interface for threats	\38\
		Create a security profile, enable extended packet capture	\38\
		Configure inbound inspection and SSL Forward Proxy	\38\
6	Logging	Set up logging for configuration changes	\38\
		Set up logging for unauthorized login attempts	\38\
7	SNMP	Use SNMP v3	\38\
		Set an SNMP string that is not easy to guess	\38\
		Only enable SNMP on internal interfaces	\38\
8	Certificates	Replace the default certificate with a certificate signed by the organization's enterprise CA	\38\
9	Updates	Keep the PAN-OS and all software packages up to date.	\38\

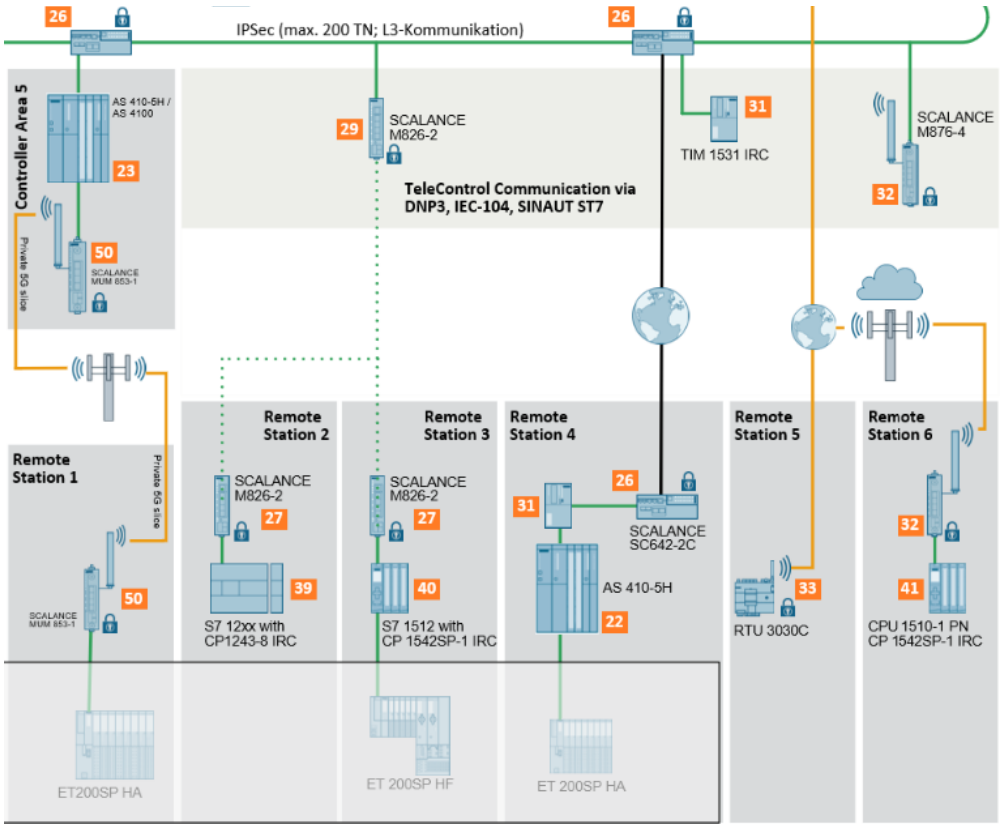
Further information about the configuration of the Palo Alto Next Generation Firewall is provided.

- \6\ – PAN-OS Administrator's Guides (select the Documents acc. Firmware)
- \7\ – Palo Alto Website about PAN-OS

6.3.2 SCALANCE Network Security Devices

In the Blueprint the secure communication on the Plant Bus and to the remote stations is implemented using SCALANCE network security devices as shown in Figure 6-2. The following table are different showcases for interconnection.

Figure 6-2: SCALANCE security network devices



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

Table 6-3: SCALANCE Security Network Devices

Function	SCI	Supplier	Type	MLFB
Secure Communication between Plant Bus and CPU410 5H Controller Station Gateway	26	Siemens	SCALANCE SC642-2C	6GK5642-2GS00-2AC2
Secure Communication between Plant Bus and Remote Station Well Service Water Remote Station Storm Water Tank 1	27 29	Siemens	SCALANCE M826-2	6GK5826-2AB00-2AB2
Secure Communication between Plant Bus and the Remote Stations External Metering Station and Storm Water Tank 2	32	Siemens	SCALANCE M876-4	6GK5876-4AA00-2DA2

For the SCALANCE Security Network Devices listed in Table 6-3 the following general hardening measures must be considered at least:

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

No.	Security Topic	Hardening Measure	Documents
1	Secure Network	Quality of service (COS) priority is set to “DSCP”	\4\ – Section 3.7
		Deactivate Spanning Tree if not required	\4\ – Section 3.8.2
		Deactivate Passive listing	\4\ – Section 3.8.3
2	Identity and Access Management	Use central authentication via RADIUS /UMC /AD. Establish password policy (complexity and change frequency) and deploy changes centrally and regularly via SINEC NMS.	\4\ – Section 3.4 Section 7
3	Reduction of Surface Attack	Disabling of unencrypted and non-required protocols. Details are provided in Table 6-5	\2\ – Section 5.7.3 \4\ – Section 3.3
		Disable of PROFINET interface completely	\4\ – section 3.5
		Restrict the DCP access to “Read-Only”	\4\ – Section 3.6
		Disabling of unused ports	\2\ – Section 5.71 \4\ – Section 3.11
		Disable all non-required services, like DCHP or DNS	
4	Secure Channels and Encryption	No Action required	
5	System Integrity	Use of NTP for time synchronization. If available, the secure NTP variant to be used	\4\ – Section 3.2
6	Logging and Monitoring	Activate Syslog client Please refer also to section 15.3	

The following table shows the settings for the protocols:

Table 6-5: Protocols

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

The secure communication between the zones is established by using IPsec VPN and the internal firewall. Table 6-6 and Table 6-7 show the settings for this.

Table 6-6: IPsec VPN configuration

1	Remote End	Remote Mode: Standard Remote Type: Manual
2	Connection	Keying Protocol: IKEv2
3	Authentication	Use CA-Certificates Don't use PSK
4	Phase 1	Use default Ciphers At least use: Encryption: AES128 GCM 16 Authentication: SHA256 Key derivation: DH group 14 Don't use Aggressive Mode
5	Phase 2	Use default Ciphers and Auto Firewall Rules At least use: Encryption: AES128 GCM 16 Authentication: SHA256 Key derivation: DH group 14

Table 6-7: Firewall settings

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

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

Table 6-8: Additional settings

No.	Type	Settings
1	SCALANCE SC642-2C	Deactivate MRP
2	SCALANCE M826-2	Create an own VLAN for SHDSL and Transfer subnet. The firewall shall be activated to restrict the access
		Use IPsec communication between 2 M826-2 to connect the subnets using SHDSL connection (transfer subnet)
3	SCALANCE M876-4	Mobile wireless configuration Authentication Method: Auto Data Roaming: Disable
		SMS: Disable SMS services, if not needed
		No service should be accessible via usb0 (mobile wireless interface). See firewall configuration Table 6-6

