Industrial Network Security Architecture

Table of Contents

1. Introduction to Industrial Network Security Architecture

Over the past decade, the world of industrial automation has adopted Ethernet as a universal communication standard - to the detriment of previous RS232/485 serial communication systems. The reasons for this are multiple: Ethernet has been shown to maintain the availability and real-time requirements of the communication between industrial control systems (ICS) and the rest of the devices, in addition to providing a vendor-independent ecosystem. Moreover, Industrial Ethernet networks allow for transparent connections with external networks at speeds several aorders of magnitude greater than traditional communication systems.

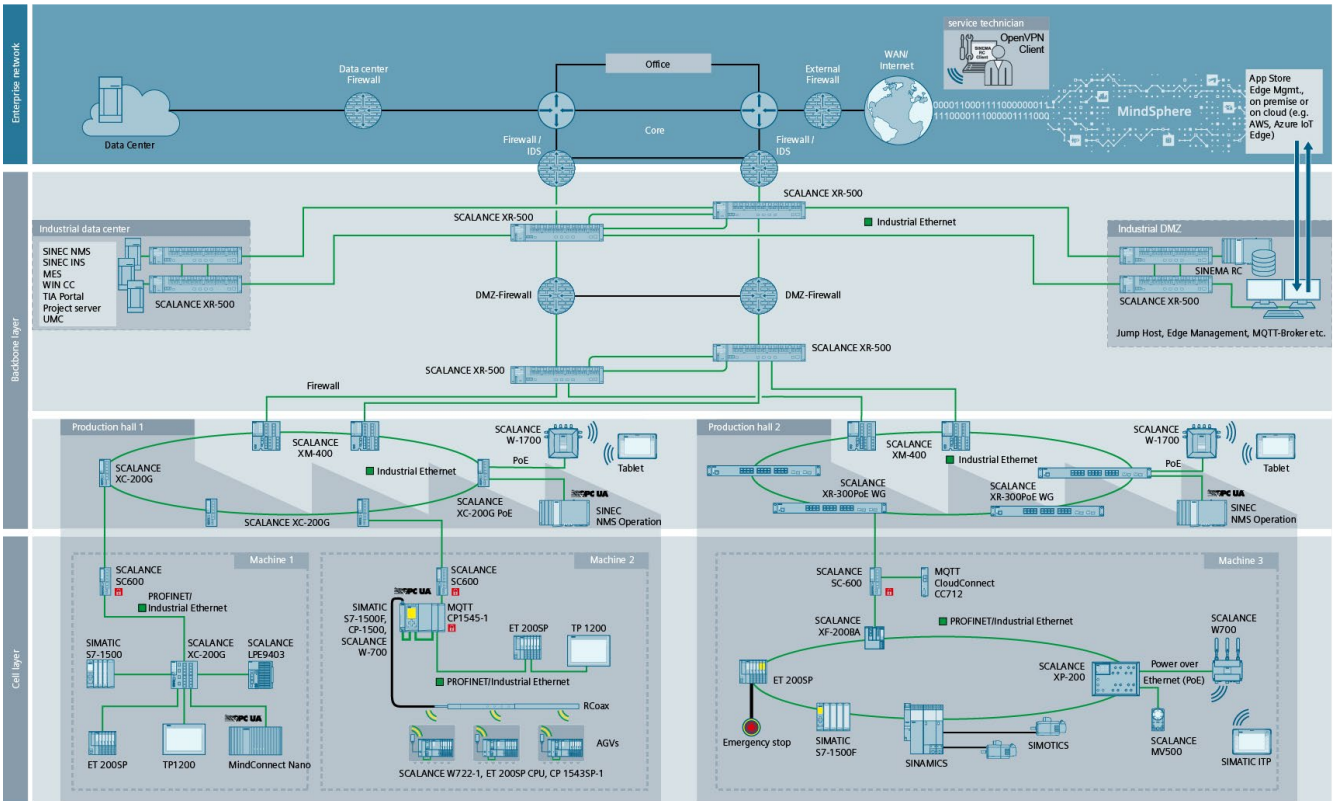
The greatest number of opportunities and threats (particularly security threats) can be found when connecting to systems outside the production operational area – such as the internet or third-party networks, for example. Professionals must take these topics into account when designing an ICS that is to be a part of the Industrial Internet of Things (IIoT) environment.

The Industrial Network Security Architecture provides a network reference guide for both Operational Technology (OT) and Information Technology (IT) professionals, who collaborate to provide services such as:

- Connectivity to previously isolated machines
- Remote access to machines in the factory
- Processing of production data via edge and cloud computing
- Providing a secure network design from cell to industrial backbone level

A secure network is a network that has security measures in place that help protect it from attackers. Of course, there is no such thing as an entirely secure network. However, taking the proper steps helps keep a network secure. This architecture is a template based on experience gained from multiple customer projects and industries.

Figure 1: Network architecture application example



The Industrial Network Security Architecture is based on the recommendations of international industrial security regulations, where it is emphasized that organizational processes for cybersecurity are as important as the technical solutions. Most international standards, such as NIST and ISA/IEC-62443, apply the concept of multiple barriers detecting and preventing a threat that may endanger critical information, goods to be produced or the integrity of data.

In order to implement security on any current industrial automation project, it is necessary to follow a holistic approach combining several solutions that support each other. A cybersecurity plan includes the following steps and procedures:

1. Network segmentation:

It is necessary to divide the plant network into separate protected zones, following criteria that is either functional or technical. This limits a failure to a particular zone of the network and prevents an uncontrolled spreading across the plant and operation. OT and IT staff must work in close cooperation to design a zone-based architecture that best fulfills both cybersecurity and production requirements.

