Cybersecurity

Defense-in-Depth Concept for the Water and Waste Water Industry

Preface

This whitepaper provides an overview on the subject of Industrial Security in the water and waste water industries. It describes the threats and risks to which industrial automation and control systems in water and waste water treatment plants and networks are exposed, and introduces best practice concepts to minimize these risks and to achieve a level of protection to be implemented that is acceptable with regards to both the economic boundary conditions and the desired security level. It also covers the demands to face the ever increasing threats due to the trends of digitalization, such as ubiquitous connectivity and large amounts of valuable data which make cyber-attacks in unprotected installations easier and more likely.

Further information regarding industrial security at Siemens can be found here:
https://www.siemens.com/industrialsecurity

The information presented in this whitepaper is current as of March 2020.

Publisher
Siemens AG
Digital Industries

Gleiwitzer Str. 555
90475 Nuremberg, Germany

Support

Please direct any questions in connection with this whitepaper to your Siemens contact person at your representative/ sales office or industrialsecurity.i@siemens.com.

Security disclaimer

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. The products and solutions of Siemens 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 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.

Products and solutions of Siemens undergo continuous development to make them more secure. Siemens strongly recommends that the latest product versions are used and that product updates are applied as soon as they are available. The use of product versions which are no longer supported and the 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/industrialsecurity.

Contents

1 Introduction

The secure operation of the water and waste water infrastructure is critical for all areas of society and industry.

In order to ensure the guaranteed supply of high-quality drinking water as well as legally compliant waste water treatment, Siemens supports consultants, partner companies such as system integrators as well as water and waste water operating companies in the designing, implementation and managing of secure automation solutions.

The increasing digitization of industrial automation and control systems (IACS) is accompanied with tight integration, large amounts of data and the use of open standards to provide the necessary direct access across all levels of the systems. The resulting enormous advantages for users have prompted experts to speak of a new industrial revolution – "Industry 4.0".

In analogy – and adapted to the water and waste water sector – concepts such as “Water 4.0” were developed which focus on automation and digitalization as key aspects of a strategy for resource-efficient, sustainable and flexible water management.

However, this trend to interconnected systems has a significant downside in the form of increased vulnerability to cyber-attacks by various actors.

Comprehensive integration and open communication standards make it significantly easier for attackers and malware – with malicious intent – to access systems. Studies and concrete incidents show that not only control systems – in contrast to information technology (IT) also known as operational technology (OT) – and production areas are recognized as worthwhile targets for attacks of various kinds. The organizations behind these attacks are also becoming increasingly aggressive in their tactics, applying more effective tools and devoting more resources to seriously disrupt or damage public life.

Considering water supply and waste water disposal as critical infrastructures implies the need to develop, implement and maintain a strategy for technical and organizational measures to protect and secure the operation of water and waste water facilities.

The reality today is that all industrial, administrative and infrastructure systems are exposed to professionally executed attacks. The changed threat situation requires a fundamental rethinking of information and operation security, access protection – as well as the entire process of defining and implementing industrial security concepts. Never has it been so important for vendors, solution providers and operators of control systems to face up to the threat they pose.

Facing the Cybersecurity Challenges and taking Action

Critical infrastructure facilities require special IT- and OT-security solutions that ensure uninterrupted plant availability, real-time capability of critical IACS functions and comprehensive constantly updated protection against threats. These requirements can be met by coordinated, broadly diversified and comprehensive concepts with components and systems suitable for industrial use.

In this regard, it is advisable to implement the so-called Defense-in-Depth concept, standardized in IEC 62443 and provided by Siemens as a leading IACS vendor as well as an IACS solution and service provider.

If the appropriate tools are used, the security of water and waste water plants and networks can be continuously monitored, and attacks can be detected and prevented. System access and communication are analyzed and documented so that companies can fulfill their obligation to identify and report environmental and security-related incidents to the authorities.

Both organizational and technical measures must be carefully coordinated: a holistic security concept relies on people, processes and technology in synergy to achieve the necessary level of protection. The IEC 62443 standard addresses all parties involved, namely IACS vendors, solution and service providers as well as operating companies; it defines responsibilities and relevant organizational interfaces, and it provides a framework for defining, implementing, documenting, testing and maintaining organizational and technical measures.

Relevant stakeholders and their responsibilities are following:

Asset Owner / Operating Company

- Implementation of an Information Security Management System
- Definition of the protection goals for the respective plant
- Definition of the security requirements for the respective plant
- Application of a comprehensive Patch Management for the control system of the respective plant

Solution and Service Supplier

- (Certified) engineering and management solution process in place
- Secure design of a system architecture for the customer solution including a Threat and Risk Analysis
- Relevant customer documentation
- Incident and Vulnerabilities Handling during the project execution
- Application of a comprehensive Patch Management for all products shall be used in the solution during the project execution

Product and System Supplier (IACS Vendor)

- (Certified) development process for products in place
- Development for products with security functionalities
- Relevant customer documentation
- Incident and Vulnerabilities Handling for entire product lifecycle
- Application of a comprehensive Patch Management for own products including 3rd-party components and software

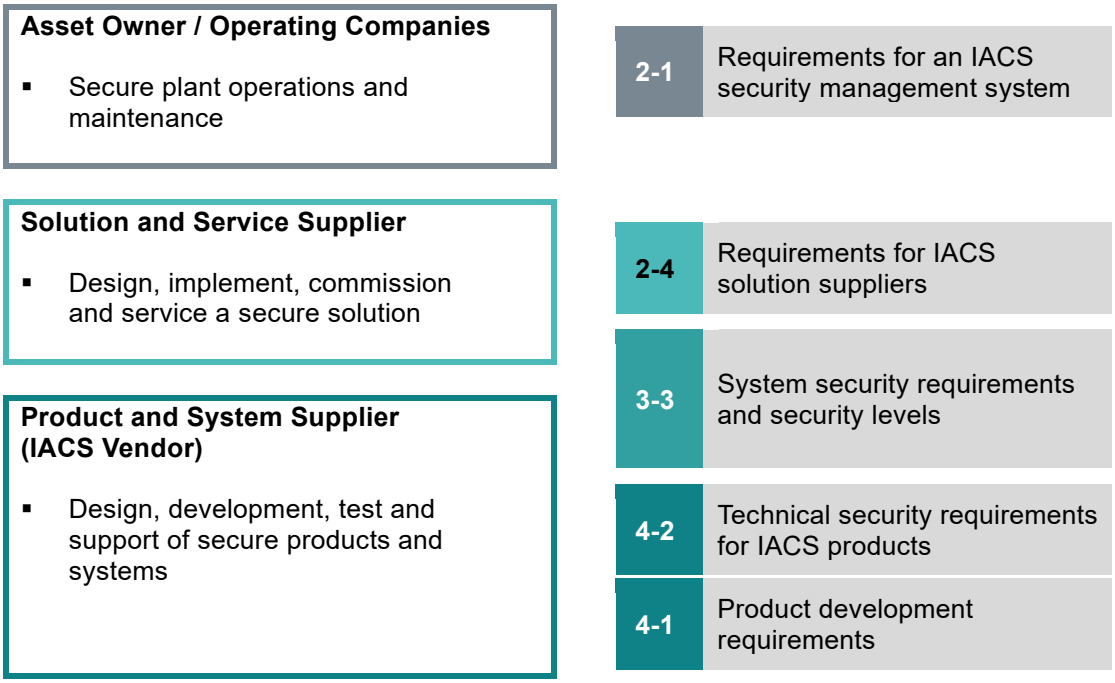

Figure 1: Standards to define the requirements on security for product and system suppliers, system integrators and/or solution suppliers as well as asset owners/ operating companies