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

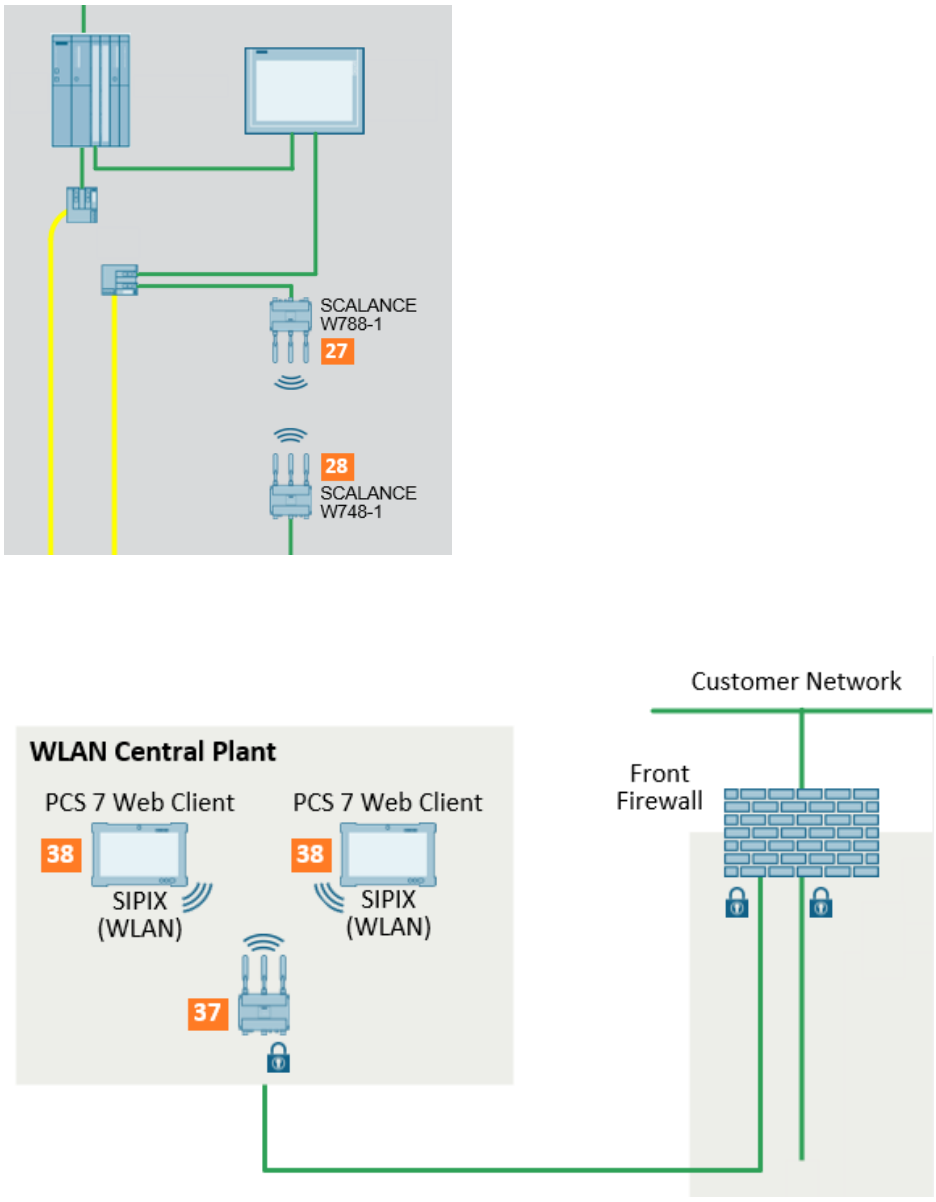
- \5\ – Checklist for Setting Up SCALANCE Devices
- \8\ – SCALANCE SC-600 – Web Based Management (WBM)
- \9\ – SCALANCE SC-600 – Operating Instructions)
- \10\ – SCALANCE M800 Web – Based Management (WBM)
- \12\ – SCALANCE M826 – Operating Instructions
- \13\ – SCALANCE M874, M876 – Operating Instructions

6.4 Network Components for Wireless Communication

Wireless communication by IWLAN is used in the Blueprint to connect I/O field devices like the Compact Field Unit (CFU) with PROFINET to automation controller CPU410-5H. Furthermore, SIPIX handhelds used for mobile configuration and operation are connected by IWLAN to the automation control system.

Figure 6-3.

Figure 6-3: Wireless Communication



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

Table 6-9: SCALANCE Wireless devices

Function	SCI	Supplier	Type	MLFB
IWLAN - Access Point for the PROFINET wireless communication to I/O field devices (please also consider c-plugs and observe national approvals).	28	Siemens	SCALANCE W788-1	6GK5788-1FC00-0AA0
IWLAN - Client for PROFINET wireless communication to I/O field devices	29	Siemens	SCALANCE W748-1	6GK5748-1FC00-0AA0
IWLAN - Access Point for the communication with mobile laptops or tablets used in the central plant	36	Siemens	SCALANCE W786-2AI	6GK5786-2HC00-0AA0

The hardening measures for the SCALANCE wireless devices are listed in

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

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

Table 6-10: Additional Hardening measures SCALANCE W

No.	Security Topic	Hardening Measure	Documents
1	WLAN encryption	Enable AES encryption for iPCF	\4\ – Section 3.9.1
2	WLAN layer 2 tunnel	Set Mac mode to ‘Layer 2 tunnel’. This is only possible if only SCALANCE devices are used.	\4\ – Section 3.9.2
3	WLAN iPCF	Use iPCF if time-critical data, e. g. PROFINET are transferred via the radio link.	\4\ – Section 3.9.3

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

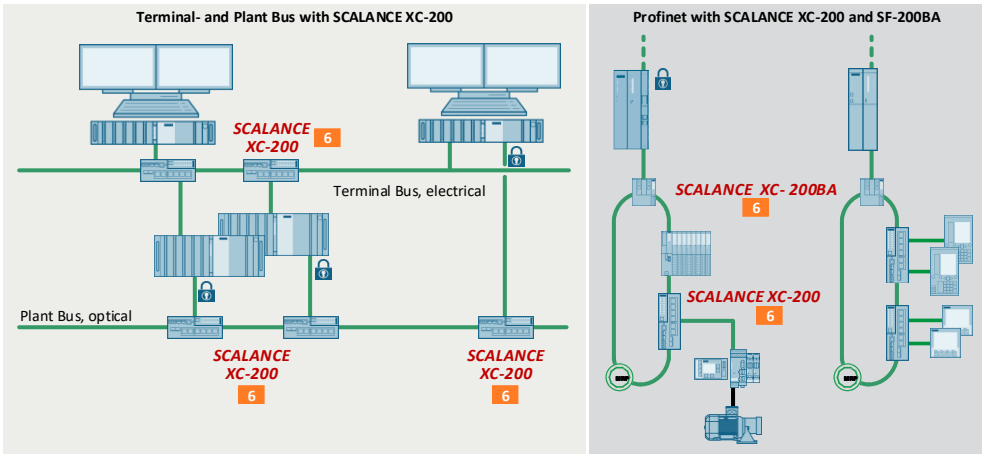
- \5\ – Checklist for Setting Up SCALANCE Devices
- \14\ – SCALANCE W780, W740 Web – Based Management (WBM)
- \15\ – SCALANCE W780, W740 – Operating Instructions

6.5 Network Components SCALANCE XC and XF

The connection of the workstation and server to the respective networks (e.g., DMZ-Subnet or Terminal bus) and the connection of PROFINET devices to PROFINET networks are implemented in the blueprint by the use of the following SCALANCE series:

- SCALANCE XC-200
- SCALANCE XF-200BA

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



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

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

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

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

No.	Security Topic	Hardening Measure	Documents
1	Ring Redundancy	Disable ring redundancy if the device is not operated in a ring	\4\ – Section 3.8.1
2	PROFINET	If the SCALNCE Device is used in a PROFINET Network the PROFINET interface functionality must be enabled.	\4\ – Section 3.5

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

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

6.6 TeleControl TIM 1531 IRC

The TIM 1531 IRC is used to connect remote stations via public or private infrastructures to the SIMATIC PCS 7 TeleControl server. It contains a telegram buffer for continuous recording of data including time stamp if the communication path is faulty or a communication partner is missing.

The following hardening measures are recommended:

Table 6-12: Hardening measures TIM 1531 IRC

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

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

- \19\ – TIM 1531 IRC – Manual

6.7 TeleControl RTU3030C

The compact SIMATIC RTU3030C is used to monitor and control outlying stations that are geographically distributed and not connected to a power supply network. The RTU can store process data and transfer it via mobile wireless to a master station.

To ensure a secure communication between the RTU 3030C in the remote station and the SIMATIC PCS 7 TeleControl server, a SINEMA RC server is installed.

The following hardening measures are recommended:

Table 6-13: Hardening measures RTU3030C

No.	Security Topic	Hardening Measure	Documents
1	VPN	Use of OpenVPN, configure RTU as OpenVPN client	\20\ – Section 1.7 and 4.16.2
2	HTTPS for WAN	HTTPS for WAN enables SMS incoming off	\20\ – Section 4.16.3
3	Web Server access	Use of HTTPS only	\20\ – Section 4.16.3

Further information about the configuration of the RTU3030C provide:

- \20\ – RTU3030C – Operating Instruction

6.8 Secured Industrial Ethernet Connections

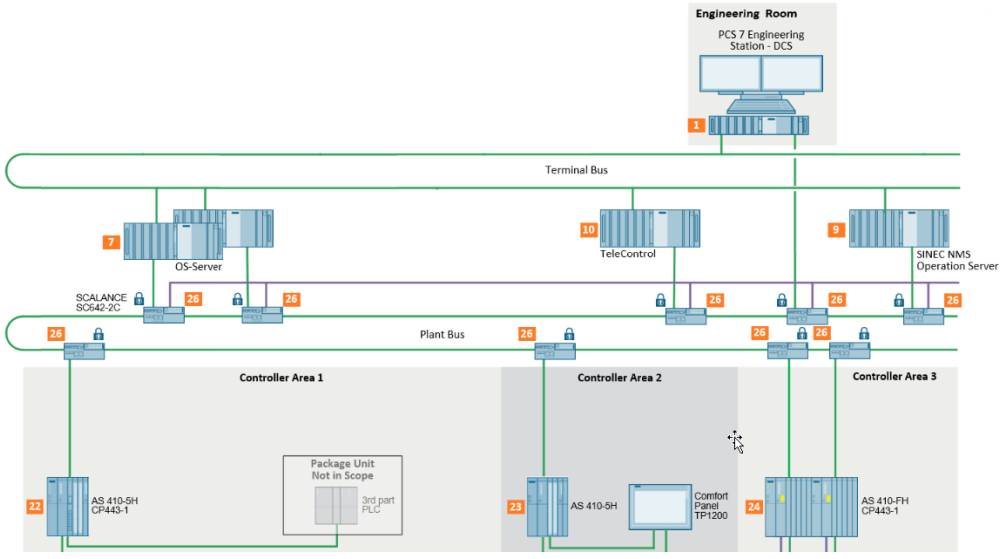
The secure communication between the Engineering Station, Server and the automation system CPU410-5H is established in the blueprint by using SCALANCE SC modules and a SINEMA Remote Connect server. This technology allows a state-of-the-art and scalable solution to provide secured communication on plant bus level.

