Network concepts for factory automation

SIMATIC S7, SCALANCE X/M/S, SIMATIC HMI

https://support.industry.siemens.com/cs/ww/en/view/109802750

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

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

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Introduction

1.1 Objective

With increasing digitalization, more and more devices need ever more data over additional connections inside a plant network. Not only additional connections, but also continuously available services (already a mainstay in the IT world) are increasingly relevant in automation systems. To meet these requirements, it is not enough to simply connect these components with one another. Rather, it is necessary to view the networking of individual components on a conceptual level and to design a state-of-the-art network according to the following criteria:

- Security
- Availability
- Performance

This document is intended to provide automation engineers with an example implementation of a possible network concept. The targeted solution serves only as an example and must be adapted based on the requirements of the plant owner.

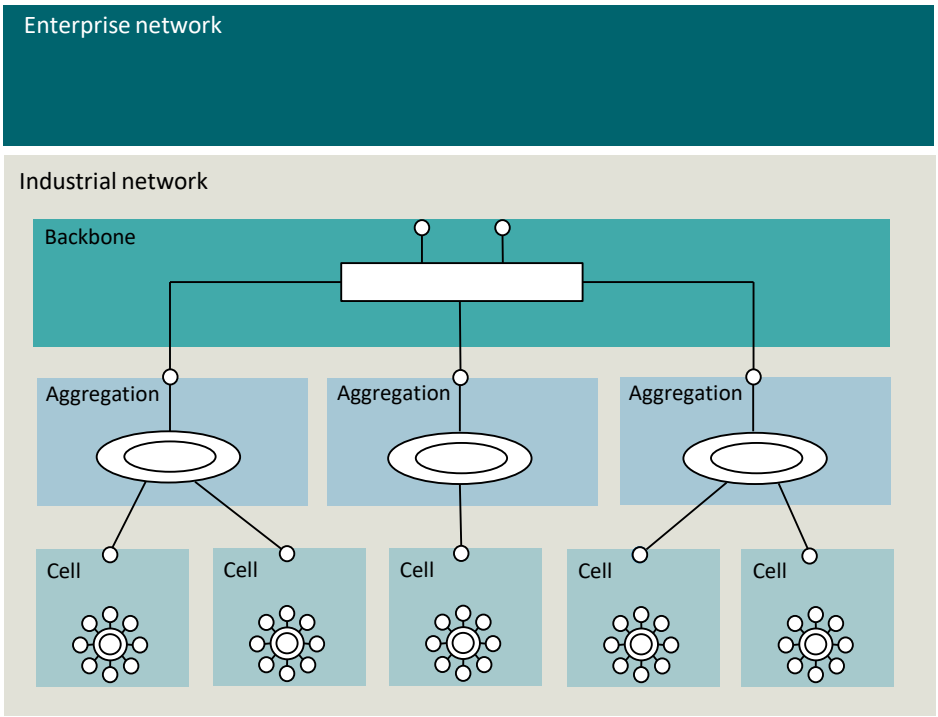
Generally applicable structure

The following image shows a potential general structure of an enterprise network. Networks in production facilities can typically be divided into three parts: cell, aggregation and backbone.

Chapter 2 describes in greater detail the requirements of each of the parts of an industrial network and how they can be implemented.

A description of an enterprise network is not part of this document.

Figure 1-1



1.2 Industrial communication in factory automation

In factory automation, there is always a need to identify opportunities for improvement in order to increase productivity in existing plants and plan new plants to be more efficient.

This is aided considerably by thorough linking of production lines and machines, from the input of raw material to production, packaging and all the way to dispatch of goods, as well as by comprehensive data collection on production parameters such as quantities, machinery timing and the like.

This makes it possible to collect data across all areas of the production facility and analyze these data with IT- or cloud-based systems and derive sustainable improvements from them. The process can be very laborious because typically machines and components from different manufacturers are connected to one another and the data collected must be analyzed and/or processed.

An industrial network from Siemens AG facilitates horizontal integration – from goods receiving to production to goods dispatch and warehousing – as well as vertical integration from the machine level to the control systems, the MES (Manufacturing Execution System) and finally to the enterprise network.

The concept presented in this document describes various levels, such as the industrial backbone, aggregation and the cell/machine level. The dimensioning of each of the levels can vary depending on the size of the plant.

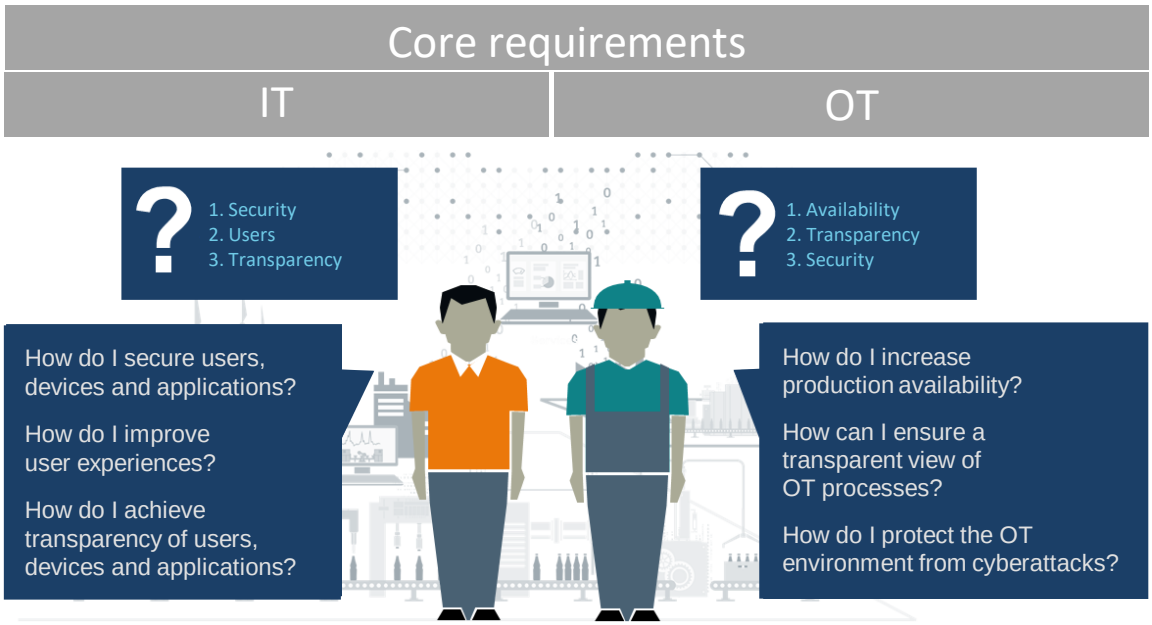
1.3 Drivers for an industrial network

Traditional network technologies and network components are designed to support enterprise networks in office or datacenter environments. They focus on providing services such as email, internet access, telephony and other centralized applications. Interruption of these services can have financial ramifications, but does not typically endanger health and safety or the environment.

By contrast, industrial communication technologies and components are designed for use in harsh environments and support time-critical industrial applications. In this case an interruption of service in an industrial network can have severe financial consequences and bring the entire operation to a standstill. Therefore it is important to know and meet the requirements of industrial networks.

Industry requires high availability of automation networks and their components. Redundant structures ensure availability of the automation network around the clock. Meanwhile, reliable provision of business-critical applications plays a central role in the office environment. In IT, transparency is essential for providing end-to-end visibility of users, devices and applications, while in OT (Operational Technology), transparency facilitates the visibility of industrial processes. In both worlds (IT and OT), cybersecurity plays a key role, its objective being to protect users, devices applications and the production environment itself from cyberattacks.

Figure 1-2



With this in mind, there are many customer requirements for an industrial network. Above all, the security of a plant and its specific requirements regarding functionality and flexibility must be taken into account.

With the increasing communication between office networks and industrial networks, additional security measures have become indispensable for attaining a suitable level of security for the plant components. A consensus must be reached between user-friendliness, flexibility and compatibility of an industrial network on the one hand, and security and safety on the other. This consensus can be achieved with network components designed specifically for the industrial environment. Such components must offer features that ensure troublefree operation of a production plant while still allowing reliable and secure network communication.

To convey a clear picture of industrial requirements, the following subheadings address typical customer requirements.

High availability

High availability of a production plant is an absolute necessity. If it is not present, economic and other damages for a company can occur. For this reason, availability must be ensured when operating a production plant. One way to achieve this is through redundant design of network connections in order to remain functional in the event of a fault. This is accomplished by using special network protocols, for example.

Specific measures for achieving high availability:

- Fast network reconfiguration time: Ring redundancy mechanism with a failover time of less than 200 ms with MRP and 300 ms with HRP.
  MRP is the standard at the field level.
- Simple device replacement with C-PLUG
- Redundant power supply
- S2 system redundancy (in connection with MRP)

Robustness

Environmental conditions vary greatly between different production plants and industry sectors across the globe. Devices used must be able to withstand these specific conditions. This also applies to network products. For example, they must resist high temperatures or dusty and corrosive climate conditions in an industrial manufacturing hall or similar locations while still performing their functions reliably and accurately. These requirements apply not only to the devices themselves, but also to their accessories such as cabling or antennae.

Individual measures for ensuring robustness of devices:

- Wide temperature range (-40 to +85 °C) and also suitable for outdoor use
- Resistant housing (up to IP65/67 protection level), EMC and shock resistance
- Fanless design, mechanical stability (e.g. quick-connect cables and connectors), retaining collars, robust cables (specifically for industrial applications)

Flexibility

As production is continuously being optimized and adapted to innovations, flexibility plays an important role in this arena. For this reason the network components and network topologies used must meet the needs of this aspect. Particular consideration must be given to network cabling and the design of devices in order to meet the demands of rough, continuously evolving industrial environments.

Individual features that provide for maximum flexibility:

- Modular components
- Combo ports for the use of different media
- Portfolio of cables and connectors for assembly in the field
- Flexibility in the required bandwidth, e.g. 10/100 Mbit/s, 1 Gbit/s and 10 Gbit/s
- Flexible network topologies (e.g. linear, ring, star, tree)

Standardization

Standardized interfaces play an important role at the cell level. Mechanical equipment manufacturers – and end customers – benefit when machinery can be integrated into the production line without any major modifications. Therefore, with respect to the network concept, standardized communications protocols should be preferred.

Individual measures for communication standards:

- Use standardized communications protocols (e.g. PROFINET, OPC UA)
- Use consistent data models (e.g. Companion Specs)
- Uniform physical interfaces (e.g. RJ45 for connecting machines)
- Define assignment of addresses and names (e.g. static IP addresses or DHCP)

Security/network security and access control

Every production area must be protected against unauthorized access. Suitable security measures include the use of firewall systems and the use of a cell security concept. Secure remote access must also be taken into account so that, for example, third-party manufacturers can perform remote maintenance on specific plant elements.

Individual measures that ensure network security:

- Specially developed security appliances, tailored for an industrial security concept
- Monitored and controlled network segments thanks to the use of SCALANCE S firewalls
- Secure remote access with zero-trust concept
- Compliance with regulations and standards (e.g. IEC 62443)

Mobile applications

Parts of a production line or warehouse can include moving systems such as forklifts and rail vehicles or portable mobile devices. These also typically require access to central systems. Specifically for rail vehicles or FTS, the IWLAN RCoax cable from Siemens offers a solution that provides uninterrupted IWLAN communication along a specific line.

Individual measures that facilitate mobile applications:

- Industrial WLAN with iPCF to support determinism and function safety via wireless networks
- IWLAN RCoax for uninterrupted wireless connection while in motion (e.g. FTS, monorail, etc.)
- Mobile applications with rapid update cycles and minimal maintenance effort

Functional security – plant safety and operational safety

Functional safety serves to protect people and machinery. This includes the ability to trigger an immediate emergency stop of a machine and pass through to the associated controller. This is possible not only with hardwired solutions, but also via industrial WLAN (IWLAN). The safety signals must be transmitted reliably and with the highest priority, regardless of the medium.

Individual measures that ensure functional safety:

- PROFIsafe, functional safety via PROFINET: no additional wiring necessary
- A defined, safe plant shutdown is possible at all times
- PROFIsafe via IWLAN

Determinism

Industrial networks are mainly used for control processes which run in a cyclic manner. Determinism is a fundamental requirement for this type of process. Cyclic processing is the essential difference between industrial communication when compared to client-server applications in IT. Some applications require short, rapid deterministic cycle times to quickly put machines in a safe state. Examples of this are PROFIsafe applications in which people and machines work closely side-by-side.

With respect to the safety requirement, signals must finish transmitting within a defined reaction time. If network devices cannot implement this requirement, then it may not be possible to perform an emergency stop even though an emergency stop switch has been pressed, for example. The notion of synchronous operation lies at the center of this issue. Operation and the expected work outcome are only ensured when sensors, controllers and actuators work in sync.

Individual measures that ensure determinism:

- Guaranteed failover times in the event of an error, plus deterministic roaming times for mobile devices
- Standardized protocols ensure interoperability: The PROFINET protocol and switches from the industrial Ethernet environment provide for predictable system behavior and rapid cycle times during data exchange.
- Synchronization of multiple drives in a machine, for example via isochronous realtime (IRT).

Industrial applications

In addition to the drivers for an industrial network mentioned above, there are additional applications that are relevant for a network concept for factory automation.