2. Asset management:

Network operators often face the challenge of knowing their installed base of factory assets. This is a prerequisite for the security concept. Therefore, it is strongly recommended to use a Network Management System (NMS) capable of automatically detecting all active devices. Based on this, the NMS provides a complete asset list with additional information for each device, e.g. device name, serial number and firmware version.

3. Network protection:

In order to properly divide the network into zones, it is necessary to define communication relations between the different zones of the factory. Based on these relations, policies must be implemented on each firewall protecting a zone. Additional insights can be gained by using solutions capable of monitoring traffic in real time, detecting anomalies, and reporting incidents.

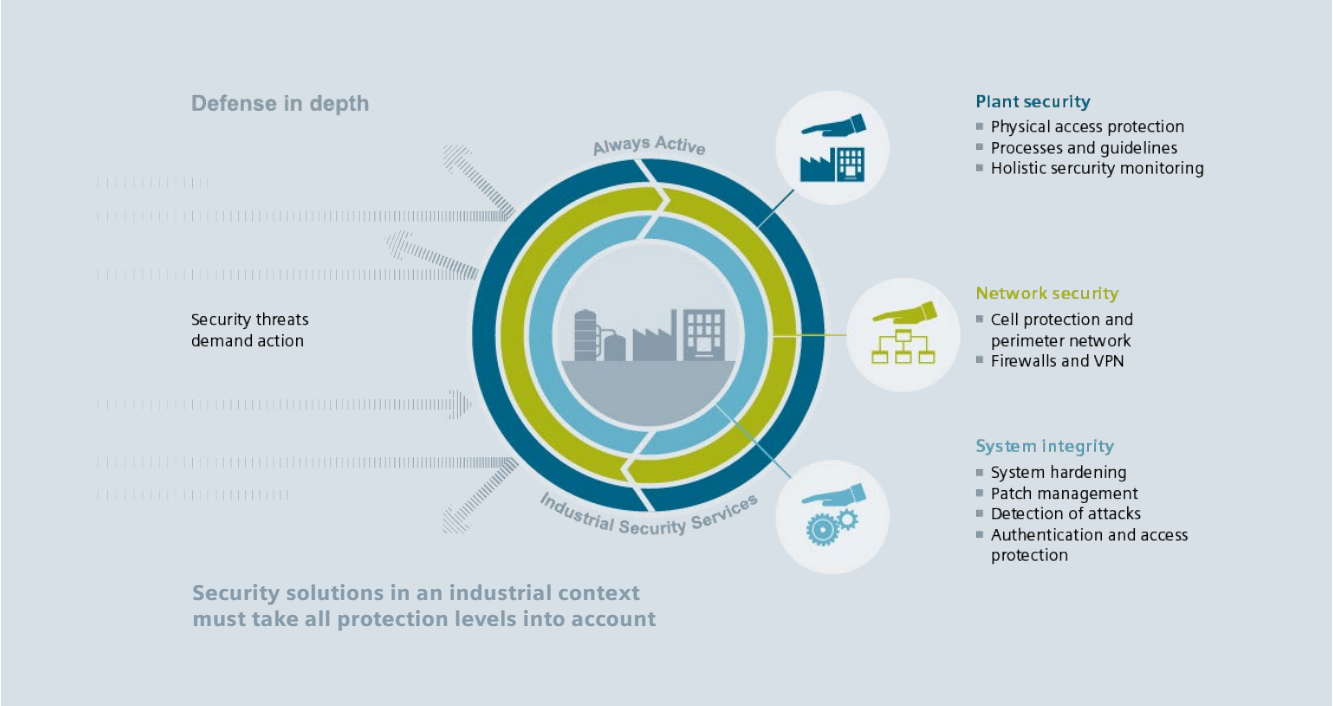
4. Secured remote access management:

For ICS maintenance, diagnostics purposes, patching and updates different suppliers must have access to OT level cells from outside the factory via the internet or from other untrusted areas unrelated to production. This requires a remote solution, establishing a secure connection out of the cell towards a rendezvous server to be compliant with the protection measures and security policies. Each remote user has its own access rights via encrypted communication. Manual management of this access is not state-of-the-art and subject to failure. Therefore, it is recommended to use a centralized secured remote access and user rights management solution (User Management Component) that integrates with the corporate access policy tool.

5. Training and awareness:

The biggest threat to the security of a facility is lack of knowledge and lack of information. The cybersecurity plan must always include employees, business partners and visitors, regardless of their role and role within the company. Trainings are needed to regularly inform people about plant-specific security measures, company cybersecurity policy and to prevent security gaps.

Figure 2: Defense in depth concept



Security requirements overview:

Implementing the necessary measures arising from a cybersecurity plan inside a facility where many IACS are present can be a difficult task. Besides a holistic approach covering the entire facility, it is also important to define detailed measures for each and every asset, including staff. The result is a set of procedures and measures that continuously and holistically monitor and protect the assets and production. Based on recommendations from NIST and the IEC organizations, it is required to apply a layered set of measures at all plant levels following a concept known as defense in depth. This provides a multi-faceted concept that gives your system both all-round and in-depth protection. The failure of a single measure will not cause the failure of the entire system. Before implementing any measure, a detailed risk analysis needs to be carried out in collaboration with the management of the company, IT and OT. The concept is based on plant security, network security and system integrity – according to the recommendations of ISA/IEC-62443, the leading standard for security in industrial automation.

Plant security:

Plant security uses a number of different methods to prevent unauthorized persons from gaining physical access to critical components. This starts with conventional building access and extends to securing sensitive areas by means of key cards. Comprehensive security monitoring leads to transparency with regard to the security status of production facilities. Thanks to continuous analyses and correlations of existing data and through comparison of these with threat indicators, security-relevant events can be detected and classified according to risk factors. On this basis and through regular status reports, plant owners receive an overview of the current security status of their production facilities, enabling them to react swiftly to threats.