1	SCALANCE SC632-2C	6GK5632-2GS00-2AC2

The SCALANCE SC modules are installed in front of the following workstations, server and automation systems:

- PCS 7 Engineering Station – DCS
- PCS 7 Engineering Station – SIS
- PCS 7 OS Server
- PCS 7 TeleControl Server
- SINEC NMS Server - Operations
- CPU410-5H, non-redundant
- CPU410-FH, redundant

Figure 6-5: Use of SCALANCE SC642-2C



Monitoring and administration of the SCALANCE SC is implemented with SINEC NMS, see section 6.3.2

6.9 Central Plant Clock

The central plant clock manages the time centrally for the entire plant and synchronizes all the other plant components via their interfaces. The central plant clock is connected to the Terminal and the Plant Bus.

The Domain Controller receives the time signal from the central plant clock via Terminal Bus connection and transfers the time to the servers and the ES systems connected on the Terminal Bus and the DMZ subnet. The OS Server transfers the time signal to connected OS-Clients and, if necessary (in case of central clock failure), sends the SIMATIC time protocol to the plant bus.

The automation systems CPU410-5H receive the time signal directly from central plant clock.

Further information regarding the configuration of the time synchronization for SIMATIC PCS 7 systems is provided by:

- \24\ – PCS 7 Time Synchronization
- \25\ – DTS 4138.timeserver – Mounting and Instruction Manual

6.10 Workstations and Server

In the Blueprint Water Plant for all Workstations and Server the Siemens Industrial Workstations (IPC) for SIMATIC PCS 7 are used. On these IPCs the necessary operating system and SIMATIC PCS 7 software is pre-installed.

In case that other PCs are used a manual installation must be performed, comply with the requirements and procedures described in the following documents:

- \26\ – PCS 7 Readme
- \27\ – SIMATIC Process Control System PCS 7 PC Configuration

The hardening measures described in the following sections are valid for Siemens Industrial Workstations (IPC) for SIMATIC PCS 7.

6.10.1 General Hardening Measures for SIMATIC PCS 7 Workstation and Server

The following general hardening measures for the PCS 7 workstations and servers must be considered:

Table 6-14: General Hardening measures for PCS 7 workstations & Server

No.	Security Topic	Hardening Measure	Documents
1	Secure Network	Use of the Windows firewall	\2\ – Section 6.4
2	Identity and Access Management	BIOS settings	\2\ – Section 6.5
		User administration with Active Directory and SIMATIC Logon	Detailed description provides section 7
3	Reduction of Surface Attack	Remove unnecessary Windows components	\2\ – Section 6.2.1
		Disable Windows services	\2\ – Section 6.2.2
		Disable Automation License Manager (ALM) server functionality if the plant is in operation	\2\ – Section 6.2.4.1
		Enable SMB signing	\2\ – Section 6.2.4.2
		Disable SMBv1	\2\ – Section 6.2.4.4
		Blocking of USB storage media Lock or disabling with other mechanical means Restricting access with Windows group policy	\2\ – Section 6.6
		USB-Ports - Disable Autorun and Autoplay	\2\ – Section 6.6.3
4	Secure Channels and Encryption	Enable encrypted communication in the SIMATIC Shell	\24\ – Section 5.7.11
5	System Integrity	Use of Whitelisting	Detailed description provides section 8
		Use of a virus scanner	Detailed description provides section 8
		Digital signatures for applications	\2\ – Section 6.13
		Patching of operating system	Detailed description provides in section 10
		Backup of engineering and system data	Detailed description provides section 13
6	Logging and Monitoring	Use of SIMATIC Logon	\2\ – Section 7.6.3, 7.6.4

Some of the abovementioned hardening measures can be set by Group Policy Objects (GPOs) of Windows. In the Blueprint the GPOs are configured centrally in the Active Directory (Windows domain) on the Domain Controllers, see section 7.

SIMATIC PCS 7 and WinCC provide with the *Security Controller* an integrated program that makes SIMATIC PCS 7 system application-specific security settings on the systems. Settings are made in the following areas by the Security Controller:

- Windows Defender Firewall
- DCOM
- Registry
- User groups
- File system rights

The firewall rules by the *Security Controller* must be adjusted afterwards where necessary, e.g., for the communication between various subnets.

Further information about the *Security Controller* program is provided by

- \2\ – PCS 7 Compendium Part F - Industrial Security, section 6.3

It is recommended that projects and libraries on the engineering stations be protected from unwanted access and that all accesses be logged, further information is provided in

- \2\ – PCS 7 Compendium Part F - Industrial Security, section 7.6.2 – 7.6.4

In the following sections, additional security and hardening measures for individual applications are described.

6.10.2 Additional Hardening Measures

For some of the SIMATIC PCS 7 workstations and servers additional hardening measures are recommended.

Secure communication on the pant bus

The secure communication on the Plant Bus is implemented on the respective workstations and servers by using the onboard interface or the use of the communication processor CP1623 for redundant operation, each with a dedicated SCALANCE SC642 module in front of the Plant Bus.

This hardening measure is relevant for:

- PCS 7 Engineering Station DCS and SIS
- PCS 7 OS Server
- PCS 7 TeleControl Server

OPC (UA) server function

When the OPC (UA) server function is enabled on SIMATIC PCS 7 systems only authorized systems should be allowed to access this function. This can be implemented by

Implementing corresponding local firewall rules on the respective workstations and servers

Limitation of OPC UA communication between client and server only to TLS, most actual cyphers and digitally signed.

These hardening measures are relevant for:

- PCS 7 OS Server
- PCS 7 TeleControl Server
- PCS 7 OpenPCS 7 Server

Hardening of the Internet Information Server (IIS)

This hardening measure is relevant for:

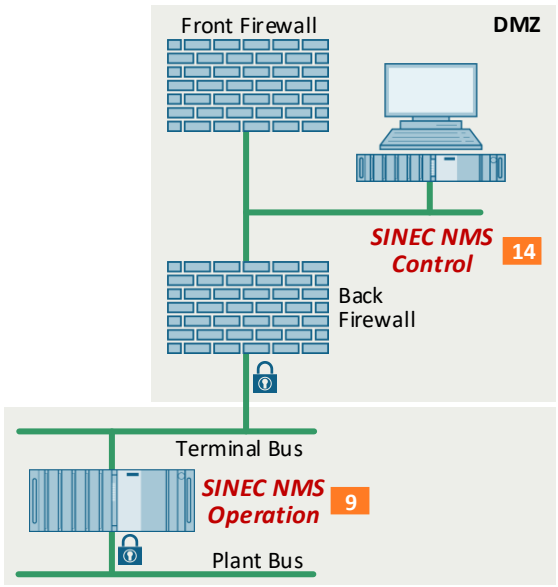
- PCS 7 Information Server
- PCS 7 Web Server

Detail descriptions provides \2\ – PCS 7 Compendium Part F - Industrial Security, section 6.15 and 6.16

6.10.3 Hardening Measures for SINEC NMS

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

Figure 6-6: Overview of SINEC NMS



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

The user management of SINEC NMS is implemented by use of the User Management Component (UMC). For SIMATIC PCS 7 the UMC server of SINEC NMS shall be installed. The local user can be created and integrated into Active Directory.

In addition to the hardening measures mentioned in section 6.10.1 it is recommended to install the SNMPv3 protocol component delivered together with SINEC NMS.

The secured communication with the Plant Bus is implemented with an internal network card together with an SCALANCE SC642.