These applications include:

- HMI applications
- TIA engineering
- Industrial Edge
- Machine-machine communication
- Cloud connection

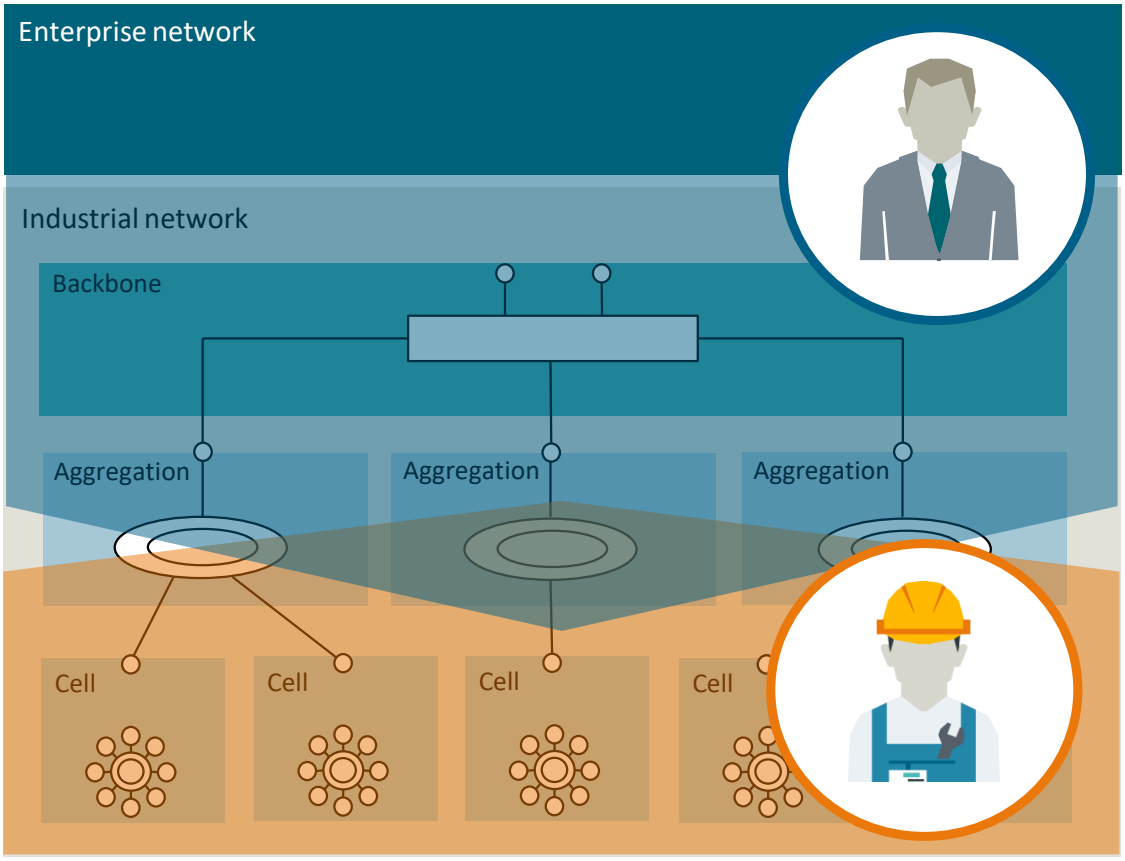
This document does not provide any general descriptions for the listed applications, but rather concrete solutions and pointers that can produce an effective network concept.

1.4 User view

As far as the network concept is concerned, it matters from which point of view the network concept is being viewed and used. First and foremost, one may distinguish between the role of "end customer" and "OEM".

Thus, there can be different solutions in the network concept which ultimately trace their origin to the difference in viewpoint between end customer and OEM.

Figure 1-3



Definitions of "Note" boxes:

Note

Note intended specifically for the end customer.

Note

Note intended specifically for the OEM.

End customer

The end customer is more concerned with high-level aspects of the system as a whole, such as security, certificate management and functional safety.

Central management of various services, such as user management and certificate management, is also relevant to the end customer.

OEM

The OEM is primarily concerned with points that affect only the OEM's machine and how it is integrated into the system. These can be aspects such as machine-machine communication or a secure remote connection to the machine for maintenance purposes. We address these concerns in detail in chapter 4.3 Connecting serial machines".

1.5 Network security objective

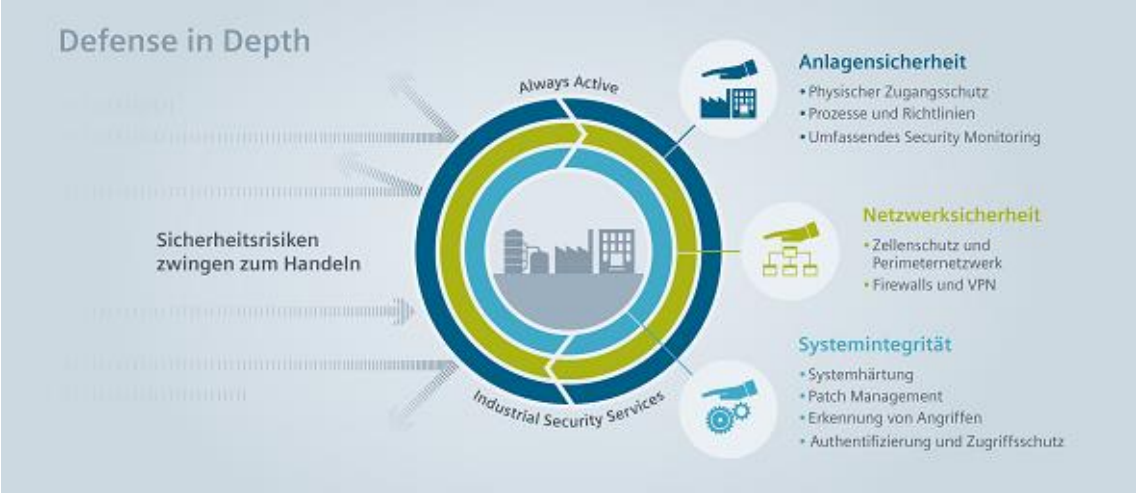
Security is an essential component of digitalization and has a significant influence on modern network design. Security requirements are already a consideration in the requirements for an industrial network (see chapter 1.3).

1.5.1 Safety and security requirements

The following aspects provide an overview of the safety and security requirements for factory automation.

- Secure network design (chapter 1.5.2)
- Reduction of attack surface
- Update management (chapter 3.4).
- Backup and restoration of data (chapter 4.1)
- User control; identification and authentication control (chapter 3.6)
- System integrity
- Trustworthiness of data/encryption (chapter 3.12)
- Limited data flow
- Security logging and monitoring (chapter 3.2)

Technical aspects are accounted for in a comprehensive security concept like the "defense in depth" concept of the IEC 62443 standard.



Because this document is concerned with network design, network security aspects in particular will be addressed in greater detail. Points regarding plant security and system integrity will not be addressed here.

1.5.2 Network design concepts

The cornerstone of secure network design begins with choosing the solution approach. Two different solutions are conceivable for the cell level:

- A cell security concept resting on a layer-3-based separation of cells
- A fully layer-2-based production network with a central firewall at the boundary of the cell level

This document pursues a solution approach that uses the layer-3-based cell security concept.

The following main points should be observed:

- **Network segmentation**
  The network is divided into independent operational units (zones) with common security levels. The security zones each implement defined security measures to attain the desired security level. The establishment of a demilitarized zone (DMZ) forms an additional zone for data traffic between the industrial network and enterprise network / internet. This can significantly reduce the risk of access violations.
- **Zone boundary protection**
  Each security zone is reachable via a defined access point protected by a firewall.
- **Securing communication between the security zones**
  All communication between the security zones must be monitored and controlled. One measure is the use of a firewall as well as segmentation into VLANs, or encrypted communication (e.g. TLS). The use of tunneling protocols such as IPSec or OpenSSL is another option.

1.5.3 Definition of network segmentation according to IEC 62443-2-1

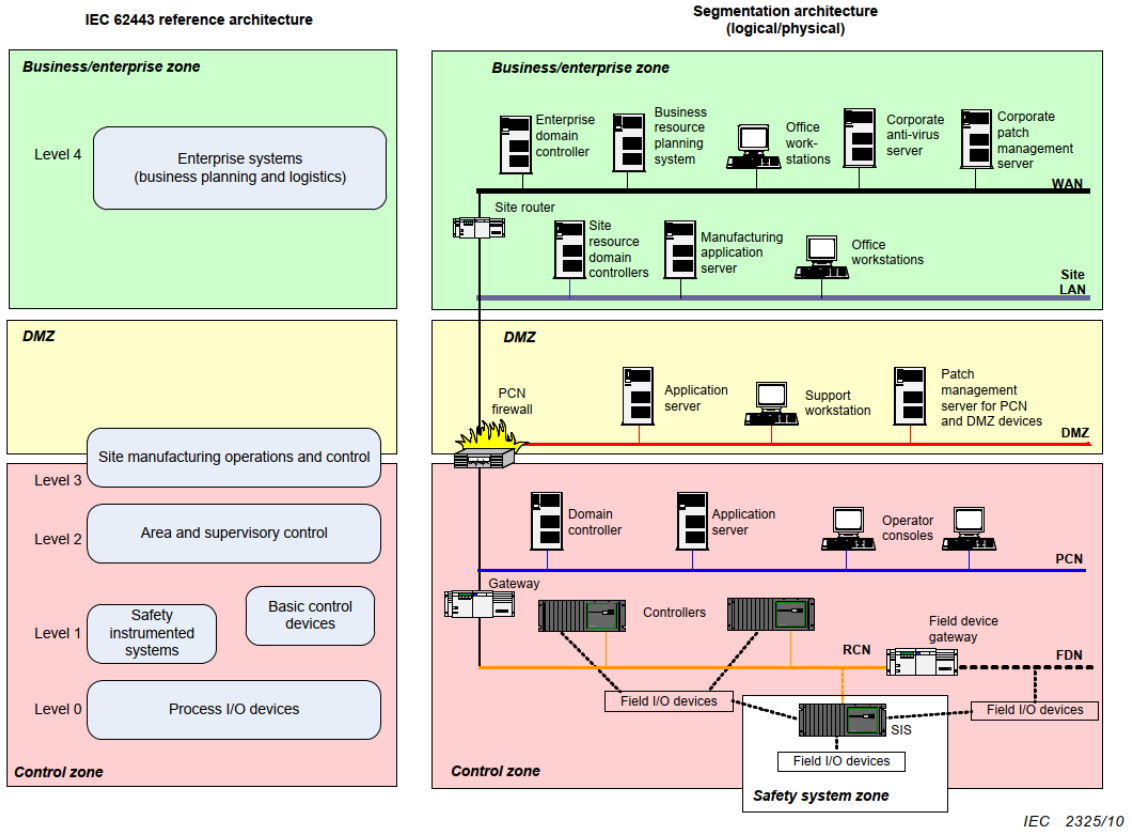
The IEC 62443-2-1 standard provides a good overview and orientation with regard to security and, in particular, to network segmentation and the protection of zone boundaries.

"Network are segmented through the use of a type of suppressor. A suppressor has the ability to control what goes through it. In Ethernet-based networks handling TCP/IP traffic, the most commonly used suppressors are firewalls, routers and layer-3 switches. Oftentimes, industrial automation and control systems (IACS for short) consist of various networks that use different physical- and application-layer technologies. These non-TCP/IP networks also use suppressors to divide and segment communication. Suppressors can be independent gateways or they can be integrated into the network interface module of an IACS device"[1].

While the insertion of a "suppressor" (term used by the standard, ordinarily a firewall) into the network can produce a new network segment and a security zone, a security zone may also encompass multiple network segments. The Figure below illustrates one possible segmented architecture for a generic IACS. This Figure illustrates how so-called function levels can be translated to the physical world of an IACS and the logical world of a zone. Note that the Figure is very imprecise and does not contain all network devices needed in an actual installation.

[1] Excerpt from the IEC 62443-2-1 standard – 11/2010

Figure 1-4



Function levels vs. security levels

It is important not to confuse the function levels of the reference model with the security levels associated with security zones. While it is generally true that the lower-level devices play a greater role in the secure functioning of an automated industrial operation, it may not be practical to apply a segmentation strategy that maps the device levels one-to-one. One commonly looks to the Purdue levels to define security zones in such a way that the zones are easy to recognize in the plant. But by definition, security zones are a logical grouping of assets with the same requirements.

Control zone

Generally accepted practice consists of using a firewall to manage the communication that connects the control zone with the enterprise zone, as shown in Figure 1-4.

Common filter strategies at the firewall are:

- The base configuration of the suppressor should cause all communication to be rejected by default while communication is only accepted in specific exceptions. This applies both to interactive user communication and to the continuous end-to-end communication between the devices between the control and enterprise zones. Whenever possible, the communication should be filtered for ports and services between matching IP pairs for the devices.
- Ports and services commonly used as attack vectors should not be opened via the suppressor. If the service is required for business reasons, additional countermeasures should be enacted to compensate for the risk.

Example:
An inbound HTTP request can be required to support an important business function. Additional compensatory measures such as blocking inbound scripts and the use of an HTTP proxy server help reduce the risk from opening this high-risk ports and service.

- The fewer ports and services are opened through the suppressor, the better this will be for security.
  Avoid communications technologies for which a large number of ports must be open.

Demilitarized zone (DMZ)

The function of the DMZ consists of preventing or greatly reducing any direct communication between the control zone and the enterprise zone.

The DMZ contains devices that serve as a bridge or buffer between devices in the enterprise zone and the control zone. A communication link is established between a device in the enterprise zone and the DMZ. The device in the DMZ then forwards the information to the receiver device in the control zone.

The filtering strategies mentioned above for the control zone are also applicable for the DMZ. For the DMZ, it is also possible to permit more risky protocols in order to simplify the management of devices in the DMZ and control zones.

There are multiple use cases where a DMZ is an advantage:

- Minimize the number of persons who directly access devices in the control zone from the enterprise network.

  Example:
  A Historian server is commonly accessed by persons located in the on-site LAN in the enterprise zone. Rather than place the Historian server in the control zone and give a large number of users direct access to this device, the security level of the control zone can be upgraded if the Historian server is located in the DMZ.

- Higher security level for important IACS devices.

  Example:
  In the case of the aforementioned Historian server, one option would be to place the device not in the DMZ but rather in on-site LAN where the majority of the users are located. This would reduce the number of persons who must access the IACS. However, because the enterprise zone is a zone with a lower security level, the server would be exposed to a less secure environment. Thus, the potential of the server being compromised would be greater in this case.

- Compensation of patching delays.
- The DMZ offers additional security protection for important IACS devices that cannot be patched as rapidly.
- Provision of improved security for the control zone by relocating administrative devices to a higher security level.

The DMZ is a suitable level in which to place devices such as antivirus servers and patch management servers.

Using the selected network concept, chapter 3.12 – Security explains how to implement the three core points of network segmentation, zone protection and securing of communication between zones.