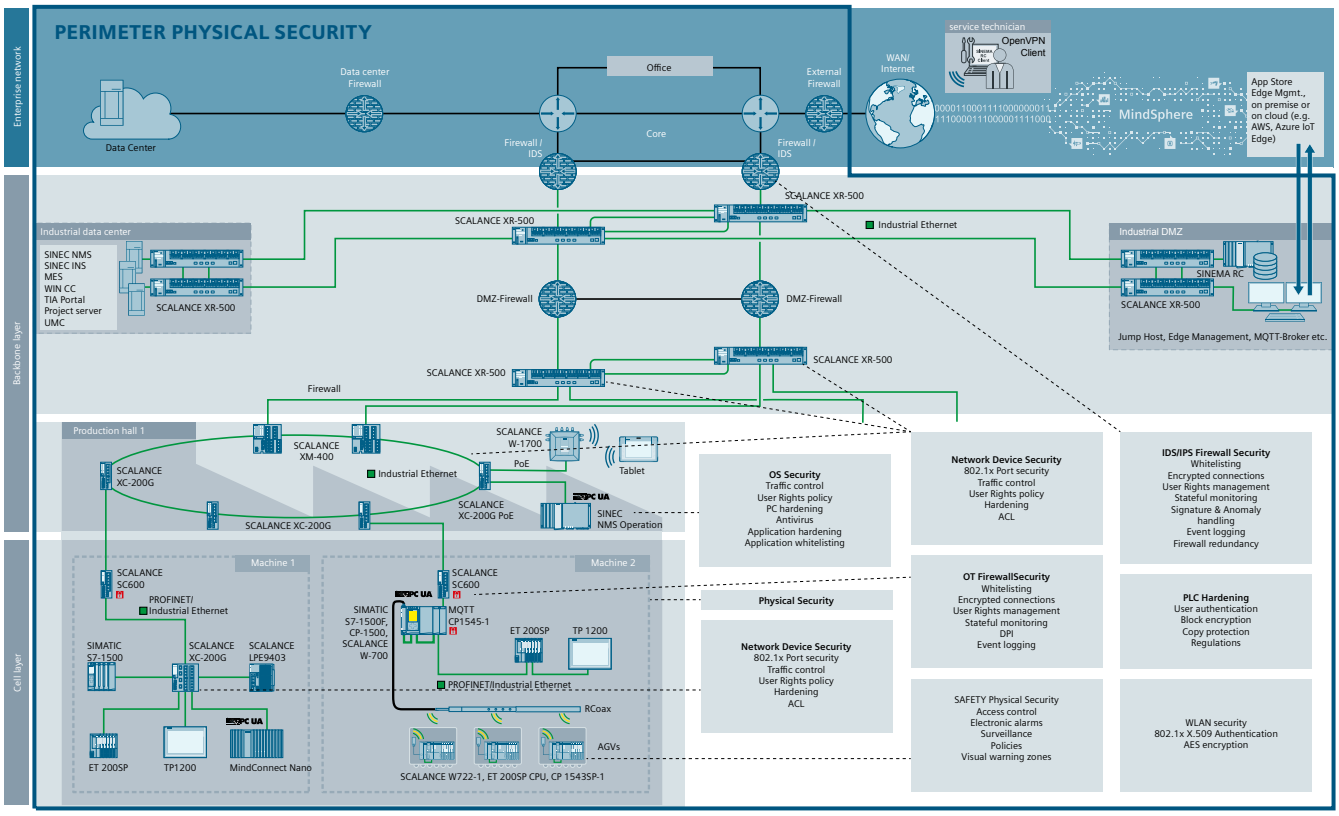
Network security:

Network security means protecting automation networks from unauthorized access. This includes the monitoring of all interfaces such as the interfaces between office and plant networks or the remote maintenance access to the internet. It can be accomplished by means of firewalls and, if applicable, by establishing a secured and protected industrial "demilitarized zone" (DMZ). The industrial DMZ is used for making data available to other networks without granting direct access to the automation network itself. The security-related segmentation of the plant network into individually protected automation cells minimizes risks and increases security. Cell division and device assignment are based on communication and protection requirements. To be protected from data espionage and manipulation, the data transmission must be encrypted by using a Virtual Private Network (VPN), for example. The communication nodes are securely authenticated.

System integrity:

The third pillar of defense in depth is the safeguarding of system integrity. Here, the emphasis is on protecting automation systems, control components, and communication components as well as SCADA and HMI systems against unauthorized access and on meeting special requirements such as know-how protection. Furthermore, system integrity also involves the authentication of users, access and change authorizations, and system hardening – in other words, the robustness of components against possible attacks.

Figure 3: Security measures in different parts of the network



2. Network Segmentation

Although in theory, the use of wired and wireless LAN allows implementation of a transparent network with a large number of devices, it is recommended to segment in isolated and independent areas, usually by means of layer 3 security devices (firewalls) due to the following reasons:

- Availability: A physical failure in a device, configuration or a spike in traffic is restricted to a local area, which avoids a larger incident across the plant.

- Security: Based on the defense in depth concept, all areas are protected by firewalls, which prevents a security breach from affecting the whole plant network.

This is also reflected within ISA/IEC-62443-3-3 SR5.1 RE1: "SR 5.1 RE 1 – Physical network segmentation:
The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks."