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

Further information on SINEC NMS provides:

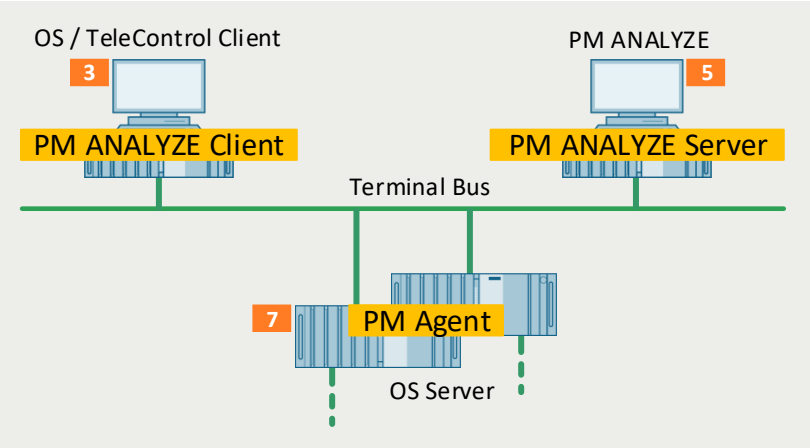
- \28\ – Network management SINEC NMS

6.10.4 Hardening Measures for PM ANALYZE

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

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

Figure 6-7: Overview of PM Analyze



For PM Analyze Server the same hardening measures mentioned in section 6.10.1 are recommended.

The use of whitelisting for the PM Analyze Server is not recommended, because it can influence the functionality of PM Analyze.

6.10.5 Hardening Measures for SIMATIC Energy Manager Pro

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

The acquisition component of Energy Manager Pro is communicating via OPU UA (HA) with the OpenPCS 7 station in the DMZ.

In addition to the hardening measures listed in section 6.10.1 the following measure must be considered:

- SIMATIC Energy Manager Pro uses the Microsoft Internet Information Service (IIS). Recommended settings are provided in \42\ – SIMATIC Energy Manager PRO V7.2 - Installation, Appendix A.2

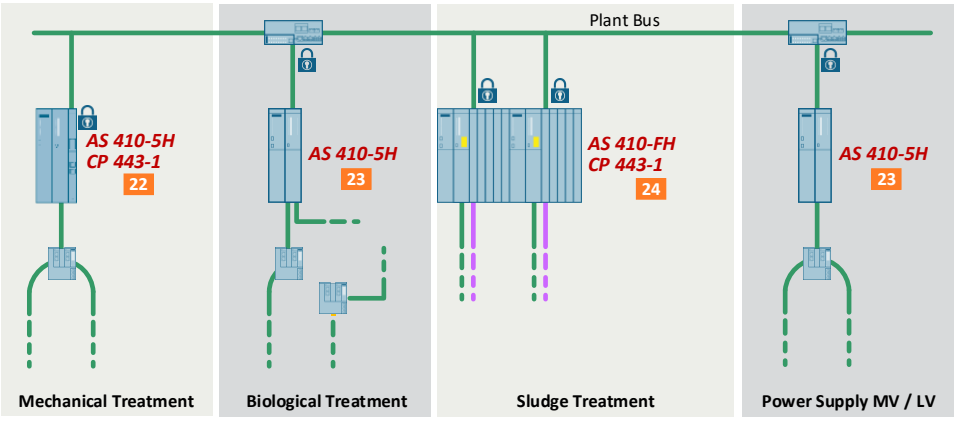
Further information about the SIMATIC Energy Manager Pro provide:

- \30\ – SIMATIC Energy Manager PRO V7.1 – Operation
- \31\ – SIMATIC Energy Manager PRO V7.1 – Acquisitions

6.11 Automation System SIMATIC CPU410-5H

In the Blueprint the Automation System SIMATIC CPU410-5H is used to control the main part of the Water Plant.

Figure 6-8: Automation System CPU410-5H / -FH



The following configurations of the Automation System CPU410 are used in the Blueprint:

Table 6-15: Overview of CPU 410-5H

22	Automation System, Non-redundant	Siemens	CPU410-5H, CPU with 2 integrated Interfaces With CP 443-1 for Plant Bus communication	6ES7654-6Cx03-3FF0
23	Automation System, Non-Redundant	Siemens	CPU410-5H, CPU with 2 integrated Interfaces	6ES7654-6Cx00-3FF0
24	Automation System, Failsafe, redundant	Siemens	CPU410-FH, Failsafe CPU with 2 integrated Interfaces With CP 443-1 for Plant Bus communication	6ES7656-6Cx33-1FF0

The secure communication between the Automation System and the Plant Bus is implemented in two different ways:

- CP 443-1 with SCALANCE SC642-2C
  For hardening measures and configuration see SC 642-2C.
- Onboard Interface with SCALANCE SC 642-2C
  For hardening measures and configuration see SC 642-2C section 6.3.2.

For the automation system SIMATIC CPU 410-5H following hardening measures are recommended:

Table 6-16: Hardening measures CPU 410-5H

No.	Security Topic	Hardening Measure	Documents
1	Protection level	Set at least to Level 2	\32\ – Section 9.2
2	Field Interface Security	Enable 'Activate additional protection at the interface'	\32\ – Section 9.4

As failsafe applications are important parts for safety of a plant, the SIMATIC Automation System CPU410 provides additional security measures to protect the failsafe application against unauthorized manipulation. By using the SFC 109 "PROTECT" together with an external key switch the protection level can be set. More details are given in \32\ - PCS 7 Process Control System CPU410 Process Automation – section 9.2.

Further information about the Automation System CPU410 provides:

\32\ - PCS 7 Process Control System CPU410 Process Automation

6.12 Automation System SIMATIC S7-1200 / -1500 Controller

In the Blueprint the Automation System SIMATIC S7-1200 / -1500 are used to control a Remote Station like Service Well Water, Line Valves, Storm Water Tanks or Main Distribution Stations.

Table 6-17: SIMATIC S7-1200 / -1500 Controller

No.	Function	Supplier	Type	MLFB
3	Automation System, Non-redundant Control the process area in a Remote Station	Siemens	S7-1200 Controller with CP 1243-8 IRC for TeleControl Communication	6ES7212-1AE40-0XB0 6GK7243-8RX30-0XE0
4	Automation System, Non-redundant Control the process area in a Remote Station	Siemens	S7-1512 Controller with CP1542SP-1 IRC for TeleControl Communication	6ES7512-1DK01-0AB0 6GK7542-6VX00-0XE0
5	Automation System, Non-redundant Control the process area in a Remote Station	Siemens	S7-1510 Controller with CP1542SP-1 IRC for TeleControl Communication	6ES7510-1DJ01-0AB0 6GK7542-6VX00-0XE0

The following hardening measures for the SIMATIC S7-1200 / -1500 Controller must be considered.

Table 6-18: Hardening Measures for SIMATIC S7-1200 / -1500 Controller

No.	Security Topic	Hardening Measure	Documents
1	Protection level	Set at least to Level 3	\45\ – Section 2.2
2	Interface Security	Security recommendations	\41\ – Section 7.6 \42\ – Section 3.4.5 \43\ – Section 4.1 \44\ – Section 4.1

Further information about the PLC SIMATIC S7-1200 and S7-1500 provides:

\41\ - S7-1200 Programable Controller

\42\ - S7-1500 Programable Controller

\43\ - SIMATIC NET TeleControl CP 1243-8 IRC

\44\ - SIMATIC NET TeleControl CP1542SP-1 IRC

\45\ - Security with SIMATIC Controller

6.13 SIPIX WLAN Client

The SIPIX handhelds are used for mobile monitoring and control the Plant as PCS 7 client, see Figure 6-3.

For SIPIX WLAN Client the same hardening measures mentioned in section 6.10.1 are recommended.

7 User Management

The user management in the Blueprint Water Plant is managed centralized by the Active Directory Domain Service. Due to the centralized user management the AGLP principle (Account, Global, Domain local, Permission) must be observed. According to this principle, the domain user accounts are initially assigned to the domain-global groups in the Active Directory. These groups are then assigned to local computer groups which, in turn, receive the permissions to the objects. This includes mechanisms for password recovery and reset mechanisms.

The logon user authentication for the SIMATIC PCS 7 applications, e.g., PCS 7 OS Client Runtime is implemented with SIMATIC Logon, based on the Windows domain groups for operator accounts.