2 Solution details

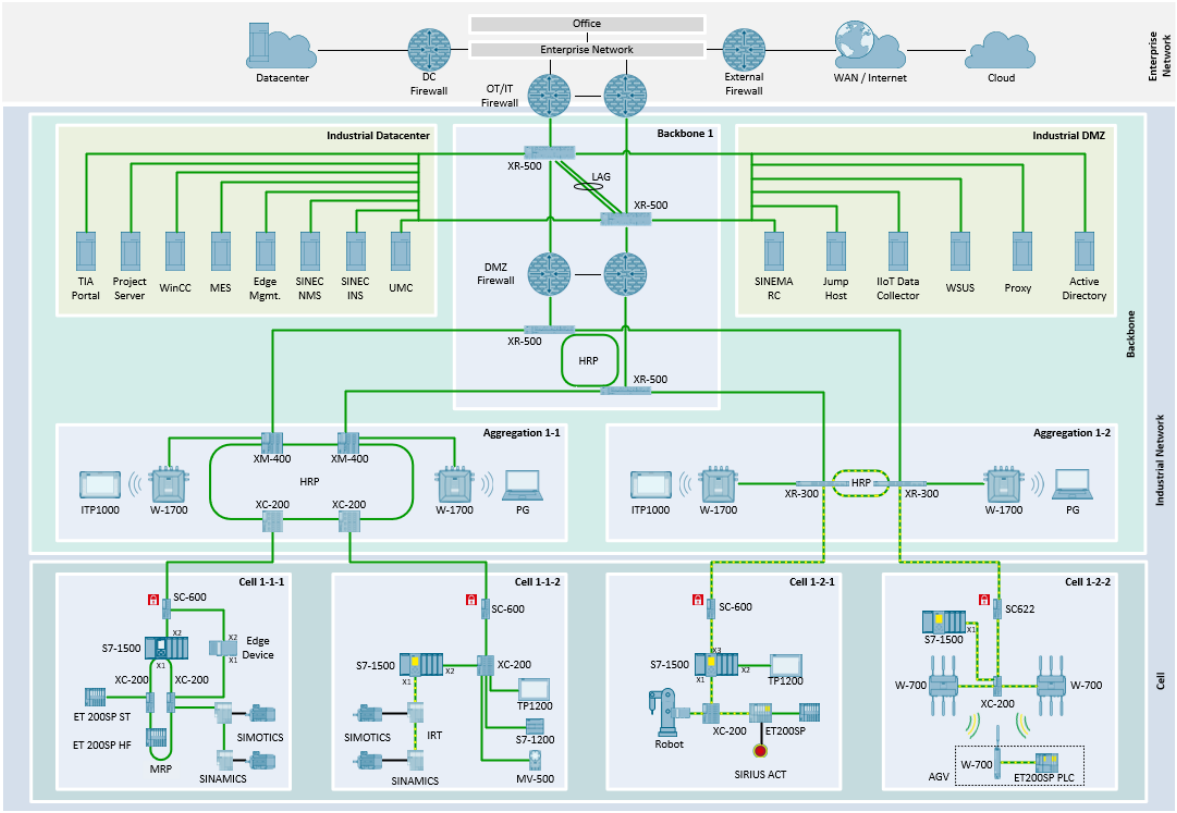
2.1 Overview of layer 2

2.1.1 Brief description of the architecture

Overview

The following Figure shows an overview of a possible site network with a schematic representation of traditional IT infrastructure with intranet, internet and datacenter as well as the link to the industrial infrastructure. The enterprise network area is outside of the focus of this document.

Figure 2-1



Digitalization is changing every aspect of our customers' businesses. The right communication networks form the basis for this change. Enterprise and industrial networks look very different, yet they are connected with a specific interface. To connect these two worlds to each other while making sure the requirements of each world are met is the highest goal here.

Figure 2-1 presents a solution in the form of a physically separated industrial network in order to deliver a structured, reliable platform that supports various communication requirements while also meeting the current security requirements (> Security Level 1).

It is possible to distinguish here between the following segments:

Enterprise network

The enterprise network is managed by IT and contains all types of office-related services. To meet the various requirements of the enterprise network and production, the two networks are physically separated so as to prevent undesired interactions. To facilitate data exchange a firewall is typically (and in accordance with the IEC 62443 standard) employed at the boundary between the enterprise network and the industrial network.

Industrial network – backbone and aggregation

The backbone is implemented as the central data communication layer. It bundles the communication from all lower levels and combines datacenters and the demilitarized zone (DMZ).

For details on the backbone level, see chapter 2.5.

Additional aggregation layers may be added as an option to combine various production cells and implement load distribution and network segmentation based on communication relationships.

For details on the aggregation level, see chapter 2.4.

Industrial network – automation cell

Cells are separate network spaces for various assembly lines, automation cells or machines. Within this space, workstations are grouped within the factory according to safety standards, communication relationships, production-specific layouts or the delivery contents of various OEMs. In turn, cells can be small tree, star or linear networks (or they may contain ring structures) if the production process requires solutions of this kind.

For details on the automation cell level, see chapter 2.3.

2.1.2 VLAN segmentation

Advantages

VLANs are utilized for flexibly connecting systems to the backbone/aggregation (e.g. WLAN access points or SINEC NMS Operation) and DMZ/industrial datacenter. The advantage of this is that switch ports and the terminal devices connected to them can be quickly and easily assigned to each respective IP subnet.

Definition

VLANs are virtual logical network segments in a physical network. They serve to restrict broadcast domains or increase the security of a network by separating data traffic. To segment the network, end nodes in a network are divided into logical subnets in which the participants can only communicate with one another but have no contact to participants in another segment.

If the network is segmented, then no more layer-2 communication between the virtual networks is possible. To still provide for targeted data exchange, routing interfaces are required in both layer-2 segments. To do this, the VLANs must be in different subnetworks and a layer-3 switch or a router or firewall is required.

If an Ethernet node wants to send a telegram to another network segment, then the data are sent via layer-3 switches, each of which has an interface in the corresponding network segments. The data packet can only be routed to the recipient via the interface in the

neighboring network. The corresponding router must be set as the default gateway of the terminal devices for this to work.

In the present network concept, the firewalls shown take on the function of the router. And for security reasons, only absolutely necessary communication is permitted.

2.1.3 Network redundancy

Central network components in particular are designed redundantly in order to meet the requirement of high availability. Redundancy protocols that support deterministic failover times are used in the backbone/aggregation group. This also makes it possible to meet realtime requirements from the industrial environment.

2.2 Overview of layer 3

2.2.1 Brief description of the architecture

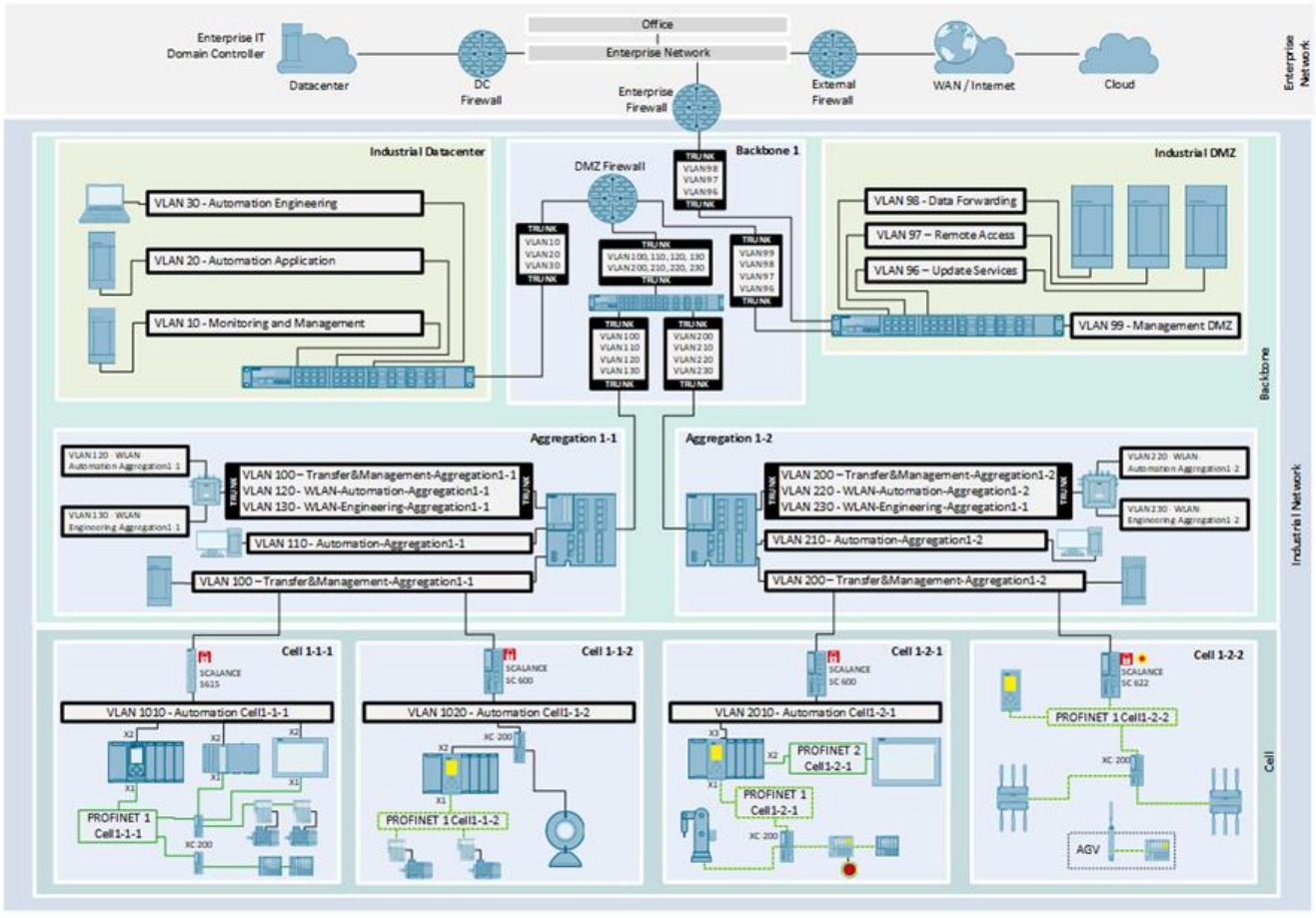
Overview

The graphic below shows the essential subnet architecture and division from a layer-3 perspective. Network segmentation is required for security reasons. Data traffic is monitored and controlled with the help of clearly defined gateways in corresponding firewalls (see 3.12 Security).

Note

The depiction deliberately accounts for only the layer-3 view in order to illustrate the subnets without loss of clarity. Thus, only one switch is shown, for example, in the aggregation, datacenter and DMZ areas to represent the various VLAN and subnet segments.

Figure 2-2



In the backbone and aggregation level, a port-based VLAN architecture is used here for reasons of cost and flexibility. This solution permits classification and segmentation of individual systems and network levels appropriate to the use case. In this case, each VLAN contains its own IP subnet. The firewalls at the gateways are responsible for routing between the networks. They can also be employed in a redundant configuration if necessary.

When assigning systems to a subnet or VLAN, here are some of the aspects which should be given consideration:

OSI layer-2 communication

Cross-subnet communication is ever only possible through routing (OSI layer 3). If OSI layer-2 communication between devices and systems is necessary (for example, because of PROFINET), then these devices must be in the same subnet.

Use case of the system

Dividing the systems into appropriate application groups can simplify assignment. Groups such as Engineering or Update Management are common.

Security aspects

From a security perspective it is a good idea to divide remote maintenance access, for example, from update management on a network level.

A VLAN configuration example can be found in SIOS (\8\).

You can find details on VLAN configuration in chapters 2.4 and 2.5.

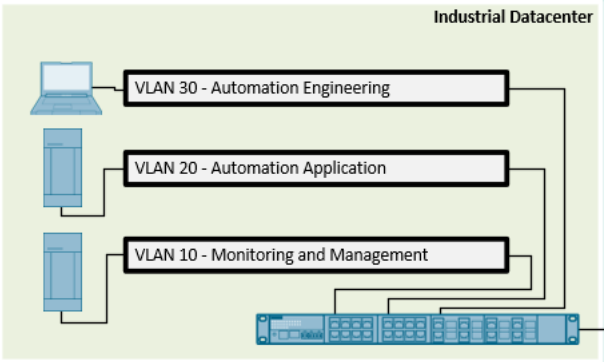
2.2.2 VLANs/subnets in the backbone level

Subnets in the datacenter

In the industrial datacenter, VLANs make it very easy to segment virtual machines. Thanks to a restrictive firewall configuration, VMs can only ever communicate in the subnets assigned to them. Exceptions must be allowed explicitly. Moreover, network virtualization used in the VM server makes it possible to configure new VLANs and subnets at any time without hardware reconfiguration. In this way for example, test systems can be effectively decoupled from production operations (see chapter 3.5 Virtualization).

In consideration of the use cases described in this document, the following division is conceivable for the datacenter:

Figure 2-3



Network Monitoring and Management (VLAN 10)

This subnet contains all administrative components necessary for network operation, such as

- SINEC NMS Control Station for orchestrating the switches and firewalls (chapter 3.2),
- SINEC INS for provision of DHCP, DNS and Syslog Server (chapter 2.6.2),
- the central user management instance in the form of a UMC ring server (chapter 3.6),

- the management interfaces of the network components (chapter 2.4.3 / 2.5.3);
- dedicated management interfaces, for example those common with virtualization servers, can also be assigned to this VLAN (see chapter 3.5).

Automation Application (VLAN 20)

This subnet contains central server components necessary for the operation of the automation solution. They include, for example:

- MES systems
- Industrial Edge Management (see chapter 3.13.6 – Network concepts for factory automation)
- Central servers of a virtualization solution (see chapter 3.1 – Visualization)

Automation Engineering (VLAN 30)

This subnet contains the necessary engineering systems for configuring and programming the automation components, such as:

- TIA Portal or Startdrive
- License server
- TIA Portal project server
- UMC server for user authentication in the TIA Portal project.