For the segmentation of the network where the IACS are located, the following criteria must be considered:

a) Safety Instrumented Systems and Functions (SIS & SIF):

Safety in automation environments covers applications, which could do harm to personnel and assets. The presence of a safety-related ICS requires isolation from the other equipment in the plant network.

b) Automation real-time communication:

The communication protocols needed for industrial automation are exchanged between controller and device, with strict requirements for delay (down to microseconds) and jitter. Therefore, devices belonging to the same automation application and ICS must be in the same zone to ensure the required deterministic communication.

c) Functional relationship:

Typically, OEMs deliver complete machines to the end customer. If several machines belong to the same production process, they should be grouped in a dedicated zone with the same security requirements.

d) Risk:

Devices identified as critical based on the risk assessment recommended by ISA/IEC-62443, must be assigned to their own security zone. Devices with the same security level can be grouped and connected into the same zone.

In ISA/IEC-62443-3-3, the security level 2 (SL 2) is defined as "Protection against intentional violation using simple means with low resources, generic skills and low motivation". To reach SL2 regarding network segmentation, a physical separation of the industrial network (OT) from the enterprise network (IT) is required (SR5.1 RE1).

Based on this requirement, the following architecture is recommended:

The industrial network consists of multiple layers highlighted in the figure 4.

Cell layer:

The topology of the cell layer depends on the required application. For applications without redundancy requirements line, tree or star topologies can be deployed. If the availability of the process is critical, it is necessary to deploy a redundant topology such as a ring. This type of topology requires the use of managed switches that support redundancy protocols. The recovery time in case of a network failure must be considered for the ICS communication parameter setup to enable continuous production. Usually, all devices within a cell belong to the same machine or functional group. If the connection of additional non-automation equipment (e.g. WLAN devices) to the same cell cannot be avoided, a VLAN separation of these devices is recommended. This additional VLAN must be secured by the cell protection firewall. The cell protection firewall acts as a secure gateway to the higher layer networks, both for application related communication to the industrial data center, industrial DMZ, and for remote access via VPN connections.

Aggregation layer:

The main purpose of the aggregation layer is to provide connectivity between the cell and backbone layer. The network devices present at this level must be able to transfer traffic at rates of several gigabits per second with high port density. A redundant topology at the aggregation layer is recommended. Multiple cells and machines related to the same production process are grouped into a dedicated aggregation network. Besides the cells, additional devices like wireless access points and network monitoring systems are connected.For the connection of cell protection firewalls, wireless access points, and management purposes, dedicated VLANs are recommended at the aggregation layer.

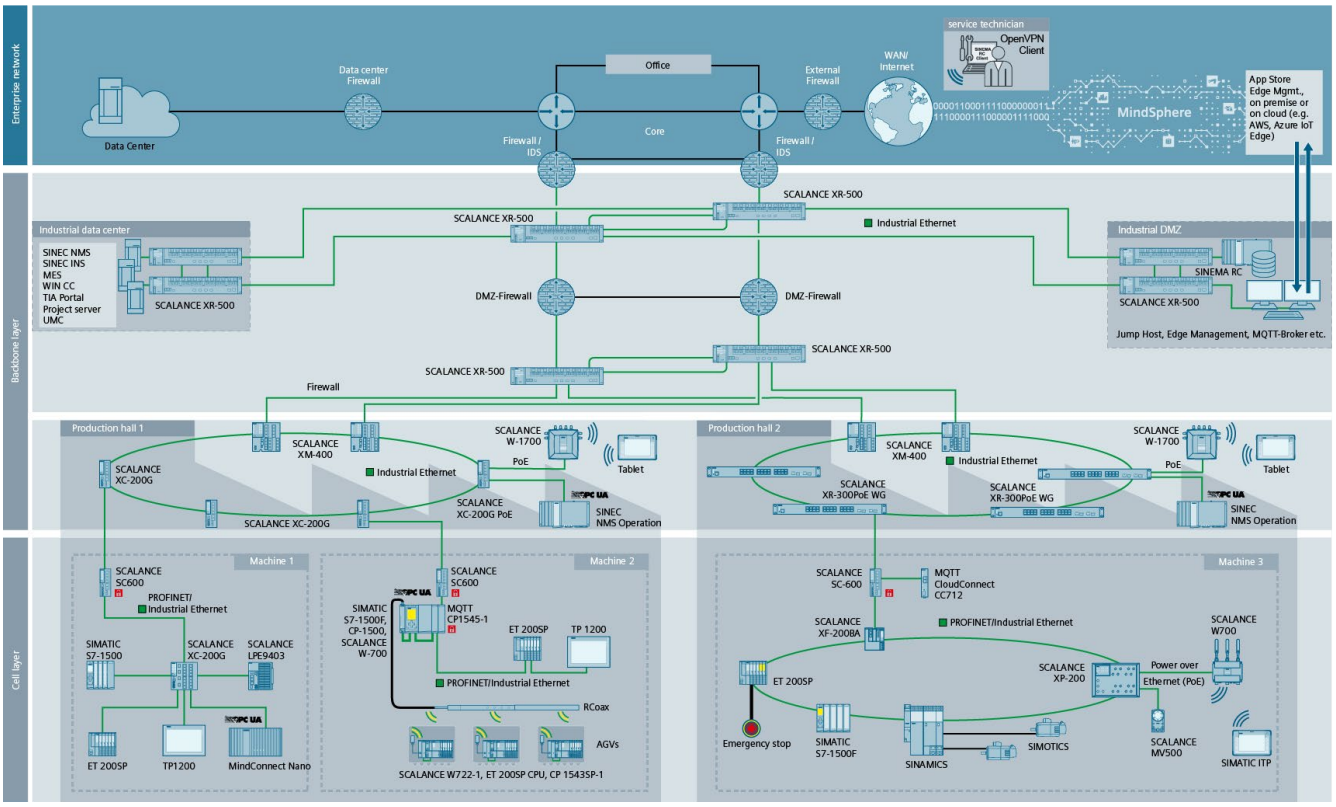


Figure 4: Layers of the industrial network

Backbone layer:

The backbone layer is the central connection point of the industrial network. It provides the redundant connectivity to the aggregation layers, the industrial data center, the industrial DMZ and the enterprise network. The devices in the backbone are Layer 3 Ethernet switches capable of static or dynamic routing. It is mandatory to use firewalls between the industrial backbone, industrial data center, industrial DMZ and enterprise network.