7.1 Domain Controller

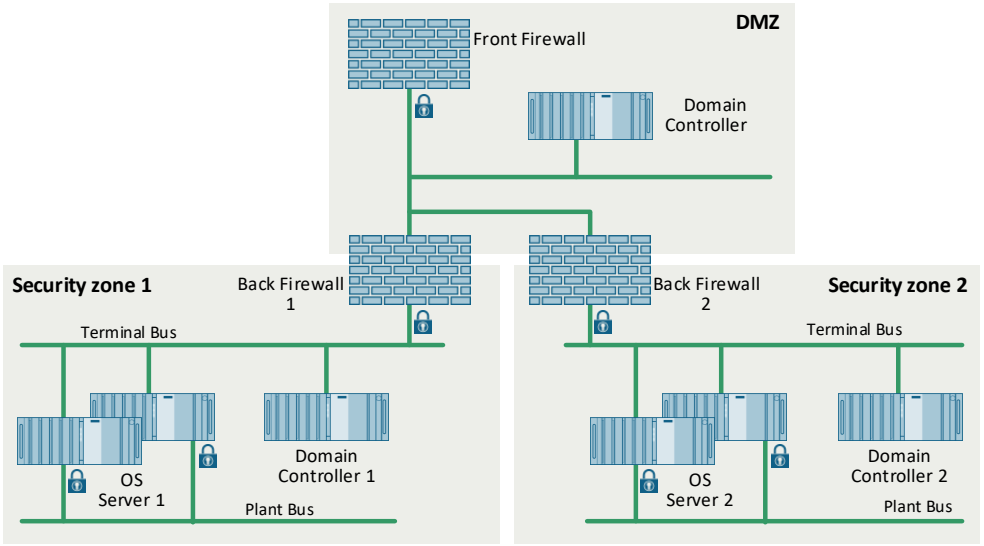
The Domain Controllers in the Blueprint are distributed in Zone 1 – Building and the DMZ, see Figure 3-3. The Domain Controller installed in the Demilitarized Zone DMZ allows the central administration of the Active Directory Domain Service by a central IT department (if needed).

Furthermore, this configuration ensures the stable operation of the distributed control system in case the connection to the DMZ failed.

If multiple subnets/security zones are present, at least one domain controller shall also be provided in each security zone, depending on requirements,
see

Figure 7-1.

Figure 7-1: Domain Controller in the distributed control system



The recommendations for the installation of Domain Controllers for SIMATIC PCS 7 is provided by:

- \2\ – PCS 7 Compendium Part F - Industrial Security, section 7.5

7.2 User Authentication and Authorization

The user authentication and authorization for the operators and engineers in the Blueprint is handled by SIMATIC Logon. SIMATIC Logon authentication is based on Windows domain groups, managed with the Active Directory. All personal user accounts are assigned to domain groups.

For operating system access, non-personalized Windows accounts per system and predefined SIMATIC groups are used. These accounts could be centrally managed by the Active Directory where all PC based machines in the terminal bus, application bus, and DMZ networks are covered.

The accounts on the different machines are configured by using Group Policy Objects (GPOs). There is a hierarchy of GPOs, applied at different scopes (servers, clients, individual machines).

The GPOs settings covered among the settings described in section 6.10, the local group membership (mapping to domain groups), password complexity and local firewall settings.

As personal user accounts are managed by the domain, all user passwords meet complexity requirements (policy enabled and enforced by default on Windows Server 2019 domain controllers).

The user authentication and authorization in the Blueprint is implemented on two layers:

SIMATIC PCS 7 Applications:

Users must log on via SIMATIC Logon before using a SIMATIC PCS 7 application, e.g., PCS 7 OS Client Runtime. SIMATIC Logon authentication is based on Windows domain groups, managed with the Active Directory. All personal user accounts at components are assigned to domain groups.

Operating system:

Some workstations or servers of the Blueprint must be permanently operational and are used by several people. One example is the PCS 7 OS client, for operator control and monitoring. These accounts are non-personalized, machine-specific, and used for Auto logon. All local accounts are assigned to domain accounts.

The user authentication on the applications in the Blueprint is mainly implemented by SIMATIC Logon with the use of domain groups. The following applications do not use SIMATIC Logon.

- PCS 7 Management Console
- SINEC NMS
- PM Analyze
- Infrastructure PC
- Terminal Server
- Quarantine Server
- Energy Manager Pro

The user authentication and authorization for these applications is implemented by local accounts integrated into the domain.

During the installation of SIMATIC PCS 7 applications a standard set of local Windows groups is created. The SIMATIC PCS 7 applications use these standard local Windows groups. The domain groups must be assigned to the local user groups.

Apart from the personal user accounts, SIMATIC PCS 7 also requires a standard set of non-personalized accounts (e.g., ENG1, OSC1-2, OSS1A, OSS1B). These accounts are members of the local SIMATIC groups. For these accounts, password changes are only permissible when the PCS 7 runtime mode is stopped, because these accounts are used for authentication of the communication between SIMATIC PCS 7 systems, among other things. Password changes of the affected user accounts must be made simultaneously on all involved systems, otherwise proper operation cannot be ensured. Therefore, it is recommended that password aging for these user accounts is disabled.

Further information on user authentication and authorization is provided in:

- \1\ – Security concept PCS 7 & WinCC (Basic), section 7.4.3
- \2\ – PCS 7 Compendium Part F - Industrial Security, section 7
- \34\ – PCS 7 SIMATIC Logon

8 Malware Protection and Whitelisting

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

In the Blueprint the protection against malware and unauthorized changes is implemented using

Anti-Virus software

The latest version of the Anti-Virus Software Microsoft Defender Antivirus released for use with SIMATIC PCS 7 is installed by default (integrated in the actual Microsoft operating systems) on workstations and servers of the Blueprint.

To ensure that the virus signatures files on all workstations and servers are up to date, a WSUS server is installed in the DMZ. This server receives the most actual virus signatures from the Microsoft update server on the internet or from an upstream WSUS server and provides these signatures to the managed virus scan clients.

The SIMATIC Management Console captures events logged by Windows Defender from all computers in the network and displays them in the "Events" window. Critical events are also displayed in the message window and could be forwarded via mail to an administrative contact.

Whitelisting techniques

The latest version of Trellix Application Control released for use with SIMATIC PCS 7 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 on workstations and servers. After the installation activation of Trellix Application Control, all executable applications and files are protected against modification.

Trellix Application Control is not installed on all workstations and servers in Blueprint. The table in section 16 shows where this application is installed.

Trellix Application Control are configured and managed centralized by using the Trellix ePolicy Orchestrator (ePO). This software is installed on the Infrastructure PC in DMZ.

Note for SIMATIC PCS 7 V9.1 and later

If an alternative endpoint protection software should be used, it is recommended to consider the following generic recommendations and that the software is checked for compatibility before productive use:

- Since version SIMATIC PCS 7 V9.1 just Microsoft Defender Antivirus is the released virus scanner.
- Plant owners, who like to use other than the released endpoint protection products in SIMATIC PCS 7 V9.1 and later versions, can do this in their own responsibility.
  In case support is needed by plant owners the Siemens customer support might ask to deactivate / deinstall these products to check whether the issues found are related to the used products. If this is the case, the support will be limited or chargeable.
  For such a scenario Siemens Industrial Security Services (\39\) can provide extended services in advance
  \35\ -" Services for 3rd Party endpoint protection products with SIMATIC PCS 7"
- For further information about this topic, it is recommended to consider this document
  \34\ - "SIMATIC Process Control System PCS 7 Managing Endpoint Security Solutions."

Further information of the use and configuration Anti-Virus software and Whitelisting is provided in:

- \2\ – PCS 7 Compendium Part F - Industrial Security, section 6.7 and 9
- \34\ – PCS 7 Managing virus scanners.
- \36\ – Utilization of Whitelisting with McAfee Application Control for PCS 7

9 Anomaly Detection

The Industrial Anomaly Detection (IAD) solution from Siemens is an important addition to the holistic "Defense-in-Depth" concept. It provides enormous added value regarding the requirement for attack detection systems, especially intrusion detection systems (IDS), which is repeatedly stated in the IT-Grundschutz compendium. For the first time, it is possible to achieve complete transparency of all network components and their communication in automation and control systems.

Deviations from normal operation are automatically detected by the IAD solution, and information on the type, timing and weighting of the communication taking place is automatically enriched and processed. As a result, processes taking place can be visually displayed and anomalies can be intuitively detected and investigated by the plant operator.