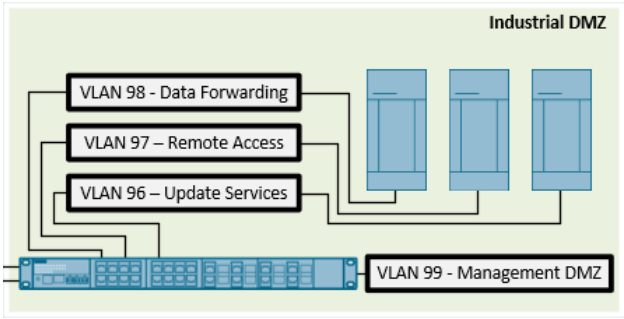
Details on these components can be found in chapter 3.3 and the ones after it.

When using templates for dynamic creation of virtual machines, it is recommended to integrate the VLAN and subnet settings directly into the configuration.

Subnets in the DMZ

Servers appear in the DMZ which can have access to unsecured networks (or are reachable from such networks) at any time. Therefore, for security reasons it is prudent to segment the servers into VLANs according to their use case. The following division is possible:

Figure 2-4



Management DMZ (VLAN 99)

The configuration interfaces of the network components are assigned to this subnet. If systems are located in the DMZ which use dedicated configuration interfaces, this network is likewise an option.

Data Forwarding (VLAN 98)

This subnet contains services characterized by a forwarding feature. This applies chiefly to proxy servers for controlling internet access and domain controllers for providing authentication services.

Remote Access (VLAN 97)

This subnet is used for hosting the remote maintenance access points. A SINEMA Remote Connect server or Jump Server may be located here, for example.

Update Services (VLAN 96)

This subnet contains servers that provide centralized updates for lower-level components and coordinate their rollout (e.g. Microsoft WSUS).

2.2.3 VLANs/subnets in the aggregation level

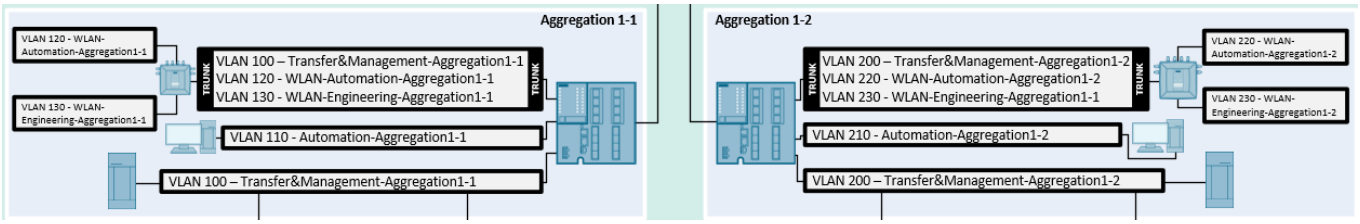
For security reasons, in the aggregation level it is prudent to decouple WLAN networks for mobile HMI applications from the actual production network, for example. Due to the great spatial extent of these network segments, investing in fully separate hardware is often very cost-intensive. In such a case, VLANs can cost-effectively increase the security level by mapping multiple network segments to a single infrastructure.

A defined communication flow can be achieved by targeted grouping of the systems. Faults that cause high network load, for example, are thus typically limited to one subnet.

Each VLAN is assigned its own subnet on the aggregation level as well. An automation solution can contain multiple aggregation levels, however.

The following is a plausible network segmentation for an aggregation level:

Figure 2-5



Automation-Aggregation (VLAN 110 / VLAN 210)

The Automation-Aggregation subnet is used for placement of automation components in the aggregation level. For example, these may be visualization systems on the line level or remote control stations for systems in the datacenter.

WLAN-Automation-Aggregation (VLAN 120 / VLAN 220)

The WLAN-Automation-Aggregation subnet receives its own SSID (see chapter 3.13 - WLAN). This WLAN network is used for connecting all mobile components of the automation solution on the aggregation level. These may be tablets, smartwatches or AGVs, for example.

WLAN-Engineering-Aggregation (VLAN 130 / VLAN 230)

The WLAN-Engineering-Aggregation subnet also receives its own SSID. This WLAN provides a dedicated WLAN network for engineering access on the aggregation level. Due to the spatial spread of this network, Field PGs may be integrated for commissioning or service calls, for example. Thus, the central servers in the datacenter are reachable throughout the whole production area.

2.2.4 Subnets on the cell level

A cell can always be divided into multiple subnets.

In this case, the CPU is often responsible for network isolation between uplink and other PROFINET networks. VLANs are used less often in this level, but they can make sense for prioritization or segmentation reasons.

In addition, special requirements regarding failsafe communication apply here (see chapter 3.8 – Safety-related communication).

Size and architecture of the cells are often determined in practice by the following motives:

- **Necessity of realtime communication between machines or plant components**

  Realtime protocols typically require layer-2 architecture. Therefore it can be necessary to bundle multiple machines within one cell. Here, realtime data traffic can run over a dedicated, cell-internal network or VLAN while layer-3 data traffic on higher levels is likewise segmented by VLANs with corresponding subnets.
  It is also possible to couple two subnets using a PN/PN coupler.

- **Vendor-based segmentation**

  Oftentimes individual segments of the production line are set up by vendors. This can also have consequences for the architecture of the automation cell. Thus, multiple machines from one vendor may be bundled in the aggregation level with a firewall component, for example.

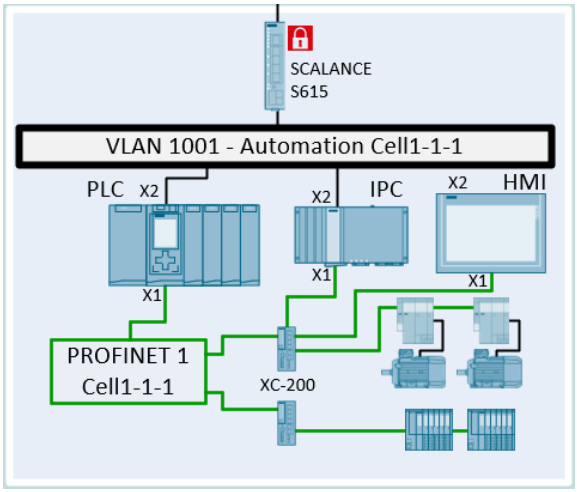
- **Segmentation for dividing communication flow**

  When using systems that cause a high level of data traffic, it is possible to subdivide the cell network into additional subnets. A classic example for such a structure are PC systems that are regularly backed up in full, or cameras for process monitoring. By placing these systems in a gigabit segment, it is possible to increase the bandwidth by a factor of 10 in comparison to a traditional PROFINET network.

Cell network examples

1. **Cell with CPU-based network isolation and 100 Mbit/s link**

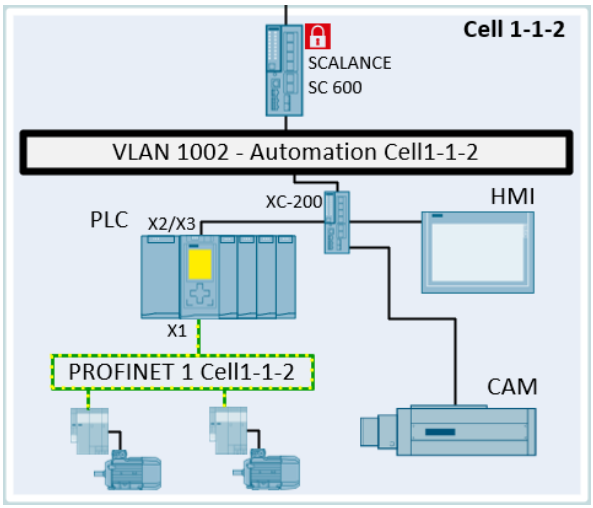
Figure 2-6



The VLAN 1010 Automation Cell1-1-1 serves here as an uplink for data from the CPU and the Industrial Edge.
The PROFINET 1 Cell1-1-1 serves as a realtime network for drives and I/O devices.
The Industrial Edge device (IPC) and the HMI Panel can access PROFINET with OSI layer 2 via the X1 interface. This allows for topology scans, for example.
The uplink and data exchange between edge and CPU happen through the X2 interface. The CPU is thus not burdened by the data traffic between the edge and higher-level systems.
Using the IP forwarding feature of the CPU, it is possible to access I/O devices from higher-level networks with OSI layer 3.

2. Cell with CPU-based network isolation and 1 Gbit/s link

Figure 2-7

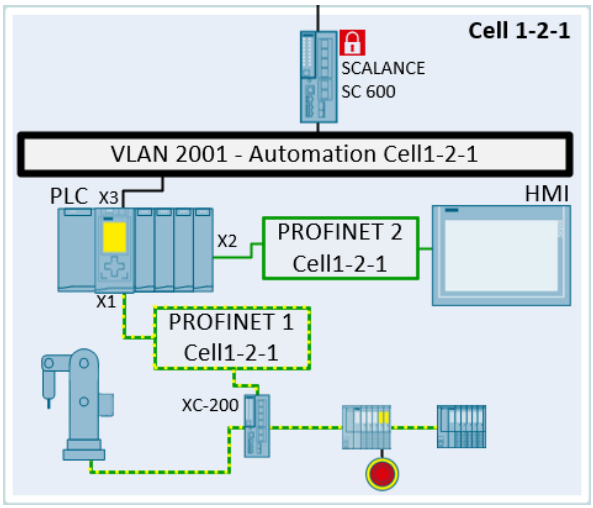


Camera-based monitoring necessitates higher bandwidth in this cell. Therefore the SCALANCE SC600 series with 1 Gbit/s interfaces is used as a firewall. The CPU is used for network isolation between the cell network and PROFINET. No realtime communication is necessary for the HMI here. Thus, a clear separation is possible here between the realtime network (PROFINET 1 Cell1-1-2) and non-realtime network (VLAN 1020 Automation Cell1-1-2).

The PROFIsafe island is likewise terminated at the CPU due to the network isolation. In this scenario as well, I/O devices are accessed via the IP forwarding feature in the CPU.

3. Cell with CPU-based double network isolation and 1 Gbit/s link

Figure 2-8

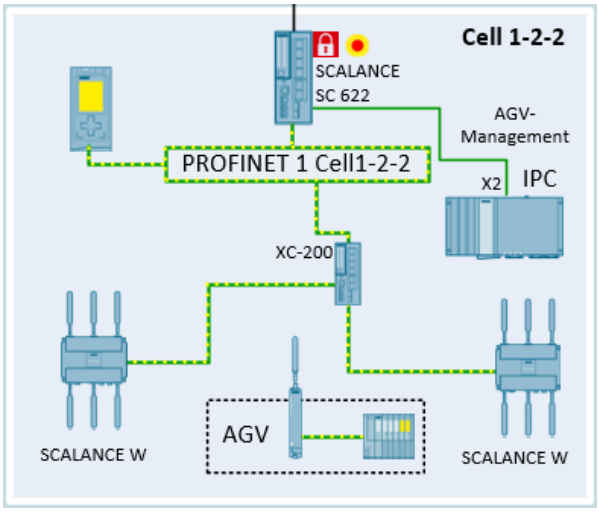


In this cell, the CPU represents the central network node. The uplink here is a gigabit uplink via the CPU. This architecture is especially suited for applications with high data load between the CPU and higher-level systems.

The HMI is decoupled from the rest of the application through network isolation. Access to I/O devices and the HMI is possible with IP forwarding. In this case, too, the PROFIsafe domain terminates at the CPU.

4. Flat cell with 1 Gbit/s link

Figure 2-9



In this arrangement, only one CPU interface is used. Here, the cell network is therefore set up as a PROFINET network with corresponding realtime communication.

The SCALANCE SC 622 module is responsible for terminating the PROFIsafe island in this case.

The devices in the cell can be accessed directly via the firewall. There is no communication load on the CPU from IP forwarding.

2.2.5 IP address assignment

IP subnet/VLAN definition

In conjunction with the VLANs, the IP subnets have a segmenting function in the network. Based on the subnet concept demonstrated above, it makes sense to assign each IP subnet to its own VLAN.

According to IETF RFC 1918, the following address ranges are available for addressing of components in private networks:

Table 2-1

Address range	CIDR notation	Number of addresses	Number of networks / network classes
10.0.0.0 to 10.255.255.255	10.0.0.0/8	16777216	1 Class A network (10.0.0.0/8)
172.16.0.0 to 172.31.255.255	172.16.0.0/12	1048576	16 Class B networks (172.26.0.0/16 to 172.31.0.0/16)
192.168.0.0 to 192168255255	192.168.0.0/16	65,536	256 Class C networks (192.168.0.0/24 to 192.168.255.0/24)

Class A network matching with VLAN ID

The Class A subnet is suitable for general addressing of the components in the network. Thanks to the 3 freely definable octets, this network can be adapted semantically for the VLAN IDs.

To accomplish this, the network is divided with the help of subnetting into individual Class C networks each with 256 addresses. The first address of the network is reserved for the network, the second address is reserved for the router, and the last address is required as a broadcast address. If the routing must be designed redundantly, then the first three addresses are required for routing (see chapter 2.2.6 and following chapters).

Thus, depending on how the routing is set up, 253 or 251 addresses are available in each subnet for other devices. Of these, the addresses listed in the Table below are reserved for the network components (switches). No addresses are reserved for the PROFINET networks because in this case the network components are typically managed by the CPU as PROFINET devices.

Table 2-2 Reserved IP addresses for network components

Subnet	Address range for network components
Monitoring & Management	10.0.10.10 to 10.0.10.99
Management DMZ	10.0.99.10 to 10.0.99.99
Transfer&Management-Aggregation1-1	10.0.100.10 to 10.0.100.99
Transfer&Management-Aggregation1-2	10.0.200.10 to 10.0.200.99
Automation Cell-1-1-1	10.1.10.10 to 10.1.10.99
Automation Cell-1-1-2	10.1.20.10 to 10.1.20.99
Automation Cell-1-2-1	10.2.10.10 to 10.2.10.99

The subnets are given semantic names based on the VLAN IDs as follows:

Table 2-3

	VLAN ID	Subnet
One-character VLAN ID	W	10.0.W.0/24
Two-character VLAN ID	WX	10.0.WX.0/24
Three-character VLAN ID	WXY	10.0.WXY.0/24
Four-character VLAN ID	WXYZ	10.W.XYZ.0/24

Note

Remember that in this case, not all VLAN IDs are mappable with this model. VLAN IDs from 1 to 4094 are theoretically possible, but it is only possible to map numbers between 0 and 255 in an IP address octet.