Industrial data center:

Industrial automation applications, engineering tools (TIA) and management systems are hosted in a dedicated industrial DMZ, the industrial data center. Here too, a consistent security concept requires segmentation in this zone. To avoid direct connections from the OT to IT and vice versa, these services and applications are placed in the industrial DMZ. The firewall controls the access between the different zones. All direct access requests from the enterprise network to OT or vice versa must be denied by default, primarily necessary to access a proxy device inside the industrial DMZ and from there, initiate an access request to the OT network. This multi-step approach increases the security and limits the attack exposure of the IACS. Depending on the industry and the risk assessment results, the industrial DMZ offers a central secured location for all network services and tools for the whole plant, such as user management servers, SCADA, Historians, MES, Engineering Stations, synchronization servers, backups, antivirus and patch and update services.

3. Asset and Network Management

The number of connected devices in industrial networks is increasing rapidly with the progress of digitalization and the Industrial Internet of Things (IIoT). A higher number of connected devices increases the exposure to cyberattacks. Ensuring an up-to-date, real-time inventory of all network devices and their configuration becomes crucial to support the process of root cause analysis in case of an incident. In sections SR2.8 and SR7.8 of the ISA/IEC-62443-3.3, the requirements for auditing and monitoring the assets can be found:

"SR 2.8 – Auditable events:

The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result."

"SR 7.8 – Control system component inventory:
A control system component inventory may include but is not limited to component ID, capability and revision level. The component inventory should be consistent with the system under consideration. A formal process of configuration management should be deployed to keep control of the changes in the component inventory baseline."
A reliable central Network Management System (NMS) provides a common database for the entire OT infrastructure that ensures full visibility of assets, provides the physical topology of the network, facilitates the diagnosis of network problems, controls the flow of information and provides user access control between the different zones of the IT and OT network. This system should be based on the ISO Network Management framework model FCAPS (fault, configuration, accounting, performance, security management), which describes and categorizes network management tasks. The Siemens implementation of SINEC NMS is based on one central control and one or more local operations.

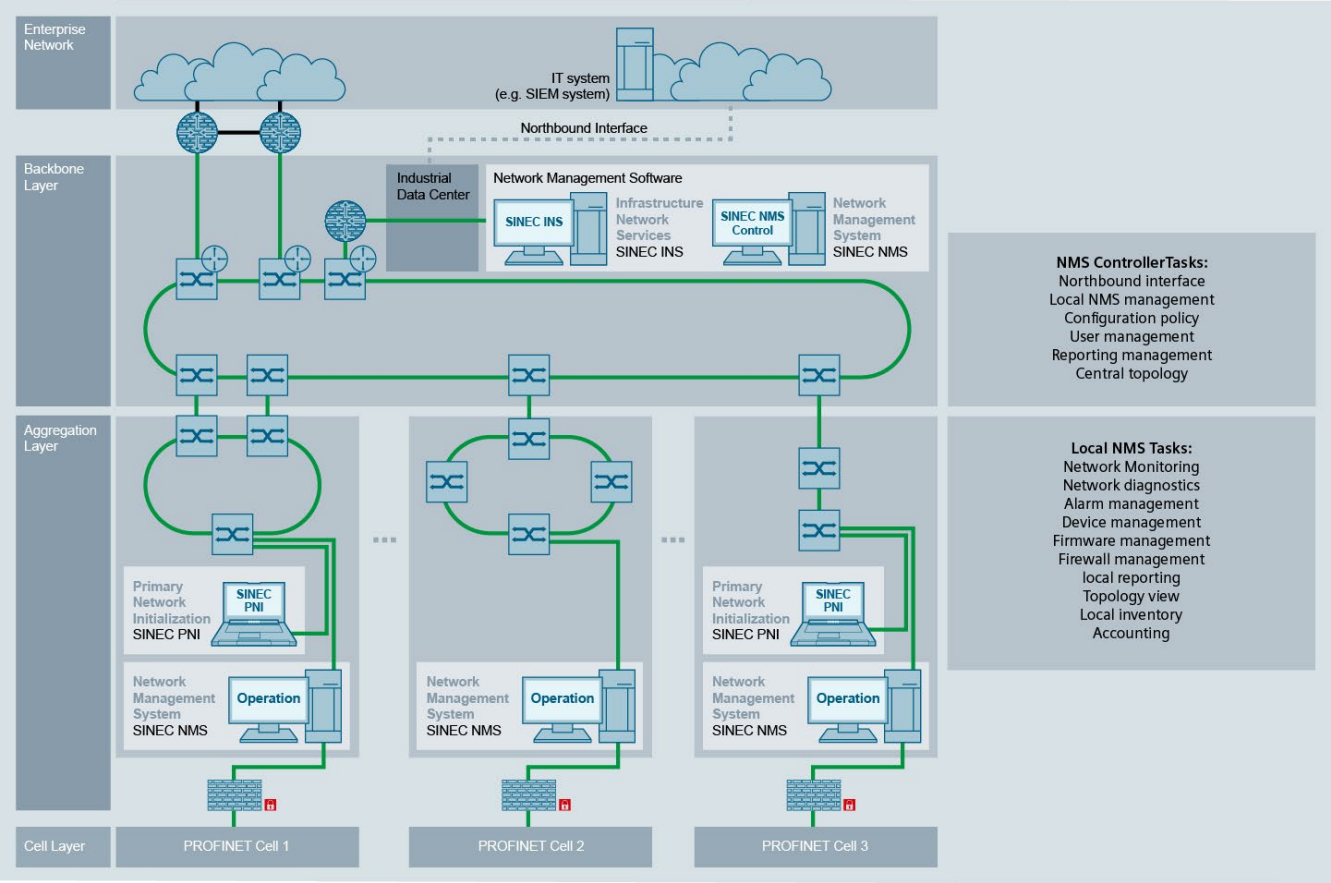
SINEC NMS Operation is hosted locally in the industrial data center of the OT network. NMS Operation discovers and interacts securely with the devices defined by the network administrator using several protocols, e.g. SNMP, which supports encryption and authentication. NMS Operation automatically monitors and collects device information to compile performance statistics and periodically sends reports to the central NMS Control. Events can be detected directly by NMS Operation or devices can send notifications and alarms. Changes like device configuration or firmware updates will be performed by NMS Operation and centrally triggered by NMS Control.