The IAD solution from Siemens can be integrated seamlessly and without influencing the operation of the automation and control systems. This applies to both new and existing plants already in production. It offers the following functionalities:

- Feedback-free implementation of an IAD sensor on the SPAN port of one or more switches.
- Processing and display of network traffic received from the sensors in the IAD Center
- Integrated database with currently known vulnerabilities and malwares
- Early detection of anomalies and cyber threats
- Visibility into assets and vulnerabilities
- Sensors and center are implemented on Siemens IPCs
- Events can be easily forwarded from the center, e.g., to a central SIEM system or SOC:

Function	SCI	Supplier	Type	MLFB
IAD Sensor	45	Siemens	IPC 427E	6AG4141-5BC10-0JA8
IAD Center	46	Siemens	IPC 427E	6AG4141-0BB00-0JA0

For further information regarding Industrial Anomaly Detection solution from Siemens, please refer to SIOS chapter “Industrial Anomaly Detection” \48\ and then Claroty Manuals \49\.

10 Patch Management

10.1 Patch Management for SIMATIC PCS 7 Components

IEC 62443 recommends the Defense-in-Depth concept as comprehensive protection of industrial facilities against cyberattacks. The protection of system integrity is one important part of the Defense-in-Depth concept, see section 2.2.

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

Patch management is a systematic procedure for installing patches on distributed control systems.

Updates differ in

- Updates for the Operating System Microsoft Windows
- These are all types of updates, service packs, feature packs and similar installations, whether these relates to security or not.
- Updates for Microsoft applications, e.g., Microsoft Office.
- Firmware and software updates because of vulnerabilities, both for Siemens software and products and 3rd party components

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

Regarding security vulnerabilities in 3rd-party components which are not owned by Siemens, the plant owner has the responsibility to ensure that these components are on the latest available patch level.

The Windows Server Update Service (WSUS) installed on the Infrastructure PC in the DMZ of the Blueprint manages the Microsoft software updates for the distributed control systems. The WSUS get the most actual Microsoft updates either from the Microsoft Update server or from a WSUS server in the customer enterprise network. The WSUS is distributing the updates to all Windows-based PCs of the distributed control system.

Additionally, the SIMATIC Management Console with its "Microsoft Software Update Management" function can be used. This gives the user the option of executing Microsoft software updates in a recommended and SIMATIC PCS 7 compliant method on all target computers on which the SIMATIC Management Agent is installed. Siemens is testing the compatibility of Microsoft updates for released Microsoft products like Windows and SIMATIC PCS 7. The list of tested Microsoft updates is available here:

- https://support.industry.siemens.com/cs/ww/en/view/18490004

Available software updates for PCS, V9.1 SP2 are published here:

- https://support.industry.siemens.com/cs/ww/de/view/109756832

For all products from Siemens, including third party components, Siemens publishes security advisories monthly. The advisories are published here:

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

Further information about patch management and WSUS is provided in

- \2\ – PCS 7 Compendium Part F - Industrial Security, section 8
- \37\ – PCS 7 Patch management and security updates

10.2 Patch Management of SIMATIC PCS 7 Software

Software updates of SIMATIC PCS 7 shall be managed via SIMATIC Management Console (SMMC).

Table 10-1: Information channels and sources for Siemens products

Nr.	Business Unit	Information channel	Source for documentation / Updates
1	Digital Industries (DI)	Notification / Advisories \47\ - Siemens ProductCert	Product / System related patches are available at \4\ - Siemens Industry Online Services Manual \22\ - SIMATIC PCS 7 SIMATIC Management Console

10.3 Patch Management of Automation and Network Components

Firmware updates of CPUs and PLC CPs shall be managed via PCS 7 ES. In the case of SCALANCE network components, firmware updates shall be centrally deployed via SINEC NMS.

Table 10-2: Information channels and sources for Siemens products

Nr.	Business Unit	Information channel	Source for documentation / Updates
1	Digital Industries (DI)	Notification / Advisories \47\ - Siemens ProductCert	Product / System related patches are available at \4\ - Siemens Industry Online Services

11 Security checks

Regular verification of the implemented security measures is a necessary organizational task that is technically supported by the SIMATIC PCS 7 Security Concept and the SIMATIC PCS 7 Compendium Part F.

The verification of the intended security measures must not hinder the availability and stability of ongoing operations.

The following components are useful for checking the specified and implemented security settings/measures:

Malware protection management consoles.

The management consoles (ePO, ...) of the virus scanning servers and whitelisting allow to detect current states in the form of dashboards, reports and messages/alerts.

SIMATIC Management Console (SMMC)

Informs about the patch status of SIMATIC PCS 7 components and Windows systems.

WSUS

Informs about the patch status of Windows systems.

SINEC NMS

The SINEC NMS software is a network management system for monitoring and managing industrial networks. It enables you to fully visualize and monitor networks. In addition, SINEC NMS enables you to configure the network infrastructure. Using the rule-based approach, you can configure across devices in the network independent of device types, or you can regularly back up the device configurations to keep up with configuration changes. Another major point is the central function for a firmware update in the network infrastructure.

Anomaly detection

See chapter 9

Active Directory

The use of an Active Directory (Windows domain) allows the central rolling out of security measures (e.g., locking removable media, activating the local firewall, password rules) and central management of users, groups and policies.

SINEC Security Inspector

The SINEC Security Inspector is a unique comprehensive security testing solution for OT/IT environments, combining market-leading and in-house tools on a single platform. The user-friendly Security Inspector management console enables simple planning and automation of individually compiled test procedures, so you can quickly and regularly determine the safety status of components, solutions or entire production networks, which saves valuable time and significantly enhances security. Detection of security vulnerabilities becomes possible within minutes.

12 Asset management

In the IT/OT sector, assets are the stocks of objects (hardware, software, documents, licenses) that are needed to implement the (control technology) requirements.

The objects should be identified and maintained in the form of a suitable inventory.

A formal (configuration) management process should be established to monitor changes in the component inventory.

A complete inventory supports or enables the implementation of a wide range of tasks, such as patch management, assignment of responsibilities and classification.

The inventory should document the following information for each component:

- Unique identifier
- Information that allows quick localization in production
- Version reference (firmware, software, versions, hardware)
- Intended use
- Handling
- Owner / Responsibility
- Criticality / Classification

Asset inventory/recording can be achieved through a variety of tools and techniques:

- ➢ Virus scanner/whitelisting management consoles provide an overview of facility installed computer systems.
- ➢ SIMATIC Management Console provides an overview of installed SIMATIC PCS 7/WinCC components, software and licenses. The source of the inventory data can be objects in the plant (online data) or objects in project data (offline data). See Table 3-2

Inventory data can be determined for the following objects of the SIMATIC PCS 7 plant:

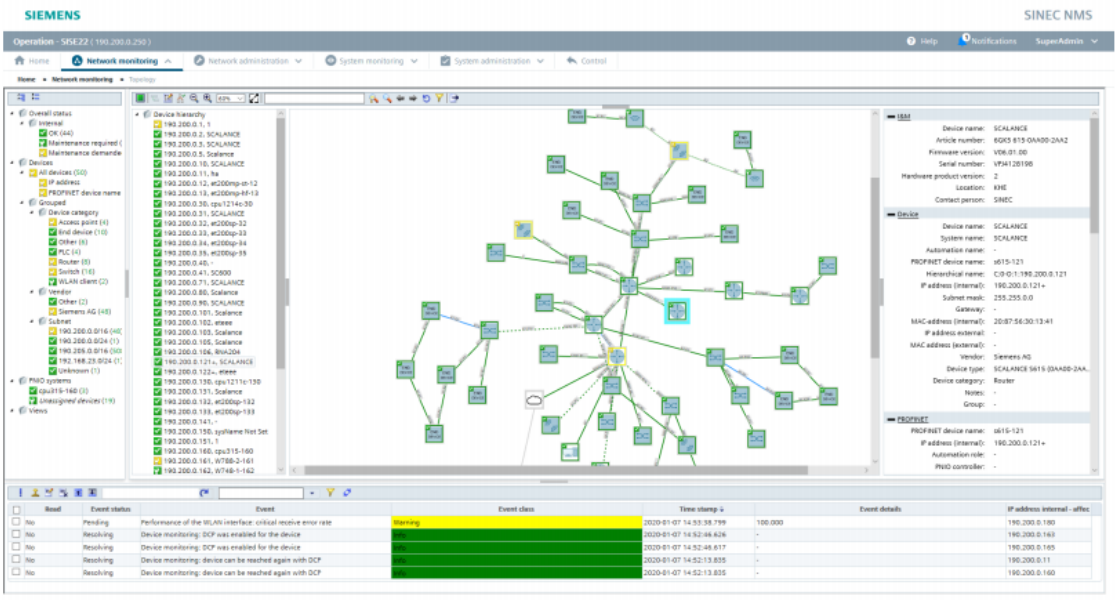
- Computers
- Network components (Ethernet switches)
- Automation system components
- Remote I/Os (including I/O modules)
- Field devices

- ➢ The use of scanning services such as "Active Asset Inventory Scan" automatically captures the installed assets and software versions in automation systems and allows the data to be used in vulnerability management systems, such as IVM (Industrial Vulnerability Manager). See chapter 15.2
- ➢ Monitoring systems, such as Industrial Anomaly Detection (IAD) can provide inventory lists of installed network components. See chapter 9

12.1 Documentation of Network topologies

A tool supporting the documentation of the networks is the network management system SINEC NMS. It is used not only for the administration of the networks, but also for the documentation of the topologies. See also chapter 5.1.4 (Administration of the network devices)

Figure 12-1: Network Topology



13 Backup and Recovering

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

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

Data backup will be categorized as following:

System Backup

System backup refers to a complete system image, e.g., a snapshot of the current system. Following data is included:

- Hardware-specific files (drivers)
- Windows operating system files and settings
- Installed programs and their configurations.
- Host devices (Hardware-specific files (drivers), Windows operating system files and settings, installed programs and their configuration)

For system backups during the runtime of SIMATIC PCS 7 (online imaging), the product "SIDSI Backup & Restore" has been tested for compatibility on IPC systems and in virtual environments.