Relevant Documents for Cybersecurity in Water and Waste water

This whitepaper describes a comprehensive security concept for industrial automation and control systems and solutions – aligned with IEC 62443 – for the protection of water and waste water treatment plants and networks. It maps general requirements to the specific protection goals and threats of the water sector; it covers DCS and SCADA systems, network concepts including remote and telecontrol as well as relevant security appliances.

Further dedicated whitepapers for the DCS SIMATIC PCS 7, SCADA systems SIMATIC WinCC Professional, V7 and Open Architecture in the water and waste water sector are available at
https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/downloads.html

For detailed technical information and practical implementation of security measures for water and waste water, please refer to the Secure Configuration Guidelines of DCS SIMATIC PCS 7, SCADA systems SIMATIC WinCC Professional, V7 and Open Architecture at

https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/downloads.html

Further information on cybersecurity is available at
https://www.siemens.com/industrialsecurity

Motivation

As mentioned above, the increasing interconnections and data exchange between industrial devices and both IT- and OT-systems to leverage the benefits of “Industry 4.0”, also fundamentally increase the threats and risks.

In addition to direct attacks, misconduct or side effects of changes in system configurations can also affect a plant or even the entire operation of the customer.

As response to these threats, legislative authorities throughout the world defined assets that are crucial for the functioning of society and economy. These assets, referred to as ‘Critical Infrastructure’ are subject to special regulations, which, among other things, prescribe the continuous maintenance of network security at ‘state of the art’ standard or the obligation to provide information regarding serious cyber-incidents.

In the EU, Directive 2008/114/EG was issued with the aim of identifying critical infrastructures and defining appropriate protection plans. The member states implemented this guideline in their national law in 2011.

In Germany, the relevant regulation for critical infrastructure is BSI-KritisV. In addition, guidelines are provided for the implementation of industry-specific security standards (B3S).

Figure 2: German IT Security Act KRITIS

Even though the current German IT security act stipulates the necessity of a regular review and assessment of the security status of critical infrastructures serving 500,000 population equivalents upwards, in view of the fact that attacks are not necessarily targeted to larger plants, small- to medium-sized water and waste water facilities and networks are also of comparable relevance to security of supply and should also be protected using professional methods.

There are different standards and guidelines which can be applied to secure IT- and OT-infrastructure. For critical infrastructures, the series IEC 62443 is internationally accepted as most comprehensive standard for industrial automation and control systems and networks. It addresses all parties involved, namely IACS vendors, solution and service providers as well as operating companies.

2 Overview of the Siemens Concept for Industrial Security

All aspects, from public and enterprise networks through the plant level down to the field level including i) plant security and physical access control as well as ii) network security and iii) system integrity, must be addressed simultaneously to protect water and waste water plants from internal and external cyber-attacks. The most suitable approach is the Defense-in-Depth-concept in accordance with the recommendations from IEC 62443.

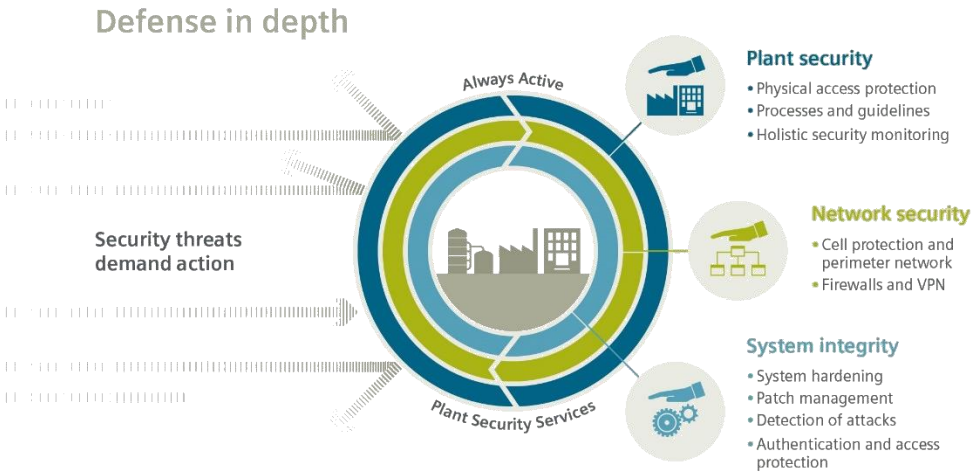

Figure 3: Defense-in-Depth concept

Defense-in-Depth is composed of multi-layered defense components and measures; plant security, network security and system integrity elements build the foundation for the industrial security concept, from the interface to management and administration systems via the operations level to the field level.

All three layers – together with the corresponding technical measures – are dealt with in detail in the Security Configuration Guidelines for Siemens DCS and SCADA systems, including physical access protection, organizational measures such as guidelines and processes, as well as technical measures to protect networks and systems against unauthorized access and espionage and manipulation. Protection on several layers and the combined effect of various protective measures lead to a high level of security, reduce the risk of successful attacks and ultimately improve system availability.

By consistently implementing a Defense-in-Depth strategy, operating companies and their security advisors take additional defensive measures to protect against cybersecurity risks and follow the general recommendation of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

ICS-CERT recommends:

- Minimizing network exposure for all control system devices. Critical devices should not have direct access to the Internet.
- Placing control system networks and remote devices behind firewalls and isolating them from the company network.
- Using secure methods such as secure Virtual Private Networks (VPN) if remote access or communication over public networks is required. Keep in mind that VPN is only as secure as the connected devices.

3 Water and Waste Water Treatment Plants

Process Overview

Essential characteristics of water supply and waste water disposal are transport over long distances as well as decentralized and widely branched water and waste water network infrastructures.

Water Supply

Water supply consists of plants for freshwater production and its distribution to connected households and industrial consumers. Raw water collection includes both surface water and well stations. The central water treatment plant cleans and processes the water to the desired quality, and finally feeds it into the water supply network.