SINEC NMS Control is located in the industrial data center and manages configuration policies, analyzes diagnostic data and provides an overview of the entire OT network infrastructure. Based on the cybersecurity plan, SINEC NMS supports the administration of access rights for users and communication relations between the different network zones. SINEC NMS Control also provides northbound interfaces for the integration into external systems and services. These include Syslog forwarding (e.g. security events), URL access (e.g. HMI system integration), inventory list (e.g. CSV) and email notifications.
Additional information is available via the links below:

Getting started with network monitoring

Deep dive into the SINEC Network Management System

Figure 5: SINEC NMS tasks



4. Network Protection

From a security perspective, the layer 3 network segmentation described in chapter 2 is not sufficient, because there is no restriction of data exchange and an identification of authorized entities is not possible. The solution is the deployment of systems to filter the traffic, detect unauthorized connections and send alarms to e.g. SCADA, Syslog or another diagnostics server in case of an event.

To ensure the necessary network protection and incident audit capability, the following recommendations within the ISA/IEC-62443-3.3 sections SR1.1 and SR5.2 can be found:

"SR 1.1 – Human user identification and authentication: The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures."

"SR 5.2 – Zone boundary protection: The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model."

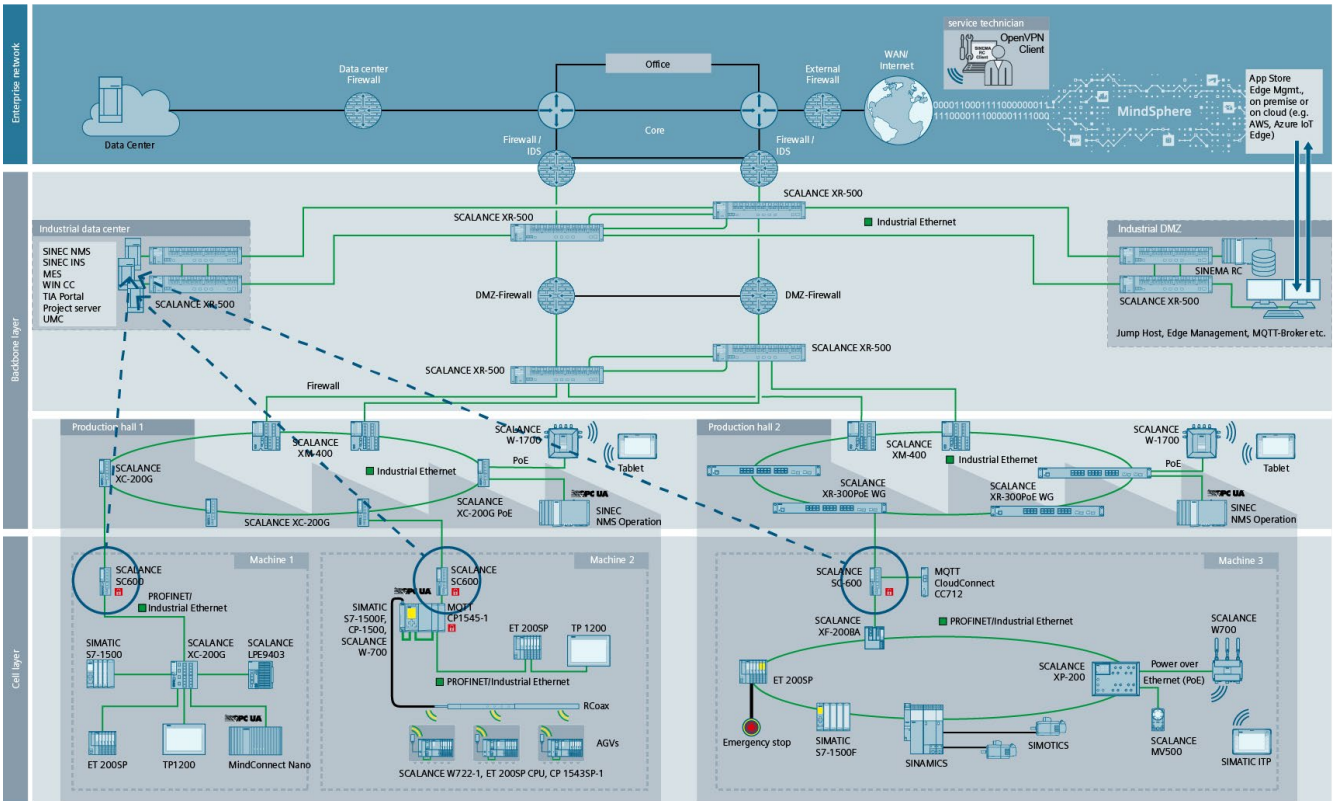
User and device authentication: As part of company policy, user access to each part of the IACS must be controlled. It is recommended to utilize an authentication server in the industrial DMZ connected to a user and device database. This database contains a list of all authorized users and devices together with their respective access rights and credentials.