For "Offline Images" the "SIMATIC IPC Image & Partition Creator" is recommended.

Project Backup

Project backup mainly refers to the backup of the PCS 7 Multiproject on the ES. SIMATIC Manager is used for such a specific project backup.

- If necessary, SIMATIC Version Trail is also required. See chapter 10.1

Component specific Data

Component specific data like databases or individual configuration of embedded or network devices requires to be backed up. The Backup & Restore for SCALANCE network devices is handled by the SINEC NMS function Configuration Repository

- \28\ - SINEC NMS Manual, section 5.4

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

Further information about Backup and Restore provides

- \2\ – PCS 7 Compendium Part F - Industrial Security, section 10

13.1 Storage

Special attention should be paid to the appropriate storage of backup media. If the data media are stored in an insecure location, an attacker (e.g., an internal perpetrator) may be able to access them and steal or manipulate sensitive information. Likewise, data media with backups can be lost or rendered unusable by unfavorable storage, climatic room conditions, malware, technical malfunctions, insufficient/insufficiently planned storage capacities or a fire.

Backups should additionally be stored in an "off-site location" with adequate protection from physical and environmental factors.

13.2 Automation of Data Backup

If an automation of the data backup is required ("data backup function with adjustable repetition rate"), an implementation is possible.

The online image as well as the (SIMATIC PCS 7) project backup can be automated time-controlled. SIMATIC Version Trail is used for automatic backup and versioning of libraries and projects.

A possible scenario is:

1. The project backups and images are generated/stored locally in a time-controlled manner and additionally stored on NAS1 in the Terminal Bus.
2. NAS1 synchronizes 1x weekly the data on NAS2 in the DMZ.
3. Possibly combine procedure with offline backups on USB hard disks or tapes, since the low effort justifies the security gained (possibly once after the SAT or an upgrade).

14 Disposal of Components

The sensitive data of the system, e.g., passwords and cryptographic material as well as configurations could be misused when disclosed to unauthorized persons.

The asset owner should purge all this data on devices securely when no longer required. In particular, sensitive data must be purged before the disposal of devices. This applies to all devices, including removable media.

\2\ - PCS7 Compendium F, section 11 provides an overview about most resetting and removing procedures. This includes capabilities or methods to remove sensitive data.

The following table provides advice how to do purging of sensitive data in the system components:

Table 14-1: Purging of sensitive data on devices.

Device Type	Data	How to Dispose
Embedded devices	Project code	CPU components must be reset to the factory state and the flash memory must be deleted. The reset to the factory state is described in the SIMATIC AS410-5H manuals: \46\ - CPU 410 Process Automation – System manual, Section 9.8 \41\ - S7-1200 Automation System, Section 15.5 \42\ - S7-1500 Automation System, Section 13.6
Network devices	Firewall rules	SCALANCE components must be reset to the factory state. SINEC NMS provides the possibility reset the SCALANCE device to factory setting by using a specific device profile. \28\ - \SINEC NMS – Operational Manual, section 7.2.1 The SIEMENS Industry Online Support (SIOS) provides manuals for all SIMATIC products used in the solution. \4\ - SIEMENS Industry Online Support (SIOS) The Palo Alto Firewalls NG must be reset to the factory default settings. \6\- Palo Alto – Reset to factory default settings
Storage media	Depending on usage	USB media, CDs, DVDs and other media must be completely erased or handed over for secure disposal (e.g., shredder)
Hosts	Configurations, passwords, cryptographic keys	Complete systems (e.g., IPC computers) must be handed over for secure disposal.

15 Optional Security Measures

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

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

Further information about the optional security measures provides \38\ - Siemens Industrial Security Service

15.1 Threat Prevention Subscription for Front- and Back-Firewalls

The Palo Alto Next Generation Firewalls described in section 6.3.1 can be enhanced with the Threat Prevention Subscription (TPS) option. We recommend the use of the TPS option if remote access is installed.

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

15.2 Industrial Vulnerability Manager

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

The Industrial Vulnerability Manager has the following features:

- Hosting of the list of components embedded in your ICS that shall be monitored over the time with regards to security flaws
- Free assignment of the components to the created monitoring list
- Integration with SIMATIC Management Console
- Integration with SINEC NMS
- Dashboards with charts and diagrams to highlight relevant information concerning the published security bulletins.
- Automatic release of security bulletins as soon as a new security flaw affecting a registered component is published by its component vendor.

- The security bulletins that are automatically generated contain the following information:
- Description of the vulnerability
- CVSS (Common Vulnerability Scoring System) score and Priority status.
- List of affected components
- Recommendations, workarounds, mitigations and patch status
- Vendor advisory link
- Assignment of a tag to the published security bulletins with regards to the handling status ("Open", "Ongoing", "Closed")
- The application is accessible via a secured web interface.

15.3 Security Information Event Management (SIEM)

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

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

A SIEM system can continuously collect network information and information from different devices, link it all up, analyze and display it, and derive the appropriate security measures.

16 Applications and Operating Systems

The following table lists the operating system and applications, installed on the host systems of the Blueprint.

Installed Software	PCS 7 Engineering Station – DCS	PCS 7 Engineering Station – SIS	PCS 7 OS / TeleControl Client	PCS 7 Maintenance Station	PM Analyze	PCS 7 OS Server, redundant	PCS / Process Historian, red.	SINEC NMS - Operation	PCS TeleControl Server	Domain Controller, redundant	PCS 7 Management Console	SINEC NMS - Control	PCS 7 OpenPCS 7 Server	PCS 7 Web Server	SINEMA RC Server	PCS 7 Information Server	Infrastructure PC	SIWA Suite Server – SEWER App.	Energy Manager Pro	SIPIX	Anomaly Detection Sensor/ Center
SIMATIC PCS 7 Maintenance Station Engineering V9.0				X																	
SIMATIC PCS 7 Maintenance Station Runtime Asset TAGs				X																	
PM Server					X																
PM AGENT						X															
PM ANALZE Client			X																		
SIMATIC PCS 7 OS Software Server V9.0									X												

Installed Software	PCS 7 Engineering Station – DCS	PCS 7 Engineering Station – SIS	PCS 7 OS / TeleControl Client	PCS 7 Maintenance Station	PM Analyze	PCS 7 OS Server, redundant	PCS / Process Historian, red.	SINEC NMS - Operation	PCS TeleControl Server	Domain Controller, redundant	PCS 7 Management Console	SINEC NMS - Control	PCS 7 OpenPCS 7 Server	PCS 7 Web Server	SINEMA RC Server	PCS 7 Information Server	Infrastructure PC	SIWA Suite Server – SEWER App.	Energy Manager Pro	SIPIX	Anomaly Detection Sensor/ Center
SIMATIC PCS 7 OS Software Server Redundancy V9.0						X															
SIMATIC PCS 7 OS Runtime Licenses						X			X												
SIMATIC PCS 7 OS Archive						X															
SIMATIC PCS 7 Process Historian Server Red. V9.0							X														
SIMATIC PCS 7 Information Server Basic Package V9.0																X					
PCS 7 TeleControl OS Engineering	X	X																			
PCS 7 TeleControl OS Runtime V9.0									X												