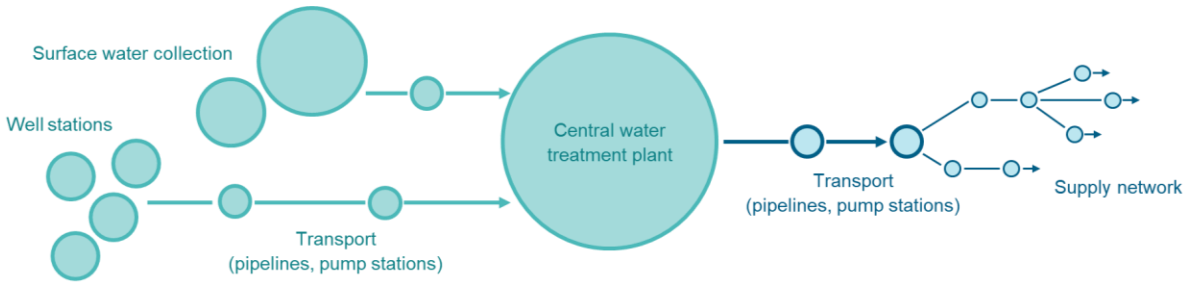

Figure 4: Water supply including water collection from different sources, central water treatment plant and transport plus distribution to the supply water network

Seawater desalination plants differ mainly in terms of the central processing; they are also covered by the following documents.

Waste water Disposal

Waste water disposal collects and purifies polluted water from households and industrial plants with subsequent discharge into natural waters, minimizing the impact on the environment. The waste water is collected by the sewage network, transported to the central waste water treatment plant by pumps and subjected to several purification processes. The cleaned water is then transported to rivers or the sea via further pumps and pipelines.

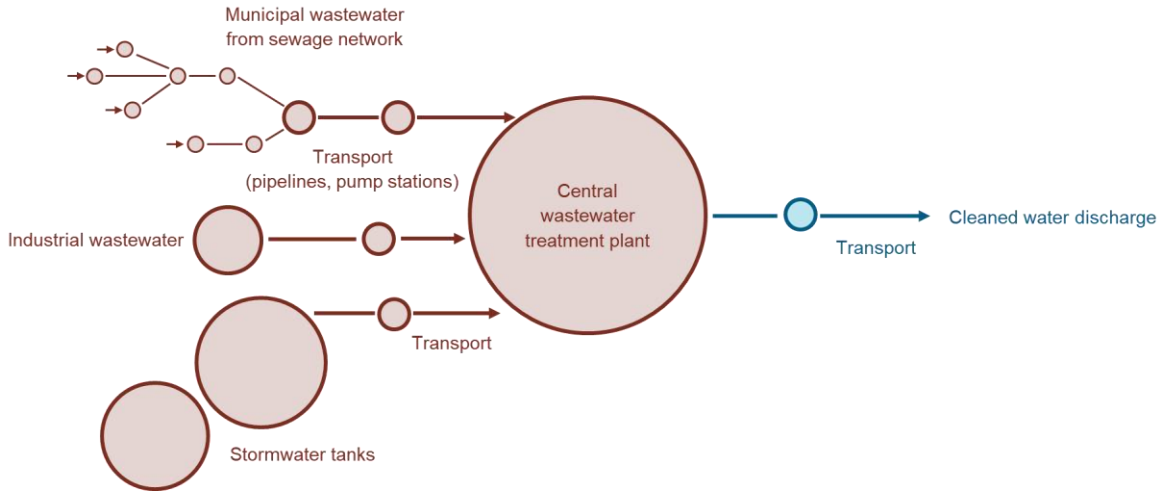

Figure 5: Waste water disposal including waste water collection from different sources, central waste water treatment plant and transport plus clean water discharge

Facilities

While the details of the processes between fresh water supply and waste water disposal differ significantly, the architecture of the automation and control system as well as the respective communication and control mechanisms are almost identical, particularly regarding safety aspects.

Industrial automation and control systems for water and waste water are very often hierarchically structured. They include a main control center, several local control rooms for individual assets such as water or waste water treatment plants as well as many on-site operator stations e.g. at each individual pumping station.

Both the central treatment plants as well as local facilities of the transport and networks are fully automated. The latter ones are typically remote-controlled substations using telecontrol technologies, partially over public communication networks.

The following section provides an overview of the facilities and functions:

Main control center

The main control center monitors and controls one or more water / waste water plants and networks that are under the responsibility of an operating association.

Main plant(s)

A main plant contains the most important process units as well as the corresponding automation and control systems (PLCs, servers, communication), including a plant-local control room for monitoring and control.

If a central supervisory main control center exists, the local control room of a main plant can be (temporarily) unmanned and remotely monitored.

External stations

There are external stations in different locations like wells, water reservoirs, pump stations etc.

Typically, external stations work stand-alone and automatically. They are usually connected via private WANs or public internet.

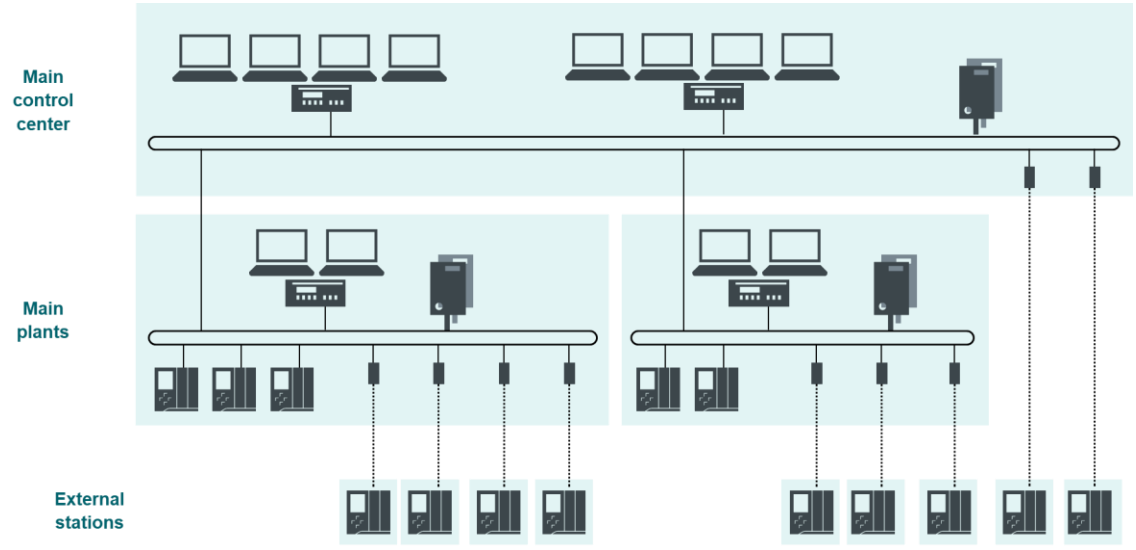

Figure 6: A typical control system architecture for hierarchical water or waste water facilities including main control center, plants with local control centers and external stations

4 Security Blueprints and Measures

Typical DCS and SCADA Configurations

Depending on the plant types and sizes as well as other influencing factors, there are different approaches for the industrial automation and control systems (IACS) of water supply or waste water disposal. Siemens offers – based on DCS / Simatic PCS 7 and SCADA / Simatic WinCC – a scalable and flexible portfolio, from small plants with local operations only, through larger water and waste water treatment plants to widely distributed networks as well as main control centers for monitoring and control of several plants of large operating associations.