Thanks to VLAN-based semantics, the purpose and/or state of the network can then be recognized implicitly through the IP address. This can greatly simplify analysis of log files or network recordings, for example.

Using the IP addresses, it is possible to draw conclusions such as the following:

Table 2-4

Criterion	Conclusion
IP address in range 10.0.0.1 to 10.0.99.255	The addressed component is located in the backbone level (datacenter or DMZ)
IP address in range 10.0.100.1 to 10.0.199.255	The addressed component is located in the network segment Aggregation 1-1
IP address in range 10.0.200.1 to 10.0.255.255	The addressed component is located in the network segment Aggregation 1-2
The second octet of the IP address is greater than 0	The addressed component is an element of a cell.

Comparing static and dynamic IP address assignment

IP addresses can be assigned both statically (by configuration in the corresponding terminal devices) as well as dynamically (using DHCP).

It is always recommended to divide networks into a static part and a dynamic part. Due to the fact that most components are configured statically, the static portion should be larger than the dynamic one.

Therefore, in this concept the last 54 addresses of the subnet are defined as a DHCP pool. Further information on DHCP can be found in chapter 2.6 – Central network services. The router and/or firewalls server as DHCP servers in this case.

Static IP addresses are used in the majority of cases for the automation components in the cells. DHCP will be used here when a programming device is temporarily connected, for example.

However, especially with serial machines, the use of DHCP can offer advantages up through the CPU level.

For example, the following base configuration is the result for the Monitoring & Management subnet (VLAN 10):

Table 2-5

Parameter	Value
Subnet address	10.0.10.0/24
Gateway/router addresses	10.0.10.1, 10.0.10.2, 10.0.10.3
Broadcast address	10.0.10.255
DHCP range	10.0.10.201 to 10.0.10.254

Appendix IV – Subnets contains a tabular overview of all subnets envisioned in this concept, along with their assignment to the corresponding VLANs.

2.2.6 Routing in the DMZ and enterprise firewall

Overview

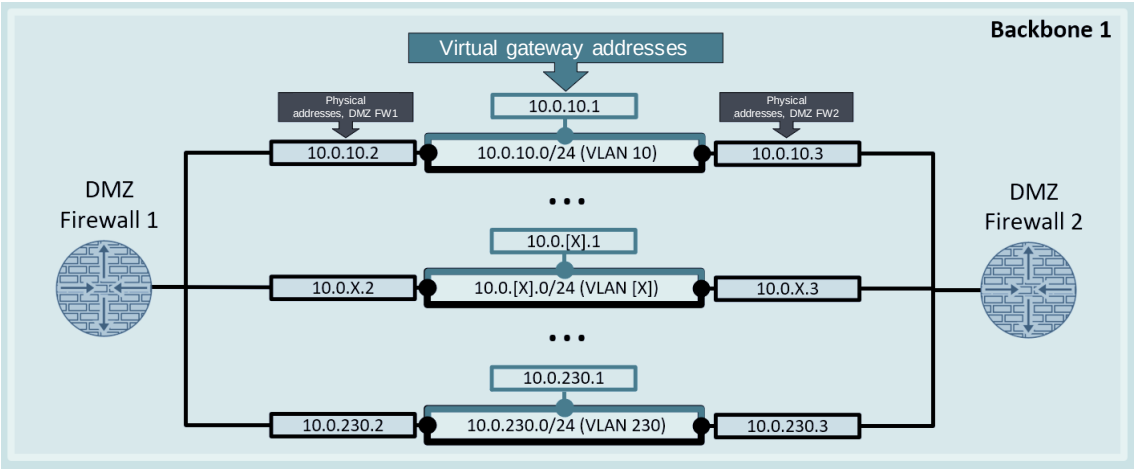
To implement router redundancy, the two firewalls in each connected subnet provide a virtual IP address. This virtual address is used as a gateway by all other components and is always the first address in the respective network segment.

The physical interfaces of the firewalls receive the second and third address of the subnet.

The networks in the DMZ are an exception. Here, the enterprise firewall assumes the function of the default gateway. Thus, the DMZ firewall receives the fourth through sixth IP address of the respective subnet in this case.

The following graphic illustrates the address architecture with virtual IP address.

Figure 2-10



The DMZ and enterprise firewalls serve as central routers between the network segments in the backbone. Due to the cascading down to the cell level, the static routes listed below are required in these firewalls:

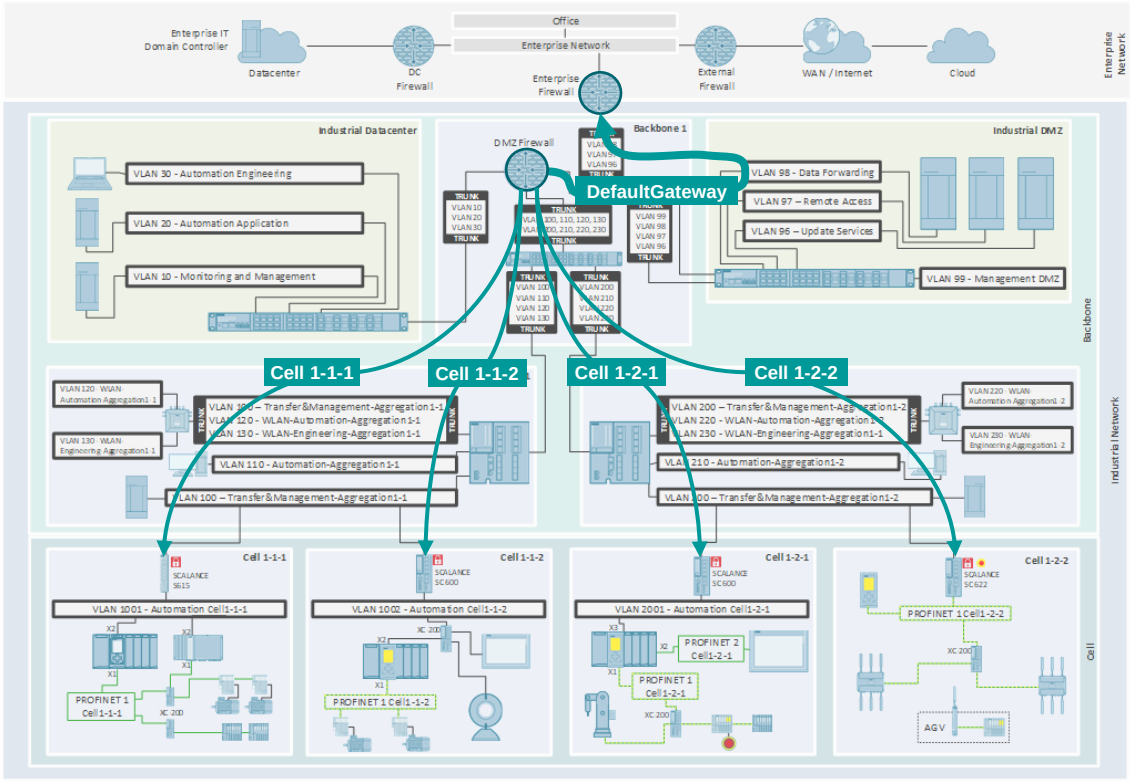
Static routes in the DMZ firewall:

Because of the network isolation on the level below, the DMZ firewall requires static routes into the individual cells. All traffic to devices in the single cells is routed through the corresponding cell firewall. The enterprise firewall serves as the default gateway for communication to enterprise networks.

In this case, the uplink traffic is routed via the Data-Forwarding subnet (if a proxy server is not being used).

The following graphic shows the required configuration of the routes in the DMZ firewall.

Figure 2-11



The configuration listed below is required for this routing. Appendix VI – Static routes contains detailed route planning with IP addresses.

Table 2-6

Destination network	Next hop	Purpose
Automation Cell1-1-1 PROFINET 1 Cell1-1-1	Cell1-1-1 Firewall (Interface in the Transfer&Management-Aggregation1-1 subnet)	Reachability of cell 1-1-1
Automation Cell1-1-2 PROFINET 1 Cell1-1-2	Cell1-1-2 Firewall (Interface in the Transfer&Management-Aggregation1-1 subnet)	Reachability of cell 1-1-2
Automation Cell1-2-1 PROFINET 2 Cell1-1-2 PROFINET 1 Cell1-1-2	Cell1-2-1 Firewall (Interface in the Transfer&Management-Aggregation1-2 subnet)	Reachability of cell 1-2-1

Destination network	Next hop	Purpose
Automation Cell1-2-2	Cell1-2-2 Firewall Interface in the Transfer&Management-Aggregation1-2 subnet	Reachability of cell 1-2-1
Default gateway	Enterprise firewall (Interface in the Data Forwarding subnet)	Default gateway for accessing higher-level networks (e.g. office or internet)

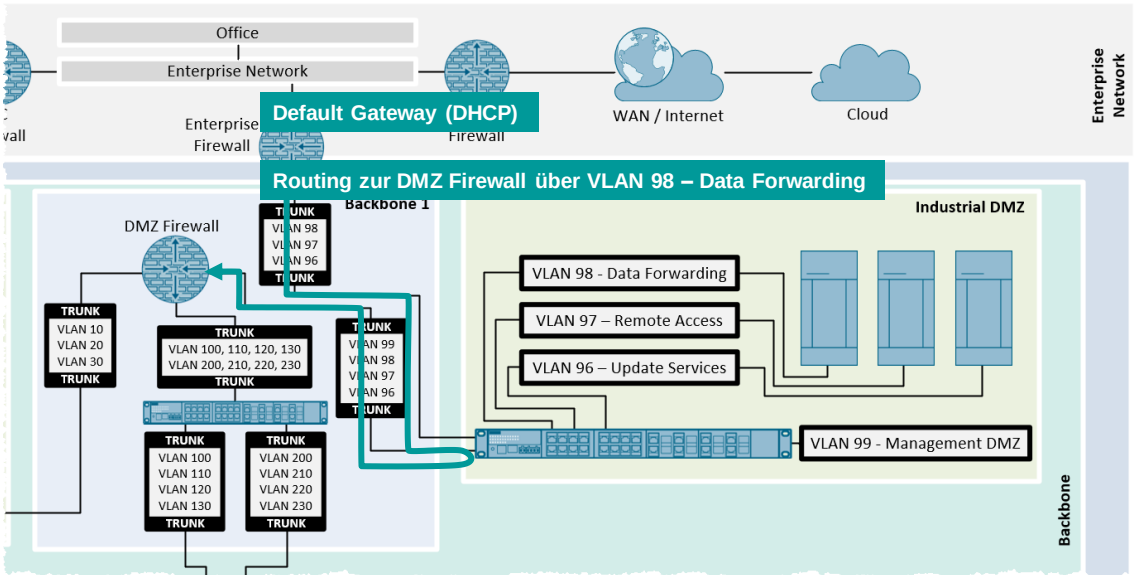
Static routes in the enterprise firewall:

The traffic from the higher-level enterprise networks is routed via the DMZ when the proxy server is in use.

In the event that direction connections also need to be established between enterprise networks and the automation solution, the traffic may also be routed directly via the DMZ firewall using the Data-Forwarding subnet of the DMZ. As a result of their configuration, the lower-level firewall components are then responsible for the routing to all lower-level network segments. The default gateway of the enterprise firewall is obtained from higher-level networks by means of DHCP.

The following graphic shows the routing path of the enterprise firewall.

Figure 2-12



The configuration listed below is required for this routing. Appendix VI – Static routes contains detailed route planning with IP addresses.

Table 2-7

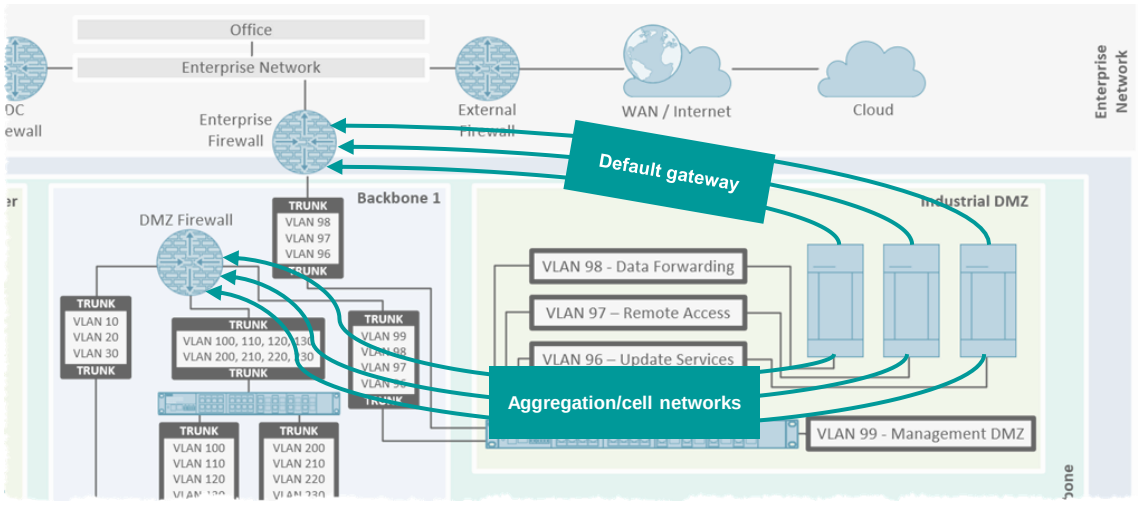
Destination network	Next hop	Purpose
Automation Engineering Automation application Monitoring and Management	DMZ firewall (interface in the Data-Forwarding subnet)	Reachability of the datacenter from the enterprise networks
Transfer&Management-Aggregation1-1 Automation-Aggregation1-1 WLAN Automation-Aggregation1-1 WLAN-Engineering-Aggregation1-1	DMZ firewall (interface in the Data-Forwarding subnet)	Reachability of Aggregation1-1 from the enterprise networks
Transfer&Management-Aggregation1-2 Automation-Aggregation1-2 WLAN Automation-Aggregation1-2 WLAN-Engineering-Aggregation1-2	DMZ firewall (interface in the Data-Forwarding subnet)	Reachability of Aggregation1-2 from the enterprise networks
Automation Cell1-1-1 PROFINET 1 Cell1-1-1	DMZ firewall (interface in the Data-Forwarding subnet)	Reachability of cell 1-1-1 from the enterprise networks
Automation Cell1-1-2 PROFINET 1 Cell1-1-2	DMZ firewall (interface in the Data-Forwarding subnet)	Reachability of cell 1-1-2 from the enterprise networks
Automation Cell1-2-1 PROFINET 2 Cell1-1-2 PROFINET 1 Cell1-1-2	DMZ firewall (interface in the Data-Forwarding subnet)	Reachability of cell 1-2-1 from the enterprise networks
Automation Cell1-2-2	DMZ firewall (interface in the Data-Forwarding subnet)	Reachability of cell 1-2-2 from the enterprise networks
Default gateway	Obtained via DHCP or through coordination with enterprise IT	Default gateway to higher-level enterprise networks

Static routes in the DMZ servers

The servers in the DMZ likewise require static routes to facilitate communication into the aggregation and cell networks. The routing table for this is largely the same as the routing table for the enterprise firewall.