For each system login and device connection to the network, credentials will be requested and unless the authentication credentials are correct, the access to the network or a system will be rejected.

All access requests will be logged and accounted in the respective device as well as in the authentication server. IEEE 802.1X with certificate-based authentication and MAC authentication (for devices without certificate support), are possible mechanisms for access control in combination with a central RADIUS server.

To prevent double administration and inconsistent data, it is possible to synchronize the RADIUS server by using a User Management Component (UMC) server with the centrally deployed Active Directory (AD). Traffic control at zone boundaries: It is recommended to use firewalls

Figure 6: Centralized OT firewall management



following the whitelisting principle, also referred to as "deny by default, allow by exception". A firewall will drop all incoming packets, unless there is a specific rule accepting the traffic. The rules can be based on MAC addresses, IP addresses, communication protocols, port numbers and in case of supporting deep packet inspection features, on the content within the payload itself. The firewall should also be able to monitor the state of an active connection (stateful) and to granularly assign rules to specific users. All relevant events can be logged and sent to a Syslog server or to a monitoring system.

Centralized OT firewall management: To avoid inconsistent configurations across multiple firewalls and to provide a firewall policy overview, a central firewall management located in the industrial data center is recommended. With this, new security policies can be applied to all devices from a single trusted location, while all configuration changes are logged over time. The firewall management can be specific for that task only or be centrally managed e.g. by SINEC NMS, which provides a graphical interface that automatically interprets user-defined communication relations to specific firewall rules and enforces them to relevant devices. Intrusion Detection & Prevention Systems (IDS/IPS): These software-based solutions offer a more advanced protection level than rule-based firewalls. Apart from behaving like a firewall, an IDS is a monitoring system that analyzes the forwarded traffic in real time and checks for known threat patterns (signature based) or deviations from the expected traffic flow (anomaly based). In the event of detecting an anomaly, the IDS will generate a corresponding alarm. The alarm requires manual follow-up. An IPS performs the same functions but does not require human intervention. In the event of unusual activity or an attack, the system can actively block the associated communication flow. Because of this automatic prevention of threats, there is a risk of generating false positives (valid communication, which will be blocked by mistake), that may affect normal traffic or deny access to the IACS. It is the responsibility of OT and IT managers to collaborate to choose between an IDS or IPS solution, analyzing which fits the business requirements best.

These IDS/IPS systems are usually installed between the OT backbone and the IT core due to the connection to untrusted external networks. If the risk analysis indicates that additional IDS/IPS are required, they may be installed at each transition between security zones. The effectiveness of these solutions depends heavily on their patterns and anomalies database, which requires continuous updates of the system. If these systems are installed inside an OT cell to monitor the communication, the real-time requirements of the automation solution must be considered. To avoid higher latency and delays, it is recommended to mirror the relevant traffic without affecting the production.

To get a better understanding of network protection, please visit the cybersecurity solutions website for industry:

Siemens Industrial Security
Video: Network security within Industrial Security

5. Secure Remote Access

Secure remote access to devices in an IACS network has become an essential service for the configuration, maintenance and updates of production relevant devices. Savings on travel expenses and time are major reasons for accessing an industrial device remotely. Additionally, in certain industries, it is forbidden to enter the production area, either for confidentiality reasons or due to worker safety.

This is reflected in SR1.14 and SR4.1 of the ISA/IEC-62443-3-3 document:

"SR 1.13 – Access via untrusted networks: The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks."

"SR 4.1 – Information confidentiality: The control system shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network and any zone boundary."

Remote access must be considered in the global cybersecurity plan. Remote users accessing the enterprise network from the outside can be both, employees of the company and external business partners. These users need to be treated as unknown while using untrusted end devices. To be able to identify these users and end devices processes needs to be implemented for granting secured access.

From a technical perspective, communication must also be carried out in a secure manner. VPN tunnels are the most common method for an encrypted remote access solution. Each remote user must be known and properly authenticated. The most efficient solution is a centralized VPN tunnel server installed within the industrial DMZ acting as rendezvous server which controls remote user, devices and