The threat and risk scenarios and the resulting necessary protective measures are largely identical for the different control system approaches; they are to be presented generically below. For each control system there are also specific documents that detail the different forms of the security mechanisms.

The examples presented are based on waste water treatment including substations. While the threats and risks between water [1]and waste water can differ, the proposed security measures (access protection, data encryption, DMZ / firewalls, encrypted communication / VPNs etc.) are identical at the product and system level.

The control system architectures presented can be used as generic blueprints that provide largely standardized security architectures that have been carefully developed by Siemens automation and security experts – with a specific focus on the water and waste water industry.

The blueprints show the most common architectures for individual process units. The use of a specific configuration for the type of process unit shown is useful, but not binding. For example, all units can also be designed identically to reduce the diversity of variants [2].

[1] The Simatic PCS 7 blueprint is applicable to seawater reverse osmosis plants as well.
[2] That means, the same controller and the same switch for each machine; the same controller, the same telecontrol protocol and the same router for each remote terminal unit.

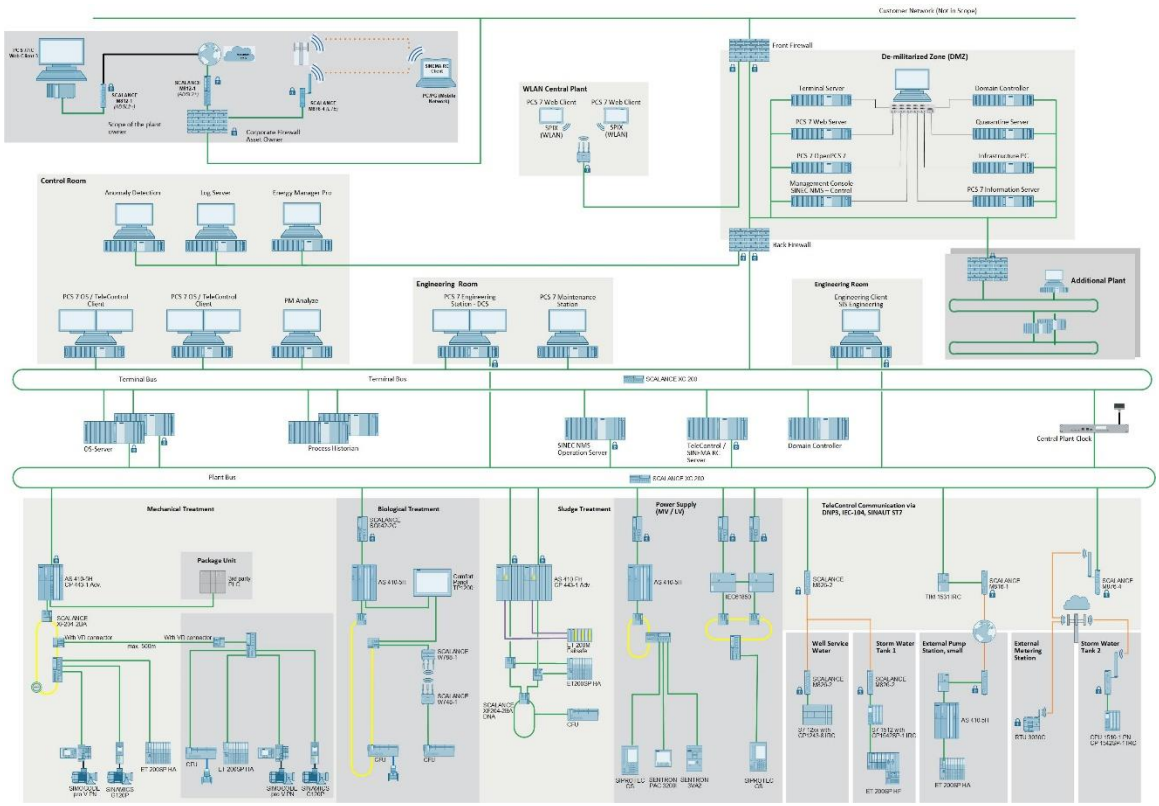

Figure 7: System architecture based on PCS 7

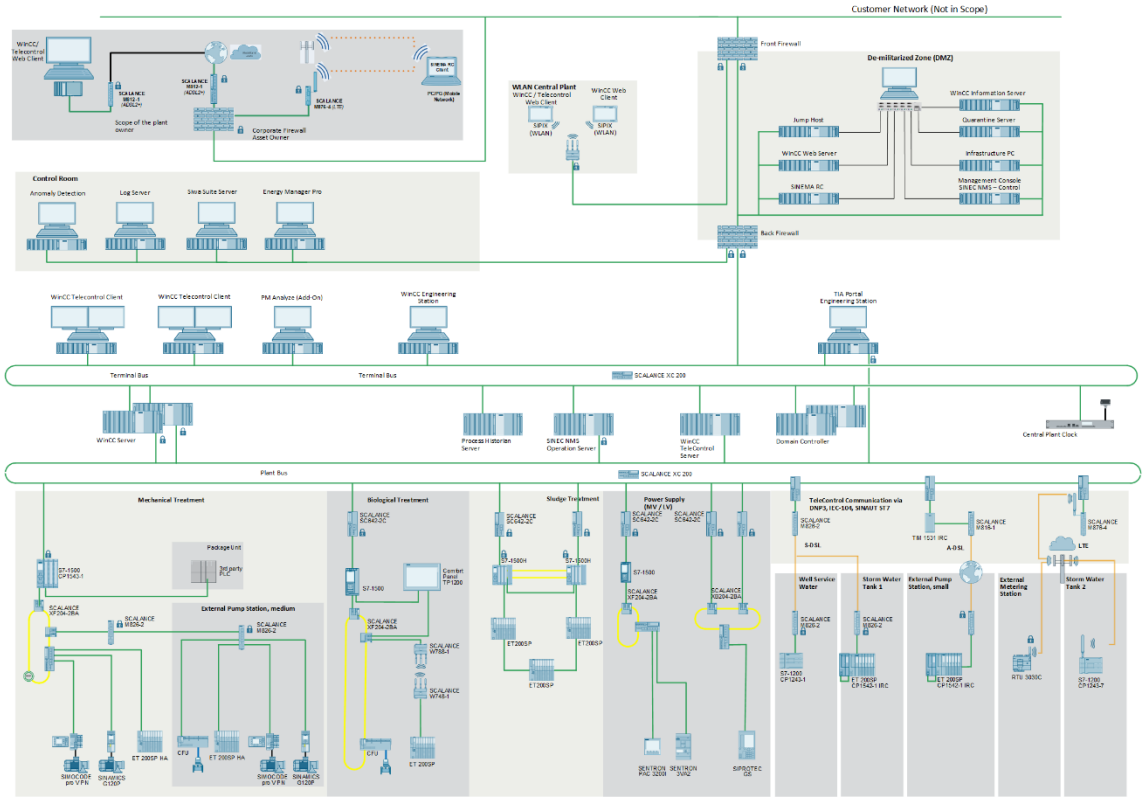

Figure 8: System architecture based on WinCC V7

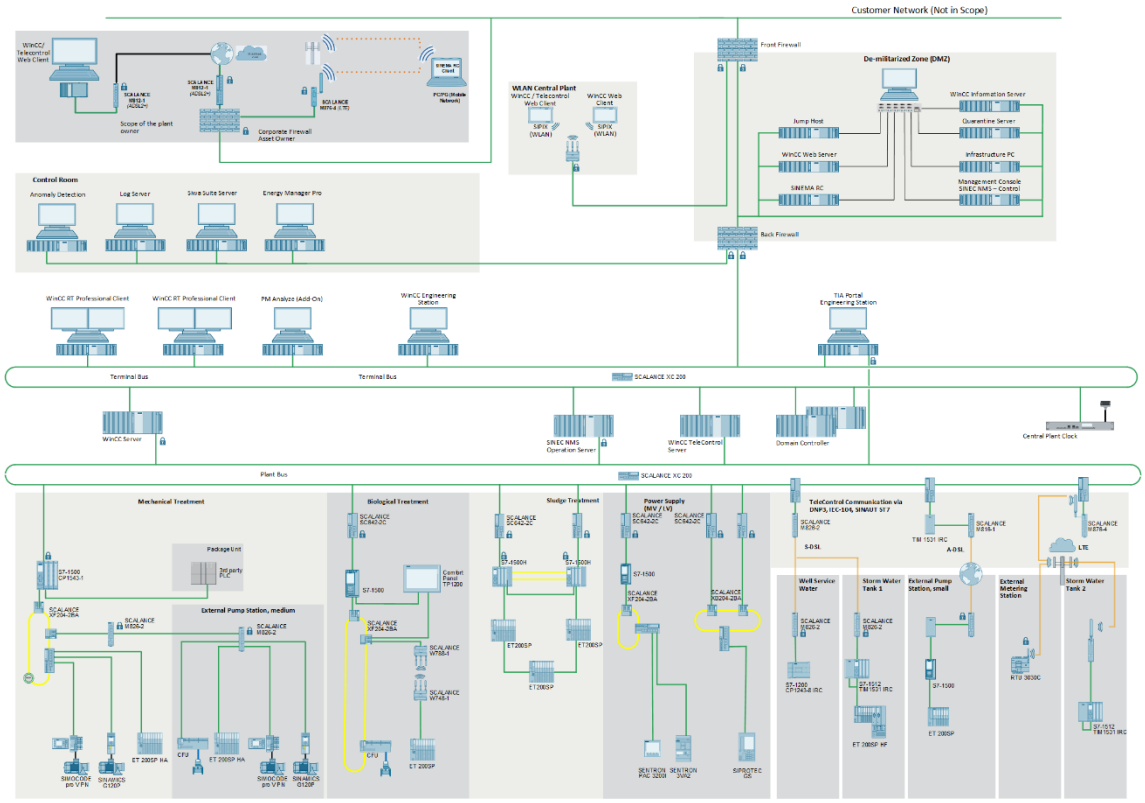

Figure 9: System architecture based on WinCC RT Professional

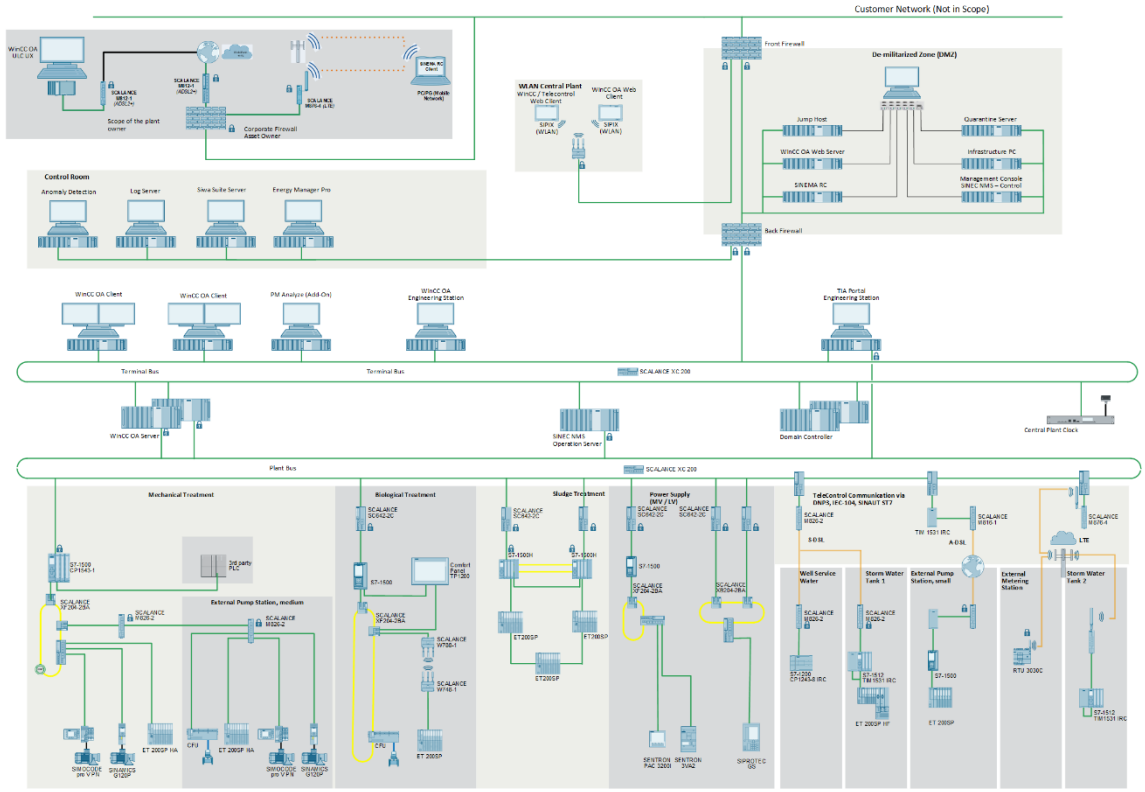

Figure 10: System architecture based on WinCC Open Architecture

Security Zones

A security zones is a physical or logical grouping of assets (PLCs, operator and engineering stations, communications devices etc.), necessary for the industrial process and control functions, that share common exposures, threats and vulnerabilities with common consequences for a security breach and therefore have common security requirements and features such as security policies, access controls.