As a rule, the enterprise firewall is used as the default gateway with these servers.

Figure 2-13



The configuration listed below is required for this routing. Appendix VI – Static routes contains detailed route planning with IP addresses.

Table 2-8

Destination network	Next hop	Purpose
Automation Engineering Automation application Monitoring and Management	DMZ firewall (interface in the subnet of the respective server)	Reachability of the datacenter from the enterprise networks
Transfer&Management-Aggregation1-1 Automation-Aggregation1-1 WLAN Automation-Aggregation1-1 WLAN-Engineering-Aggregation1-1	DMZ firewall (interface in the subnet of the respective server)	Reachability of Aggregation1-1 from the enterprise networks
Transfer&Management-Aggregation1-2 Automation-Aggregation1-2 WLAN Automation-Aggregation1-2 WLAN-Engineering-Aggregation1-2	DMZ firewall (interface in the subnet of the respective server)	Reachability of Aggregation1-2 from the enterprise networks
Automation Cell1-1-1 PROFINET 1 Cell1-1-1	DMZ firewall (interface in the subnet of the respective server)	Reachability of cell 1-1-1 from the enterprise networks
Automation Cell1-1-2 PROFINET 1 Cell1-1-2	DMZ firewall (interface in the subnet of the respective server)	Reachability of cell 1-1-2 from the enterprise networks
Automation Cell1-2-1 PROFINET 2 Cell1-1-2 PROFINET 1 Cell1-1-2	DMZ firewall (interface in the subnet of the respective server)	Reachability of cell 1-2-1 from the enterprise networks
Automation Cell1-2-2	DMZ firewall (interface in the subnet of the respective server)	Reachability of cell 1-2-2 from the enterprise networks
Default gateway	Enterprise firewall (interface in the subnet of the respective server)	Default gateway to higher-level enterprise networks

2.2.7 Routing in cell firewalls

Overview

The cell protection firewalls and CPUs with IP forwarding do not have a redundant design in this concept. Nevertheless, sufficient free space should be left when planning the addresses in order to accommodate potential expansions. This means that the first device inside the cell (typically the CPU) receives the fourth IP address in the subnet because the first three addresses are reserved for a possible redundant default gateway.

A reserve should be planned even with the external interfaces of the cell firewalls into the Transfer&Management-Aggregation network. Due to the fact that in the aggregation networks, a high number of network components in the lower address range tend to require management, the following address scheme is recommended.

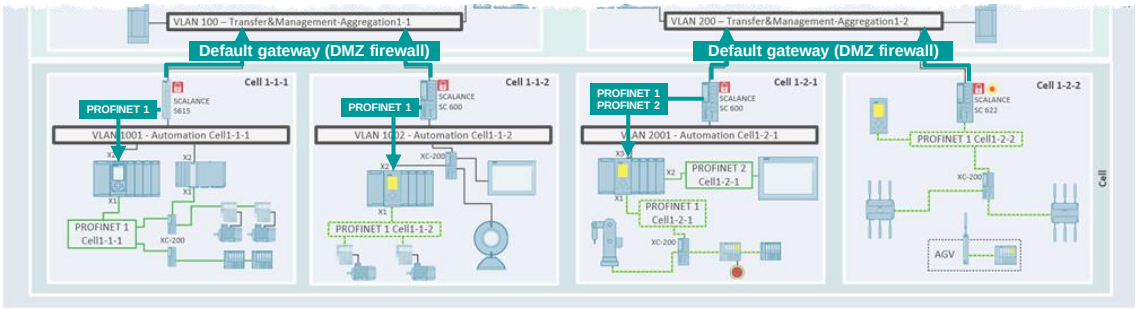
Table 2-9

Component	Interface	IP address
Cell 1-1-1 firewall	internal (automation cell 1-1-1)	10.1.10.1/24
	external (Transfer&Management-Aggregation1-1)	10.0.100.110/24
Cell1-1-2 firewall	internal (automation cell 1-1-2)	10.1.20.1/24
	external (Transfer&Management-Aggregation1-1)	10.0.100.120/24
Cell1-2-1 firewall	internal (automation cell 1-2-1)	10.2.10.1/24
	external (Transfer&Management-Aggregation1-2)	10.0.200.110/24
Cell1-2-1 firewall	internal (automation cell 1-2-2)	10.2.20.1/24
	external (Transfer&Management-Aggregation1-2)	10.0.200.120/24

Static routes into the Transfer&Management-Aggregation network

To ensure the reachability of devices in the CPU's lower-level networks, the cell firewalls require the routes shown in the Figure below. Routing into higher-level networks is performed by the DMZ firewall that is defined as a default gateway.

Figure 2-14



The configuration in the cell protection firewalls as listed below is required for this routing. Appendix VI – Static routes contains detailed route planning with IP addresses.

Table 2-10

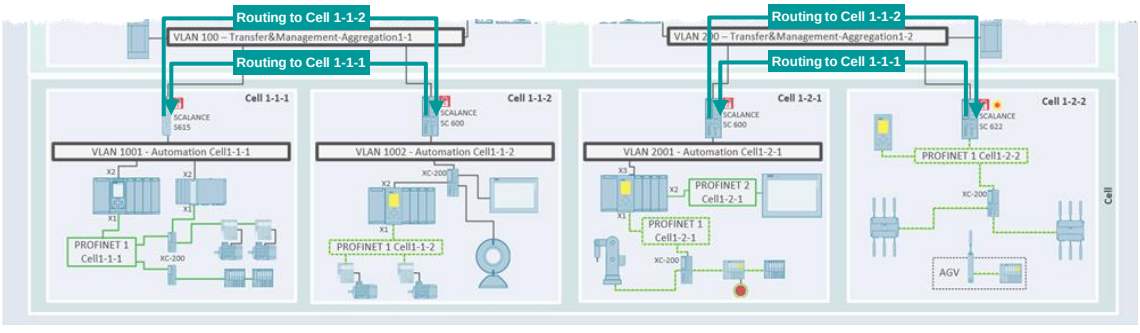
Firewall	Destination	Next hop	Purpose
Cell 1-1-1	PROFINET 1 (Cell1-1-1) Default gateway	CPU Cell1-1-1, *X2* DMZ firewall, *Transfer&Management-Aggregation1-1*	Routing of access to PROFINET devices via the CPU Default route into higher-level networks
Cell 1-1-2	PROFINET 1 (Cell1-1-2)	CPU Cell1-1-2, *X2*	Routing of access to PROFINET devices via the CPU
	Default gateway	DMZ firewall, *Transfer&Management-Aggregation1-1*	Default route into higher-level networks
Cell 1-2-1	PROFINET 1 (Cell 1-2-1) PROFINET 2 (Cell 1-2-1)	CPU Cell1-2-1, *X3*	Routing of access to PROFINET devices via the CPU
	Default gateway	DMZ firewall, *Transfer&Management-Aggregation1-2*	Default route into higher-level networks
Cell1-2-2	Default gateway	DMZ firewall, *Transfer&Management-Aggregation1-2*	Default route into higher-level networks

The routes described above ensure that the communication between individual cells is also routed via the DMZ firewall.

Static routes into other cell networks

It is also possible to route cross-cell communication within an aggregation level over nothing but the associated Transfer&Management-Aggregation subnet. This makes the hop to the DMZ firewall no longer necessary. With regard to availability and performance, communication is not dependent on the aggregation level uplink.

Figure 2-15



To establish this routing scheme, the following additional rules are necessary in the cell firewalls:

Table 2-11

Firewall	Destination	Next hop	Purpose
Cell 1-1-1	Automation Cell1-1-2	Firewall, Cell1-1-2, *Transfer&Management-Aggregation1-1*	Routing of access from cell 1-1-1 to the Automation Cell1-1-2 subnet
	PROFINET 1 Cell1-1-2		Routing of access from cell 1-1-1 to the PROFINET 1 Cell1-1-2 subnet
Cell 1-1-2	Automation Cell1-1-1	Firewall, Cell1-1-1, *Transfer&Management-Aggregation1-1*	Routing of access from cell 1-1-2 to the Automation Cell1-1-1 subnet
	PROFINET 1 Cell1-1-1		Routing of access from cell 1-1-1 to the PROFINET 1 Cell1-1-1 subnet
Cell1-2-1	Automation Cell1-2-2	Firewall, Cell1-2-2, *Transfer&Management-Aggregation1-2*	Routing of access from cell 1-2-1 to the PROFINET-Cell1-2-2 subnet
Cell1-2-2	Automation Cell1-2-1	Firewall, Cell1-2-1, *Transfer&Management-Aggregation1-2*	Routing of access from cell 1-2-2 to the Automation Cell1-2-1 subnet
	PROFINET 1 Cell1-2-1		Routing of access from cell 1-2-2 to the PROFINET 1 Cell1-1-1 subnet
	PROFINET 2 Cell1-2-1		Routing of access from cell 1-2-2 to the PROFINET 2 Cell1-1-1 subnet

2.2.8 Routing to S7-1500 controllers

In the event that CPU also handles the network isolation tasks in the cells, access to the PROFINET nodes is routed through the CPU.

To do this, enable the "IP forwarding" feature in the CPU. No other routers must be defined except for the default gateway. In this case, the CPU receives the first PROFINET address.

The CPUs always receive the following configuration:

Table 2-12

Destination	Next hop	Purpose
Default gateway	Cell protection firewall, Automation-Cell subnet	Routing of traffic into higher-level networks

Note Due to the fact that the S7-1500 does not support free configuration of the routing tables, only subnets that are directly connected with the CPU can be addressed with IP communication from higher-level network segments (e.g. datacenter). Therefore, if using cascading architectures, no direct access is possible from the datacenter to the I/O devices of the cascaded controllers.

Additional information can be found in the "IP forwarding" chapter of the manual "SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication" (\15\ )

2.2.9 Routing in cell devices

If the device is located in a subnet that is isolated by the CPU, then the corresponding interface of the CPU must selected as the default gateway.

If the device is located directly in the automation cell network, then the cell firewall serves as the default gateway.

For the devices in cell 1-1-2, for example, the result is the following configuration for the default gateways:

Table 2-13

Component	Default gateway
Drives	CPU, *X1*
Camera	Cell protection firewall, *Automation Cell-1-1-2*

2.2.10 Routing in aggregation networks

For the devices in the aggregation networks, the corresponding interface of the DMZ firewall is defined as the default gateway.

Table 2-14

Component	Default gateway
Devices in the Automation-Aggregation subnet	DMZ firewall *(Automation-Aggregation interface)*
Devices in the WLAN-Engineering-Aggregation subnet	DMZ firewall *(WLAN-Engineering-Aggregation interface)*
Devices in the WLAN-Automation-Aggregation subnet	DMZ firewall (*WLAN-Automation-Aggregation interface*)
Devices in the Transfer&Management-Aggregation subnet	DMZ firewall (Transfer&Management-Aggregation interface)

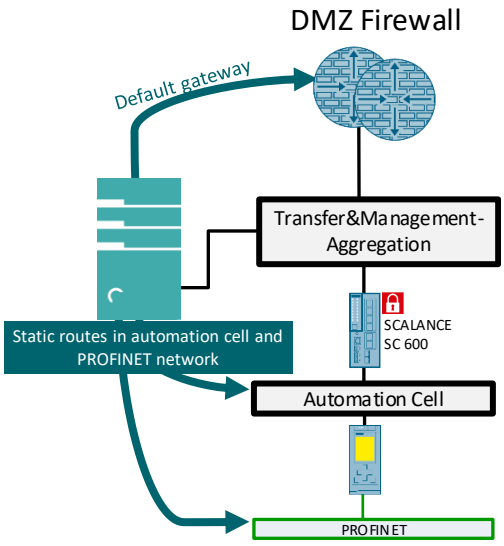
2.2.11 Routing in servers of the Transfer & Management networks on the aggregation level

The servers located in the Transfer&Management-Aggregation networks provide centralized services on the aggregation level. These devices occupy a unique position with regard to routing.

Routes to the cell devices are necessary for the provision of services in the automation cells. The communication path into the datacenter, DMZ and other subnets on the aggregation level is routed via the default gateway.

The routes are stored in the operating system (Windows) as persistent routes.

Figure 2-16



The routing configuration below is the result for such servers.