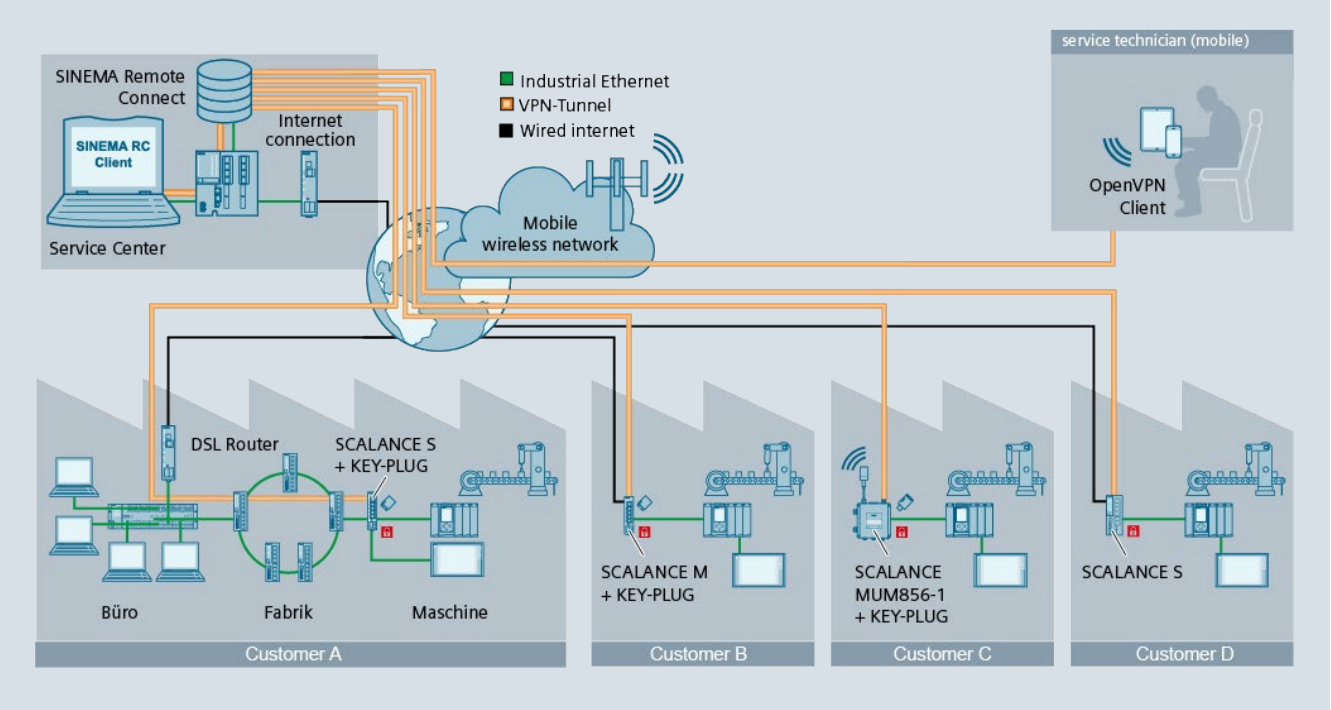


Figure 7: Remote access – Example of SINEMA RC configuration

communication relations. This server provides interfaces to integrate the UMC and AD servers for authentication.

To establish a remote access connection, the user's VPN client initiates an encrypted tunnel to the rendezvous server. In parallel, the VPN endpoints of the cells (e.g. cell protection firewall) establish an independent tunnel to the same rendezvous server. Depending on the configuration of the server, the access to the OT network is granted to the remote user. Each connection to the remote access server is logged and can be exported for further analysis.

If the risk assessment result requires a higher security level, a jump host-based solution must be implemented. A successfully authenticated external user accessing the jump host obtains access to a PC or hosted VM inside the industrial DMZ, not directly to the OT IACS. This access is established by a remote desktop connection. All tools and programs required for the user's remote operational tasks must be provisioned on the jump host. To be able to access the OT IACS a second VPN client connection is established from the jump host to the rendezvous server. Based on user rights, access to the OT network is granted.

The jump host solution minimizes the risk of malware or security threats affecting the OT network. A four-eye-access principle adds human intervention possibilities to the jump host solution, by controlling which tasks are carried out.

Additional information about a secured remote access solution is available under:

SINEMA Remote Connect

Technical video SINEMA Remote Connect

Jump host configuration

6. Training and awareness

The most important part of a cybersecurity plan is its people, not devices. Human errors cause more cybersecurity incidents than an operating system's vulnerabilities.

As such, in chapter 4.3.2.4 of ISA/IEC-62443-2-1 the following statement can be found:

"Provide all personnel (including employees, contract employees and third-party contractors) with the information necessary to identify, review, address and, where appropriate, remediate vulnerabilities and threats to IACS and to help ensure their own work practices are using effective countermeasures."

The company's management, risk managers and technical managers of the OT and IT networks have to develop a continuous training plan that ensures staff knowledge is up-to-date. This includes threats against the integrity of networks and assets, as well as how to respond to cybersecurity incidents. This training plan as part of the company's cybersecurity policy must be regularly reviewed to develop the required knowledge for a safe and secured integration of new technologies in the production facility.

The training plan includes the following components:

- Physical security: Workers must be informed of necessary safety measures according to the work environment, either in the office or within the production area. The plan should include information about the areas that each worker can access and access control policies.
- General cybersecurity awareness: All workers in the company must be trained to avoid security incidents, ranging from the correct use of internet access, computers, phones, USB devices, and social engineering protection.
- Role-related technical training: Depending on the technical responsibility of each worker, there must be specific trainings related to the cybersecurity of the devices in their scope of work. For OT network administrators, training should include device hardening fundamentals, firewall configuration, secured VPN connections, backup, patching and maintenance policies.

The links below provide additional information:

Siemens SITRAIN courses

Siemens Professional Services

Siemens Industrial Security Services

7. Epilogue

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 to 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 our page on industrial security.

Siemens' products and solutions undergo continuous development to maximize security. 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 a customer's exposure to cyber threats.

Siemens is the first company to receive TÜV SÜD certification (based on ISA/IEC-62443-4-1) for the interdisciplinary process of developing Siemens automation and drive products, including industrial software. With additional product-specific TÜV SÜD certifications, Siemens proves that the product development process is fully compliant with ISA/IEC-62443-4-1 and that substantial technical product requirements are implemented in compliance with ISA/IEC-62443-4-2.

Further information on certification standards

Siemens Industrial Security RSS Feed

The following links provide further insight regarding various cybersecurity topics for Industrial Automation applications:

Primer for cybersecurity in Industrial Automation

Secure remote access management

Industrial Wireless LAN for challenging applications

Security hardening checklist for network devices

Cloud connectivity for industrial plants

Industrial network management and monitoring

The following links provide some examples of the Siemens approach for developing secured networks in different industry branches:

Cybersecurity for I&C systems

Line integration for food and beverage industries

Industrial networks for wind power

Industrial networks for the process industry

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Deutschland

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Produced in Germany

Security information
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 only form one element of such a concept. For more infor-mation about industrial security, please visit

https://www.siemens.com/industrialsecurity