The definition of security zones of the control system is aligned with the exposure and security requirements for the processes and functions.

For each zone, the security requirements and tolerable risk levels must be documented. The documentation includes the extent and functionality of the zone, its security level, and the threats and risks associated with it etc. It serves as a guideline for the security measures that must be applied in order to protect the assets, functions and the controlled processes

This concept provides a multi-layered security approach that takes Defense-in-Depth into account.

The main security zones of an industrial automation and control system (IACS) for water and waste water facilities are:

Control Room

The Building / Control Room Zone contains engineering and operator stations providing monitoring and control functionality. It also contains further infrastructure servers, for example network management, domain controller and time server.

In addition, it may also contain servers for data and information processing, for example quality and energy monitoring. These functions are typically less critical but can be protected using the same security infrastructure.

Central Plant

This zone contains the most important and critical subsystems of the IACS for the secure operation and the availability of the system and the process. This includes automation systems / controllers, IO systems as well as field instrumentation and drive and protection devices.

The highest level of protection applies to this zone, both physically / technically and organizationally.

Demilitarized Zone

The Demilitarized Zone (DMZ; also referred to as a perimeter network) is a subnetwork that exposes services to an untrusted, external network (in the case of IACS typically the operating company's IT network, in some cases directly the internet).

Systems and applications hosted in the DMZ have access to both internal and external networks and are therefore most exposed to attacks. The front- and back-firewalls restrict the connections to the minimum required.

External / Remote Stations

This zone comprises widely distributed, external / remote stations, connected via private WANs or public network infrastructure including radio connections and telecontrol technologies. Since the stations are usually located in unsupervised and partially publicly exposed areas, security requirements are higher and include physical access protection and monitoring against tampering. In emergencies, it is possible to temporarily operate individual substations locally without network connection to the main control system.

In principle, the communication from the Central Plant Zone to the External Stations – the so-called Conduit – would have to be regarded as a separate security zone, which includes the public network infrastructure. As the latter is not the responsibility of the IACS vendor or solution and service provider but of the operating company and the internet service provider, this was not considered here.

WLAN Access

If – especially for service and maintenance activities – mobile devices are used in the plant area, wireless access is required.

Because wireless connection may be exposed to the public communication infrastructure, devices in this zone are considered as "untrusted".

Corporate IT / Internet

External zones are not operated by the IACS. Devices in these zones have lowest security level, are exposed to the internet and most likely to be attacked. They are considered as "untrusted", so all communication is restricted to connections to the DMZ.

Security Cells

A process unit is a physical or logical grouping of assets, the associated process of which can run for a certain period without being connected to the rest of the plant, i.e. a process unit must remain independently operational for a while. A process unit can correspond to a security cell if there are appropriate security policies and measures in place, that include control of physical access, access to computer and networks with appropriate authentication and authorization as well as monitoring and control of the process.

The strategy of dividing plants into security cells increases the overall availability of the entire system, as this can limit threats and security-incidents to the immediate environment, i.e. to one cell.

In water and waste water facilities, security cells will typically correspond to individual process units such as mechanical and biological treatment in the central plant as well as sewage network segments and pump stations in the external / remote stations.

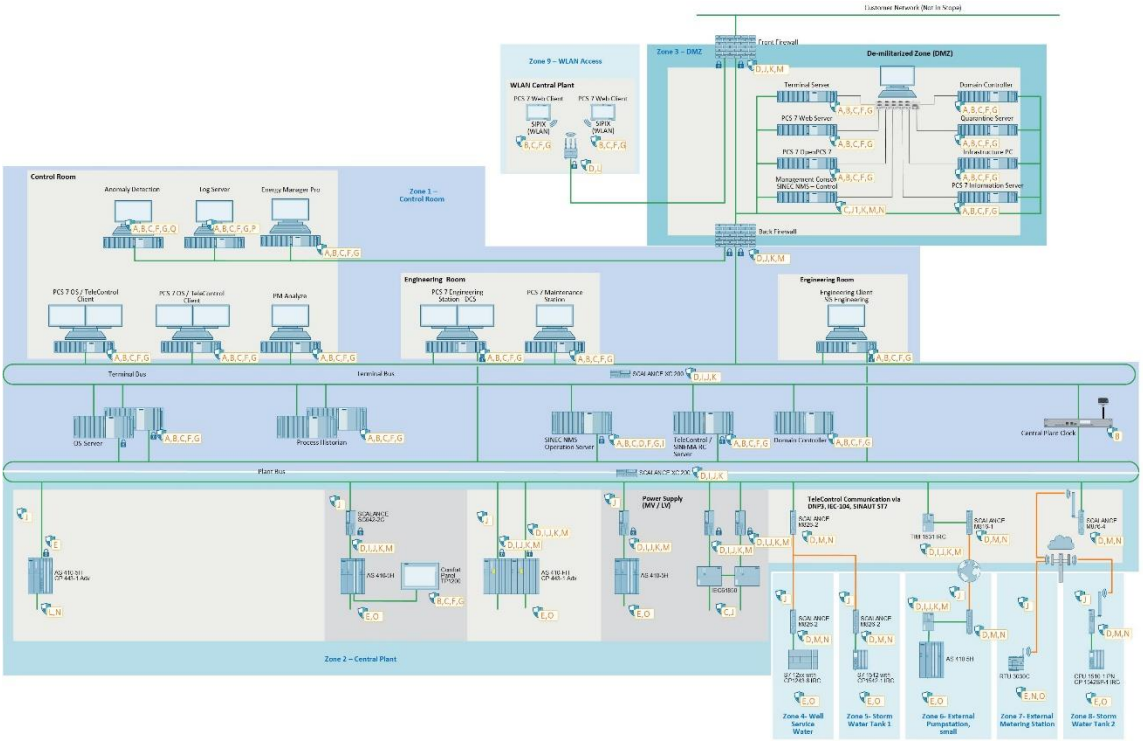

Figure 11: Security zones / cells and industrial security measures (example for PCS 7)

Threats and risks

All security-related measures are derived from a detailed threat and risk analysis (TRA) in accordance with IEC 62443.

This document is based on a generic TRA that takes standard water and waste water plants and typical operating environments into account.

Based on these assessments, special blueprints (reference system architectures) were developed to implement generic security measures, with a focus on protection of networks and system access.

However, for each specific installation, a specific TRA is recommended, which is normally required. TRA, control system architecture and measures to be implemented can then be based on these general considerations in order to minimize the adaptation effort.

The following main threats have been identified and have to be assessed considering protection goals and the intended operational environment.