Installed Software	PCS 7 Engineering Station – DCS	PCS 7 Engineering Station – SIS	PCS 7 OS / TeleControl Client	PCS 7 Maintenance Station	PM Analyze	PCS 7 OS Server, redundant	PCS / Process Historian, red.	SINEC NMS - Operation	PCS TeleControl Server	Domain Controller, redundant	PCS 7 Management Console	SINEC NMS - Control	PCS 7 OpenPCS 7 Server	PCS 7 Web Server	SINEMA RC Server	PCS 7 Information Server	Infrastructure PC	SIWA Suite Server – SEWER App.	Energy Manager Pro	SIPIX	Anomaly Detection Sensor/ Center
PCS 7 TeleControl SINAUT Driver [1)]									X												
PCS 7 TeleControl DNP3 Driver [1)]									X												
PCS 7 TeleControl IEC 60870-5-101/-104 Driver [1)]									X												
PCS 7 TeleControl Server Basic									X												
PCS 7 Management Console V9.0									X												
PCS 7 Management Console Agent	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X		
SINEC NMS Server								X				X									
SIMATIC PCS 7 OpenPCS 7 V9.0													X								

Installed Software	PCS 7 Engineering Station – DCS	PCS 7 Engineering Station – SIS	PCS 7 OS / TeleControl Client	PCS 7 Maintenance Station	PM Analyze	PCS 7 OS Server, redundant	PCS / Process Historian, red.	SINEC NMS - Operation	PCS TeleControl Server	Domain Controller, redundant	PCS 7 Management Console	SINEC NMS - Control	PCS 7 OpenPCS 7 Server	PCS 7 Web Server	SINEMA RC Server	PCS 7 Information Server	Infrastructure PC	SIWA Suite Server – SEWER App.	Energy Manager Pro	SIPIX	Anomaly Detection Sensor/ Center
SIMATIC PCS 7 Web Server Basic V9.0														X							
SIMATIC PCS 7 Web Server license														X							
SINEMA Remote Connect V2.0									X						X						
SIMATIC Energy Manager V7.1																			X		
PCS 7 PowerControl OS Engineering	X	X																			
McAfee Application Control, latest released version For PCS 7 Version 9.1 Microsoft Windows Defender	X	X	X	X	X	X	X		X		X		X	X	X	X		X	X		
Anomalie Detection																					X

Installed Software	PCS 7 Engineering Station – DCS	PCS 7 Engineering Station – SIS	PCS 7 OS / TeleControl Client	PCS 7 Maintenance Station	PM Analyze	PCS 7 OS Server, redundant	PCS / Process Historian, red.	SINEC NMS - Operation	PCS TeleControl Server	Domain Controller, redundant	PCS 7 Management Console	SINEC NMS - Control	PCS 7 OpenPCS 7 Server	PCS 7 Web Server	SINEMA RC Server	PCS 7 Information Server	Infrastructure PC	SIWA Suite Server – SEWER App.	Energy Manager Pro	SIPIX	Anomaly Detection Sensor/ Center
Claroty (CTD & Sensor Software)																					

17 Appendix

17.1 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

Industry Online Support

Industry Online Support is the previous address for information on our products, solutions and services.

Product information, manuals, downloads, FAQs and application examples - all information is available with just a few mouse clicks: support.industry.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:

17.2 Links and literature

When selecting the documents listed below, always make sure that they are the most recent edition

Table 17-1

No.	Document
\1\	SIMATIC Process Control System PCS 7 Security concept PCS 7 & WinCC (Basic) https://support.industry.siemens.com/cs/ww/en/view/109780811
\2\	Process Control System PCS 7 Compendium Part F - Industrial Security https://support.industry.siemens.com/cs/ww/en/view/109815443
\3\	SIEMENS devices with Achilles certification https://new.siemens.com/global/de/unternehmen/themenfelder/zukunft-der-industrie/industrial-security/zertifizierung-normen.html
\4\	Siemens Industry Online Support https://support.industry.siemens.com
\5\	Checklist for Setting Up SCALANCE Devices https://support.industry.siemens.com/cs/ww/en/view/109745536
\6\	PAN-OS® Administrator's Guide https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html
\7\	Palo Alto Website about PAN-OS https://docs.paloaltonetworks.com/pan-os.html
\8\	SCALANCE SC-600 – Web Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109754815
\9\	SCALANCE SC-600 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109754812
\10\	SCALANCE M800 Web – Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109751635
\11\	SCALANCE M812, M816 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/90316607
\12\	SCALANCE M826 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/99450800
\13\	SCALANCE M874, M876 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/74518712
\14\	SCALANCE W780, W740 Web – Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109759652
\15\	SCALANCE W780, W740 – Operating Instructions https://support.industry.siemens.com/cs/ww/de/view/109759651
\16\	SCALANCE XC-200 / XF-200BA Web – Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109750283
\17\	SCALANCE XC-200 – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109743149
\18\	SCALANCE XF-200BA – Operating Instructions https://support.industry.siemens.com/cs/ww/en/view/109750282
\19\	TIM 1531 IRC – Manual https://support.industry.siemens.com/cs/ww/en/view/109748454
\20\	RTU3030C – Operating Instruction https://support.industry.siemens.com/cs/ww/en/view/109750942
\21\	Industrial Ethernet Security basics and application – Configuration Manual https://support.industry.siemens.com/cs/ww/en/view/109738463
\22\	SIMATIC PCS 7 - SIMATIC Management Console https://support.industry.siemens.com/cs/ww/en/view/109805386
\23\	deleted

No.	Document
\24\	PCS 7 Time Synchronization https://support.industry.siemens.com/cs/ww/en/view/109805436
\25\	DTS 4138.timeserver – Mounting and Instruction Manual http://www.mobatime.com/customer-area/product-resources/timeserver/dts-4138timeserver.html
\26\	PCS 7 Readme https://support.industry.siemens.com/cs/ww/en/view/109806027
\27\	SIMATIC Process Control System PCS 7 PC Configuration https://support.industry.siemens.com/cs/ww/en/view/109812498
\28\	Network management SINEC NMS https://support.industry.siemens.com/cs/ww/en/view/109762749
\29\	SIMATIC Energy Manager PRO V7.1 – Operation https://support.industry.siemens.com/cs/ww/en/view/109742442
\31\	SIMATIC Energy Manager PRO V7.1 – Acquisition https://support.industry.siemens.com/cs/ww/en/view/99086102
\32\	PCS 7 Process Control System CPU 410 Process Automation https://support.industry.siemens.com/cs/ww/en/view/109815344
\33\	PCS 7 SIMATIC Logon https://support.industry.siemens.com/cs/ww/en/view/109812142
\34\	SIMATIC Process Control System PCS 7 Managing Endpoint Security Solutions https://support.industry.siemens.com/cs/ww/en/view/109813043
\35\	Services for 3rd Party endpoint protection products with SIMATIC PCS 7 https://support.industry.siemens.com/cs/ww/en/view/109810527
\36\	Utilization of Whitelisting with McAfee Application Control for PCS 7 https://support.industry.siemens.com/cs/ww/en/view/88653385
\37\	PCS 7 Patch management and tested security updates https://support.industry.siemens.com/cs/ww/en/view/18490004
\38\	Palo Alto - Best Practices for Securing Administrative Access section https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html
\39\	Siemens Industrial Security Services https://new.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html
\40\	SIMATIC Energy Manager V7.2 Installation https://support.industry.siemens.com/cs/ww/en/view/109742441
\41\	SIMATIC S7 1200 Programable Controller https://support.industry.siemens.com/cs/de/en/view/109759862
\42\	SIMATIC S7 1500 Programable Controller https://support.industry.siemens.com/cs/de/en/view/86140384
\43\	SIMATIC NET: S7 1200 TeleControl CP 1243-8 IRC https://support.industry.siemens.com/cs/ww/en/view/109777054
\44\	SIMATIC NET: S7 1500 TeleControl CP 1542SP-1 IRC https://support.industry.siemens.com/cs/ww/en/view/109741690
\45\	Security with SIMATIC S7 -Controller https://support.industry.siemens.com/cs/ww/en/view/90885010
\46\	See \32\
\47\	ProducCERT Advisory Page https://new.siemens.com/global/en/products/services/cert.html%23securitypublications
\48\	Anomalie Detection https://support.industry.siemens.com/cs/sc/4987/industrial-anomaly-detection?lc=de-DE
\49\	Claroty Manual https://claroty.com/continuous-threat-detection/

17.3 Change documentation

Table 17-2

Version	Date	Modifications
V1.0	04/2020	First version
V2.0	07/2020	Addition of the chapter 14 Disposal of Components
V3.0	11/2021	Addition of new chapter 9 Anomalie Detection Addition of the chapter 11 Security Checks Addition of the chapter 12 Asset Management Addition of the chapter 12.1 Network Topologies Addition of the chapter 13.1 Data Storage Addition of the chapter 12.1 Automatic Data Backup Deleting chapter 6.8.1 & 6.8.2 (CP1628/CP443 Adv,) Deleting old chapter 14.3 Anomalie Detection
V4.0	09/2023	Update PCS 7 9.1