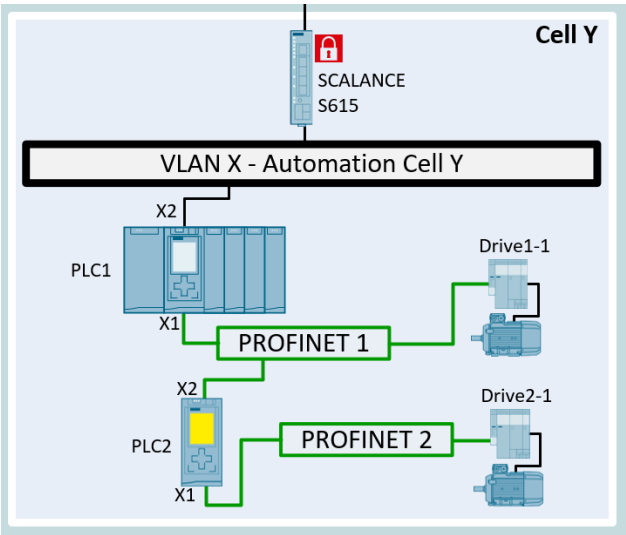
Table 2-15

Destination	Next hop	Purpose
Automation cell networks	Cell protection firewall, Transfer&Management-Aggregation subnet	Routing of traffic into lower-level networks
PROFINET networks		
Default gateway	DMZ firewall, *Transfer&Management-Aggregation* subnet	Routing of traffic into higher-level networks

2.2.12 Routing to cascaded controller architectures

Due to the fact that the S7-1500 CPUs only support IP forwarding, devices located behind cascaded CPUs cannot be reached with OSI layer-3 services.

Figure 2-17



Reachability for the components pictures is as follows:

The components "CPU2" and "Drive1-1" are reachable on OSI layer 3 with IP forwarding through "CPU1". Here, for example, it is possible to access web servers from higher-level networks.

"Drive2-1" is only reachable from higher-level networks via S7 routing for online diagnostics or configuration changes. The S7 routing mechanism (OSI layer 7) offers more flexibility in this case for configuration and diagnostic access. Provided that the intervening subnets in the respective TIA project are known, access through cascaded architectures is possible here as well. For more detailed information on this topic can be found in chapter 11 of manual \10\. Access with OSI layer-3 protocols, for example access to the web server, is not possible here.

2.3 Network structure in the cell level

2.3.1 Requirements for the cell level

The cell level is ordinarily subdivided into many individual cells and must be especially secured against unwanted access because a network interruption in these areas can lead to an immediate production halt.

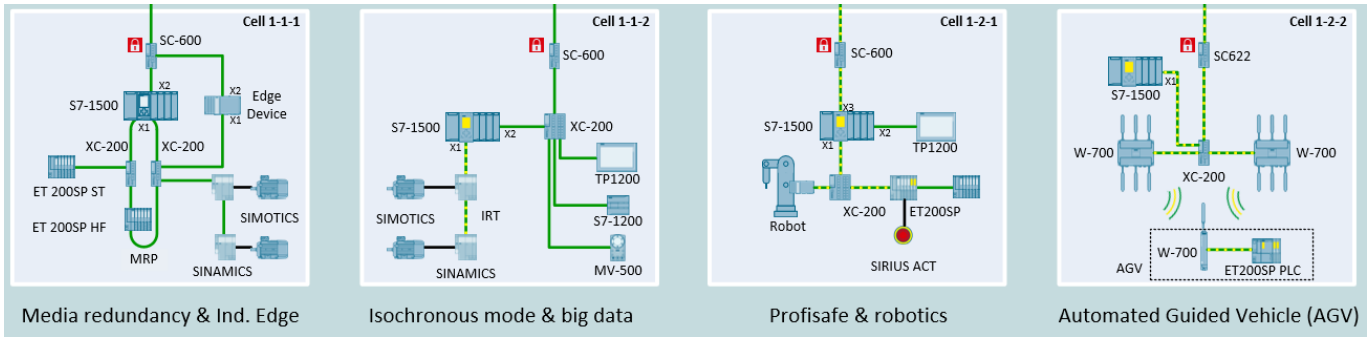
In general, these are the network-relevant requirements that must be verified for each individual cell:

- **Availability**
  Availability can be increased with redundancy mechanisms such as MRP.
- **Security**
  Use of a cell security concept and protection of the cell with a firewall
- **Protection of man and machine**
  Verification according to safety standards and use of functionally safe communication such as PROFIsafe
- **Realtime communication**
  Guarantee true-time, deterministic data transmission through the use of PROFINET I/O
- **Reachability of cell controller and field devices**
  Ensure reachability between cell and higher levels for parameter assignment, diagnostics and data exchange
- **Reusability**
  Simplify reusability of the cell with dynamic name and address assignment
- **Networking of machines**
  Process-related data exchange between machines with the help of OPC UA and Open User Communication (OUC) of PROFINET I/O in case of strict realtime requirements

2.3.2 Use cases

Four typical factory automation applications are depicted in the chosen network concept for the cell level.

Figure 2-18



General properties of the cells

Due to additional network isolation within the cell, the CPU in its role as cell controller requires two interfaces. Alternatively, a communication module such as the CM1542-1 may be used to obtain more interfaces. In general, always pay attention to which functions are required at the

interface and whether the interface can fulfil these functions. One good example is PROFINET IRT, which is only supported on the internal X1 interface of the CPU.

The IP routing feature in the CPUs is required in order to reach devices in the lower-level network of the cell (e.g. with the S7-1500 CPUs) so that IP-based services remain possible. The possibility for S7 routing should also be provided for. Also consider that layer-2-based services such as PROFINET DCP are not possible between networks.

Machine-to-machine communication based on OPC UA necessitates a server and client feature in the CPU. For details, see chapter 3.11.

The selected solution approach that uses the cell security concept is based on a layer 3 separation of the cell from the rest of the network. According to IEC 61784-3-3 (PROFIsafe), the integrated interfaces of the CPU (cells 1-1-1, 1-1-2, 1-2-1) or a 2-port router are needed for network isolation (cell 1-2-2). This cell firewall with routing functionality, present in each cell, in most cases forms the interface between the OEM and the end customer. For details, see chapter 3.8.2.

In this case, the OEM provides the firewall as a part of the machine. The device must support the required functions, such as layer-3 routing, firewall, fixed IP addresses or DHCP, etc. These are based on the requirements of the end customer.

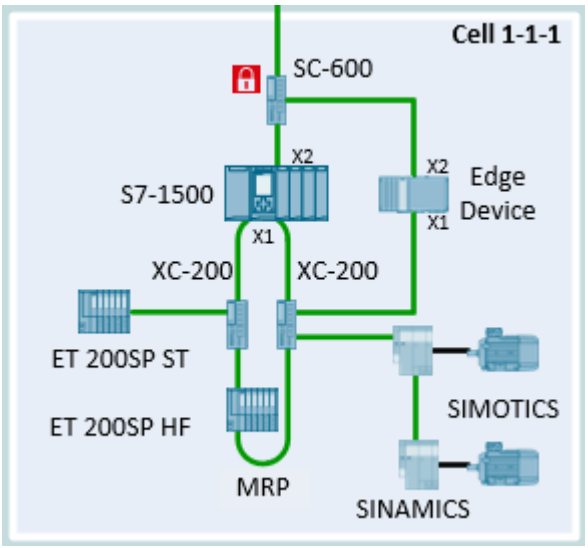
The end customer must define how the machine (and with it, the firewall) will be integrated into the line. In such case, the end customer must consider functions such as name assignment and address assignment, as well as the required routing function.

In the variant described here, fixed IP addresses are used inside the cell. As described in chapter 2.2, unique cross-cell IP addresses are used. In this way it is possible to reach all devices from the datacenter. The necessary configurations for routes and firewall rules are easier to implement than they would be if using NAT.

Cell 1-1-1 – media redundancy and Industrial Edge

Availability is an important consideration in cell 1-1-1. To ensure availability, an MRP ring is created between the controller and the switches. Additional nodes are connected from the switches. For example, non-MRP-capable nodes are reached via stubs (ET 200SP ST / SINAMICS converters). In addition, it is possible to run automation-specific software thanks to the presence of an Industrial Edge device.

Figure 2-19



The Media Redundancy Protocol (MRP) is specified in the IEC 61158 Type 10 "PROFINET" standard. The ring may only consist of devices that support this function. The maximum number of ring participants is 50. Otherwise, reconfiguration times of more than 200 ms may occur. All devices connected within the ring topology must be members of the same redundancy domain and must possess the same port settings.

PROFINET RT operation is possible with the use of MRP. PROFINET IRT operation, on the other hand, is only possible with the MRPD extension (Media Redundancy with Planned Duplication of frames). For the devices that support MRP and MPRD, please refer to the FAQ \7\, "Which IO controllers and IO devices support the following functions in STEP 7 (TIA Portal)...". PROFINET RT communication is interrupted if the reconfiguration time of 200 ms is greater than the selected response watchdog time of the I/O devices. In particular when using PROFIsafe, the reconfiguration time must be considered in the safety watchdog times.

Additional guides on MRP:

- In the PROFINET function manual in the chapter on media redundancy \12\
- In the application example "Configuration of a Ring Topology Based on MRP" – \13\.
- If RSTP is also being used, the FAQ "What should you watch out for when configuring the PROFINET MRP ring with regard to RSTP packages (Rapid Spanning Tree Protocol)?" (\14\) provides additional information.

The Industrial Edge device requires not only a connection into the lower-level cell network for querying machine data, but also one into the higher-level plant network in order to provide the data it processes. In this way, the device can query information from the PROFINET devices via layer-2 access. Also make sure that relevant services are reachable for the edge device (such as Edge Management, NTP, etc.).

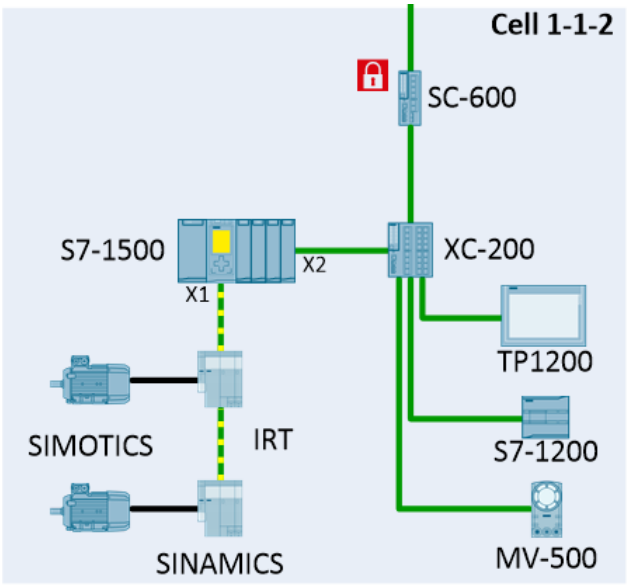
Additional guides on Edge in the automation cell:

- Chapter 3.14.

Cell 1-1-2 – isochronous mode and big data

Data exchange under strict realtime requirements is the focus in cell 1-1-2. It plays a crucial role especially with motion applications. The implementation relies on PROFINET IRT. Like with MRP, all devices located in the IRT linear topology must support the IRT function and must be part of the same synchronization domain.

Figure 2-20



The strict realtime requirement necessitates precise design of the network as well as of the data exchange. In the process, parameters such as network bandwidth (typically 100 Mbit/s), bus send clock, application cycle as well as the line depth must be accounted for.

Besides PROFINET IRT communication, PROFINET RT (for example PROFIsafe) and NRT (for example OPC UA) can be transmitted over the same line. In the cell, the converters require not only isochronous data exchange but also safety-focused communication.

Additional guides on PROFIsafe and IRT in the cell:

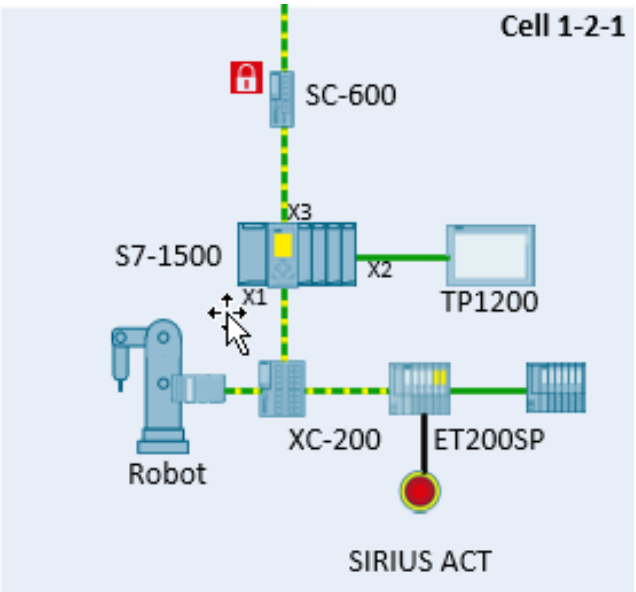
- Chapter 3.8.

The topic of big data, for example transmission of machine-adjacent images and videos, has been considered in the cell. The camera images are transmitted via gigabit-capable devices from the SCLANCE SC-600 and XC-200 families.

Cell 1-2-1 – PROFIsafe and robotics

Because of a robotics application, the topic of safety-related communication is addressed in cell 1-2-1.

Figure 2-21



PROFIsafe is used for safety-related communication within the cell, guaranteeing requirements such as data integrity (data are current and correct), authenticity (correct recipient) and prompt transmission (timeliness) between the partners.

The so-called "Flexible F-Link" is available for safety-related communication across cell/subnet boundaries. Here, the Flexible F-Link relies on standard communication mechanisms of the CPUs (Open User Communication).

Additional guides on PROFIsafe:

- Chapter 3.8

For the robot it must be ensured that the PROFINET requirements (such as supported I/O update time, PROFIsafe, LLDP, etc.) are met appropriately for the application. The link to the robot for commissioning and servicing is typically facilitated with a local interface. In the cell level in general, thought should be given to whether a port will be reserved specifically for servicing purposes so as to connect tools that require layer-2-based services.