Physical Access

Physical access to the plant, the network and parts of the plant is the most critical threat. Uncontrolled access would mean full control over the plant.

The geographically distributed remote stations cannot be easily secured or monitored through regular physical presence. Physical access is typically restricted by similar measures as in the main plant. In addition, remote stations are typically designed to work stand-alone and automatically.

Introduction of malware via removable data storage media

Removable data storage media are a common gateway for malware. If an employee is not aware of the risk, he/she can connect a (personal) USB stick to a PC in the automation or office network and possibly infect the system. The risk of introducing malware in this way is widespread because security measures in the private sector are generally extremely weak.

Intrusion via remote access / internet

Widely distributed control systems require access via remote communication over public networks, including wireless radio communication, which can be exploited for cyber-attacks. In particular, the front firewall to the internet is likely to be attacked. Remote access can be a risk if it is not properly designed and managed.

Human error and sabotage

Lack of awareness or ignorance regarding the high risk of certain behavior are the most common reasons for internal attacks. Clearly defined guidelines are often deliberately ignored since they require slightly more effort.

In larger companies, there can be a significant difference in the IT security know-how of employees in various departments.

Dissatisfied employees can attack the operation in a targeted manner.

Technical malfunctions

Software and hardware errors can never be entirely excluded. Hardware defects due to harsh environmental conditions (dirt, temperature, moisture, etc.) are likely to occur if no proper precautions are taken and can lead to system failures or malfunctions.

Industrial security portfolio and measures

The blueprints for industrial automation and control systems provide key security features via secure products (device hardening, ...), at system level (security zones and cells, zone and cell isolation and protection via firewalls, ...) as well as a solid basis for further measures to be implemented by the IACS solution and service provider and/or end customer (user and roles and accounts, network management, VPN tunnels over public networks, security and virus pattern management, ...).

The following list provides an overview of available security measures:

1. Operating system hardening, e.g. via dedicated operating system build, security policies

   Central operating system and IACS patch management

   Central antivirus pattern management, endpoint security, application whitelisting
2. Central firmware patch management for SCALANCE network and security devices via SINEC NMS
3. SIMATIC Controller firmware update
4. Central identity and access management via Windows Domain Controller for Windows user roles and accounts, password policies, aligned IACS roles and accounts via SIMATIC Logon
5. Operating system backup and restore
6. IACS project / data backup and restore via SIMATIC Manager on ES (backup server is project specific)
7. Central network and network security and device management and backup via SINEC NMS
8. Security zones and cells, zone and cell protection via network segmentation, firewalls

   Encrypted communication between various security zones / cells

   Restriction of IP addresses, restrictions of services / ports, packet inspection for all firewalls
9. Encrypted IPSec VPN for remote communication
10. Encrypted WLAN, layer 2 tunnel, WLAN iPCF
11. Field Interface Security for S7-410 and S7-1500: communication for dedicated field device interfaces restricted to IO operation; other communication requests rejected
12. Logging of network communication; for SCALANCE devices centrally via SINEC NMS
13. Central, passive anomaly detection for communication based on deep packet inspection
14. Quarantine server as central data transfer point, e.g. for configuration or engineering data

5 Management of Industrial Security

Most security and protection goals can only be achieved through a combination of technical and organizational measures.

The latter include establishing a security management process in the organization. The first step in determining required actions is to analyze and assess the relevance of specific threats and risks. The significance of an identified risk depends on the effects – for example on the water supply – associated with the likelihood of occurrence. Errors in the threat and risk analysis (TRA) have a direct impact on the achievement of the security and protection goals. This can lead to ineffective, insufficient or expensive measures. It is also possible that vulnerabilities are not being identified and corrected.

When a new facility is being planned, a threat and risk analysis should be carried out in a very early planning phase. This is the perfect time for risk identification, classification and definition of an implementation plan for cybersecurity measures. According to this approach, a "secured by design" and more cost-effective concept can be achieved.

Figure 12: Risk assessment decision table for use in conjunction with a prior plant-specific risk analysis. The risks involved must be reviewed regularly

The risk analysis provides security and protection goals that form the basis of specific organizational and technical measures. The measures must be reviewed or tested following implementation. The risks must be reassessed on a regular basis and in case of technical or organizational changes affecting the original TRA.

The blueprints, including the security measures presented above, are based on thorough threat and risk assessments for "generic" water and waste water facilities; for individual facilities and solutions, specific assessments and appropriate adjustments of the blueprints and measures are required.

6 Industrial Security throughout the Lifecycle of Water and Waste water Plants

A few years ago, security for industrial facilities focused on protecting peripheral controls. New threats appeared to be abstract and theoretical, and few industrial end customers and operators were interested in these issues.

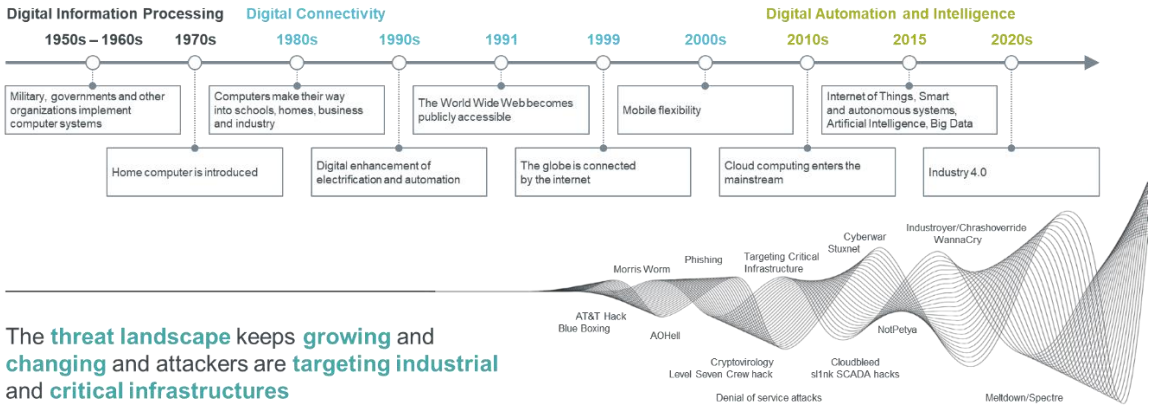

Figure 13: Cybersecurity incidents in industry and critical infrastructure

Media reports on security incidents have attracted increased attention. It became clear that industrial automation and control systems and infrastructure facilities were also on the target list for cyber-attacks. Vulnerabilities and possible consequences can be serious, therefore the defense against the attacks – along with the advancing digitalization – is an indispensable factor.

Siemens – as vendor and single-source supplier of industrial automation and control systems – is well positioned to support system integrators and operating companies in coping with these increasingly demanding challenges. Risks can be successfully minimized by taking security requirements and measures into account during the design, development and operation phase and by implementing a holistic security concept.

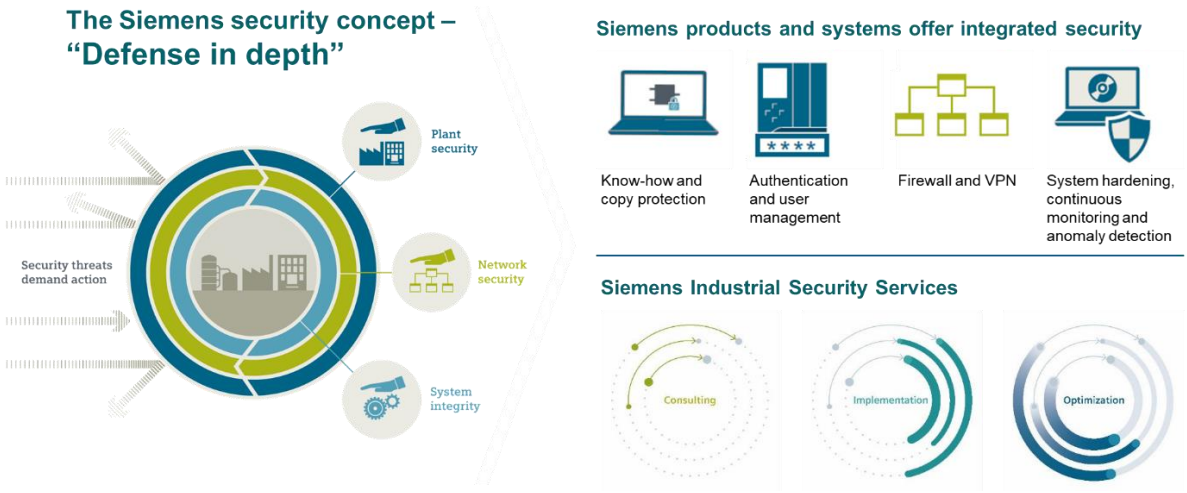

Figure 14: Industrial security portfolio: concept, products and services

However, engineering and technology alone are not enough –processes and organizational measures must also be implemented and need to be continuously adapted.

With many years of expertise, Siemens is also a strong partner in the field of industrial security for water and waste water facilities. Siemens offers a broad portfolio of security products and services as well as an effective industrial security concept.

Industrial Security Services

Dedicated security services can support consultants, system integrators, EPCs and operating companies with the design and operation of secure automation environments. This assisted process extends from an assessment of risks, organizations and existing measures to the design and implementation of a secure automation operation onto the continuous monitoring and optimization of the industrial security status.

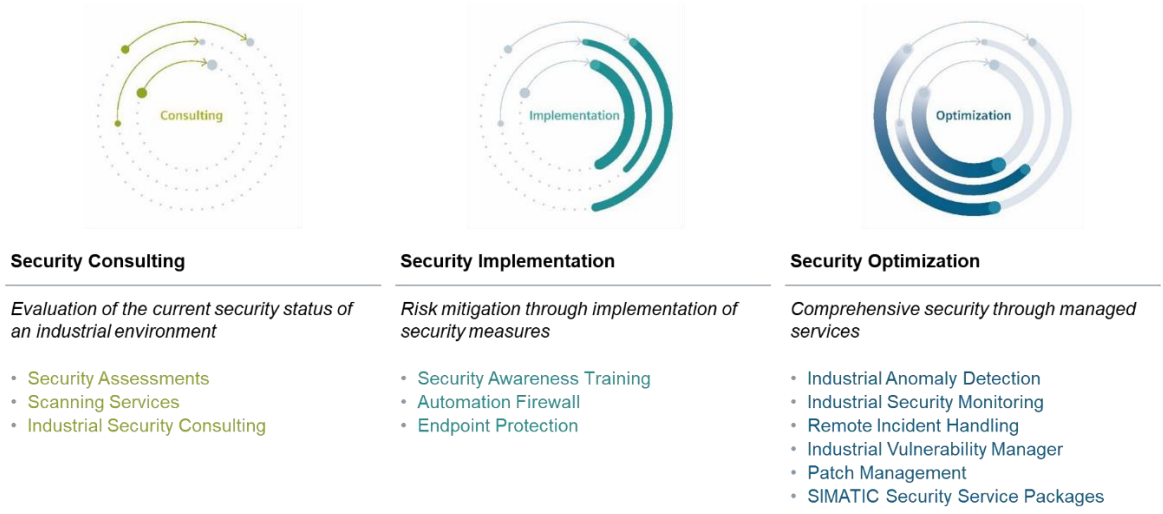

Figure 15: Portfolio around industrial Security Services

Security Consulting

The consulting phase creates transparency of the security status of a plant and identifies vulnerabilities and risks. Necessary measures are summarized in an action plan, showing how the security status of a plant can be raised to a desired level. Example are the IEC 62443 or ISO 27001 assessments, in which actions for a specific water or waste water treatment plant are specified in order to comply with the relevant parts of the standard. This assessment can also be used during the planning phase to identify required actions and measures for the desired security level.

Scanning services can be used to achieve transparency on existing automation devices, in combination with security monitoring or vulnerability management, to continuously check against pre-defined security levels.

Figure 16: Siemens product development process, IEC 62443-4-1 TÜV certified

Security Implementation

The next step is to implement the proposed measures to address the identified weaknesses. Resources include hardware (such as firewalls) and software (such as antivirus, whitelisting and anomaly detection). Clear instructions and guidelines on IT- and OT-security are also included.

Most of these measures have already been considered during the phase of the blueprints presented above.

Security solutions can only work properly if employees have been trained accordingly. Employee awareness and comprehension should be continuously promoted through workshops, web-based training or equivalent measures.

Security Optimization

Another key aspect of the Siemens service in this area is supporting customers in the continuous monitoring of industrial plants as well as managing vulnerabilities and patches.

The Defense-in-Depth strategy creates a suitable basis for optimizing security in automation environments. Siemens Industrial Security Services provides support for companies in the implementation of appropriate measures. The comprehensive range of services, from security assessments up to continuous monitoring helps customers to reduce the security risk associated to their water or waste water treatment plant or water networks.

7 Conclusion

Considering water supply and waste water disposal as critical infrastructure implies the need to develop a security strategy and take countermeasures to continuously protect and secure the operation of water and waste water plants and networks.

Siemens provides all required portfolio elements to develop a security strategy and to implement the desired security level with the right products, systems, solutions and services.

Even though most of the current standard enforce only large facilities to act now and be audited on a regular basis, the relevance to small and medium sized water and waste water plants and networks is of similar relevance and should be implemented based on the same comprehensive methodology.

If the appropriate tools are used, security of water and waste water plants and networks can be continuously monitored, and attacks can be prevented, analyzed and documented.

Please contact your local Siemens sales representative to take the next important step together.