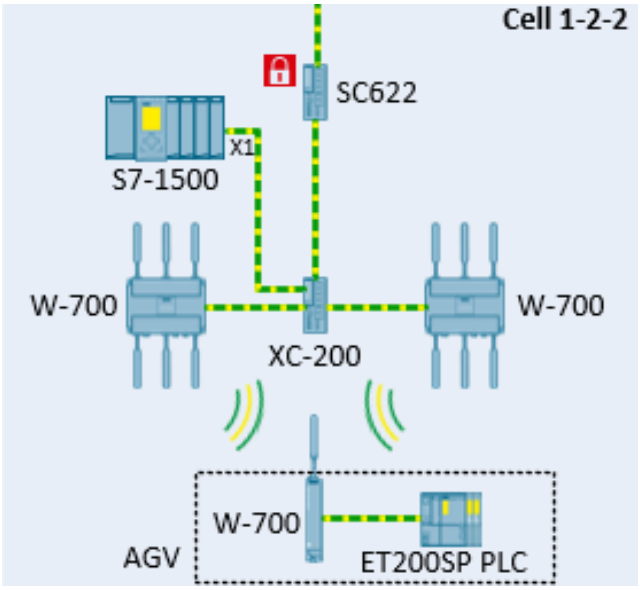
Additional guides on PROFINET:

- Chapter 3.7

Cell 1-2-2 – AGV

The focus in cell 1-2-2 is on AGVs (Automated Guided Vehicles) and mobile automation solutions. Highlights are topics and technologies such as PROFINET I-Device, IWLAN in general and in combination with PROFIsafe.

Figure 2-22



The intrinsically safe AGV is in an I-Device relationship to a master controller and communicates its data over IWLAN using PROFIsafe.

Additional guides on I-Devices in the cell:

- Chapter 3.7.

To ensure deterministic communication, the iPCF or iPCF-MC feature makes sense from a technical standpoint and may be required depending on the application. To ensure PROFIsafe addresses are unique, the network of the cells is safely isolated from the overlying plant network of the SCALANCE SC622. In this way it is possible to achieve independence from other cells; now only the uniqueness of the PROFIsafe addresses within the cells must be ensured.

Additional guides on PROFIsafe and WLAN in the cell:

- Chapter 3.8
- Chapter 3.13.

Because there may be a significant number of vehicles in a facility and commissioning efforts must be kept to a minimum, identical configurations are often used on the AGVs – provided that this is feasible from a safety standpoint.

2.3.3 Quantity structure

The applications and the depicted configurations in the cells are intended as examples only. A minimal quantity structure has been depicted deliberately for the sake of simplicity. In practice, cells may contain hundreds of devices. There may also be multiple controllers that share a

control task in the cell. In these cases it is important to note the following quantity structure considerations.

PROFINET line depth

The maximum line depth depends on the update time of the PROFINET system (RT/IRT) and the network components used (for example, the various cycle times of the switches have a major effect on the line depth).

PROFINET load calculation

By default with SIMATIC controllers, 50% of the maximum available bandwidth of the PROFINET X1 interface is reserved for PROFINET I/O (data feed from the CPU to the network). How much of this is actually used depends on the update time, the number of I/O devices and the size of the I/O data.

Further details on PROFINET line depth and load calculation

- PROFINET installation guidelines from PI: \9\

Bandwidth and queue size

When choosing hardware, attention should be paid to the bandwidth that must be supported and the queue size of the interface. The interface may become saturated, especially with larger linear topologies with high communication load (RT and NRT). In such cases, design in advance is recommended, for example with the design program SINETPLAN: \10\

Max. nodes in the MRP ring

An MRP ring can contain up to 50 subscribers in the default case. For further information on MRP configurations and quantity structures, please refer to the manuals for the switches: \56\

Address ranges (IP address band, safety addresses)

The quantity structures with regard to IP addresses are defined by the subnet masks used. In this case, the 255.255.0.0 /16 mask (for 65,534 devices) or the 255.255.255.0 /24 mask (for 254 devices) are frequently chosen.

With safety I/O devices, the safety addresses also have to be considered. Here, a distinction is made between two types of addresses. With the PROFIsafe address type 1, a maximum of 1022 different F target addresses may be assigned. With PROFIsafe address type 2, 65,534 devices may receive a unique safety address.

Special considerations in nested networks

If the S7-1500 is acting as an IP router to other lower-level networks within a cell (example cell 1-1-1, Figure 2-19 or cell 1-1-2, Figure 2-20), attention must be paid to limiting IP forwarding to a lower-level network. This function stores static routes on the basis of the IP addresses. It is not currently possible to add more routes.

2.3.4 Scalability

When scaling a cell, the focus is on the controller as a core component. In most cases, it defines the size of the cell based on its performance, maximum quantity structure and supported functions.

The number and properties of the interfaces must be considered in a network concept. With the S7-1500 controllers for example, there are devices with one interface (e.g. the CPU 1511-1 PN) as well as devices with three interfaces (e.g. the CPU 1518-4 PN/DP). It is possible to increase the number of interfaces by using communication modules (CP 1543-1, CM 1542-1). In such case, the functionality that the interface needs to support is important, for example PROFINET RT or IRT. For details, refer to the technical specifications of the devices.

Further details with regard to functionality of the interfaces are explained in chapter 3.7.

2.3.5 Components used

The example for the cell level shown in Figure 2-18 has been constructed and validated with the following core components from Siemens:

Table 2-16

Components	Description
SCALANCE XC200	Any coupling switches to the cell level from the XC/XF/XB/XP200 switch series
SIMATIC S7 controller	S7-1500 controller • At least 2 interfaces • IP forwarding • OPC UA server/client • S7 routing All common PROFINET S7 controllers with current firmware support MRP and forward BPDUs (passive listening telegrams). You can find an overview in this article: https://support.industry.siemens.com/cs/ww/en/view/102325771
Distributed I/O	ET 200SP station with IM155-6 PN HF All common PROFINET I/O devices with current firmware support MRP and forward BPDUs. You can find an overview in this article: https://support.industry.siemens.com/cs/ww/en/view/102325771
SCALANCE SC622-2C	• Layer-3 routing • Firewall • Network isolation according to IEC 61784-3-3 ("PROFIsafe") • 2 ports
SCALANCE S615	• Layer-3 routing • Firewall • 4 ports

2.4 Network structure in the aggregation level

2.4.1 Requirements for the aggregation level

The task of the aggregation network is to:

- interface multiple cells
- facilitate communication relationships between the cells
- link with the backbone network

The aggregation level commonly encompasses a closed area of an industrial network, for example a hall of a factory or a production area within a hall.

Physical separation

Depending on the necessary physical separation within the industrial network, both electrical (up to 100 m) as well as optical connections (e.g. 1 Gbit multimode up to 750 m, singlemode up to 120 km) may be used.

Availability

A ring topology is used to achieve the required availability of the aggregation network. This offers a useful redundancy firstly because one line can fail without consequences; secondly, costs in comparison to a redundant star structure are actually lower because when compared to a linear topology only one additional connection is needed between two switches.

WLAN

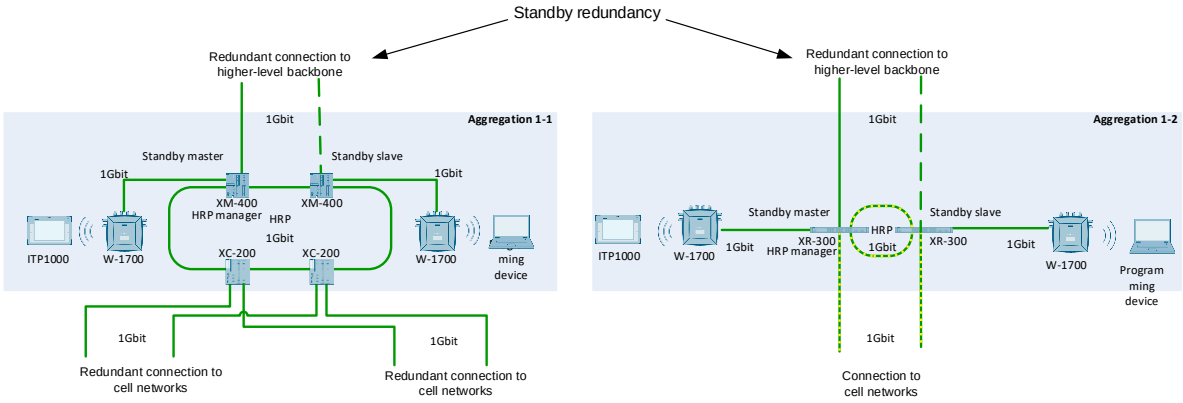
If there are requirements for a wireless network, the aggregation network offers access points for connecting to the necessary WLAN. The physical footprint of the aggregation ring topology can usually be chosen within the space such that it supports the placement of the WLAN APs for the required radio coverage. Unlike copper and fiber-optic cables, wireless transmission methods use radio waves. The propagation characteristics of the electromagnetic waves can differ considerably and depend on the spatial environment and the installed wireless infrastructure.

The radio link is established to the mobile nodes by connecting a SCALANCE W access point to the aggregation network. Currently, data rates of up to 1733 Mbps can be achieved with SCALANCE W-1700 and the 802.11ac Wave 2 standard.

2.4.2 Topology

The following diagram shows the topology of the two aggregation networks for this network concept.

Figure 2-23



Redundancy in the aggregation network

The rings are monitored with the ring protocol HRP (High Speed Redundancy Protocol). The switches are connected to each other via ring ports. The XM-400-1 is configured to be the redundancy manager (RM). The other switches are redundancy clients. Using test telegrams, the redundancy manager checks that the ring is free of interruptions. The redundancy manager sends test telegrams via the ring ports and checks their receipt at the other ring port. The redundancy clients forward the test telegrams. If the ring is broken and the test telegrams from the RM no longer arrive at the other ring port, the RM interconnects its two ring ports and immediately informs the redundancy clients about the change. The reconfiguration time following the interruption of the ring is at most 300 ms.

Connection to backbone

The aggregation network is redundantly coupled to the backbone network via standby redundancy.

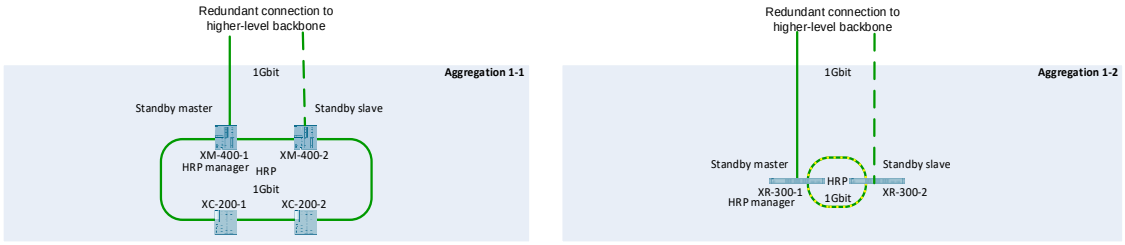
The standby feature is an extension of HRP and has the same deterministic failover time of at most 300 ms.

Standby redundancy is a procedure by which rings, each ring secured by itself with high-speed redundancy, are redundantly coupled. In the ring, a master/slave device pair is configured in which each monitors the other via its ring ports. In the event of a fault, data traffic is re-routed from one Ethernet connection (standby port of the master / standby server) to another Ethernet connection (standby port of the slave).

In the industrial network depicted, standby redundancy is configured for coupling to the backbone on the side of the respective aggregation. For Aggregation 1 here, XM-400-1 is the standby master and XM-400-2 is the standby backup.

The following diagram shows the redundant connection to a higher-level backbone network via standby redundancy.

Figure 2-24



Additional guides on HRP and standby links:

- Configuration of HRP Rings with Standby Link
  https://support.industry.siemens.com/cs/ww/en/view/109739600

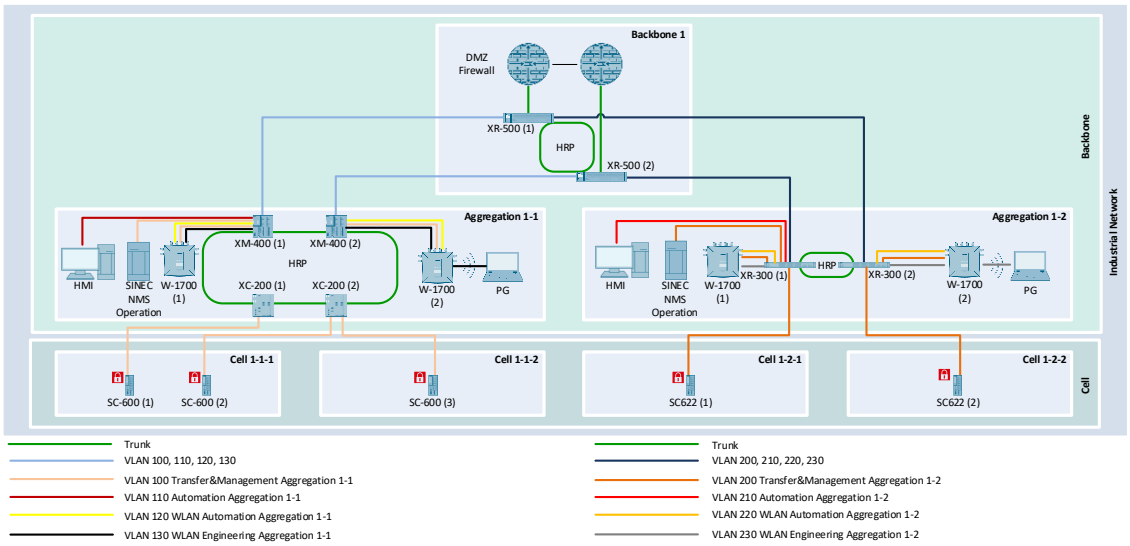
Bandwidth

Rates of 1 Gbit/s are intended for the link to the higher-level backbone both within the aggregation and for connecting to the cells.

2.4.3 VLAN segmentation

The following schematic diagram shows the necessary settings and VLAN assignments for both the terminal devices as well as the network ports in order to facilitate the layer-3 concept from chapter 2.2.

Figure 2-25



VLAN table for Aggregation 1-1

Table 2-17

Device	Port	Function	VLAN ID 1	VLAN ID 100	VLAN ID 110	VLAN ID 120	VLAN ID 130
XM-400 (1)	1.1	Trunk XC-200	T	T	T	T	T
	1.2	Trunk XM-400	T	T	T	T	T
	1.3	Uplink XR-500	M	M	M	M	M
	1.4	W-1700	-	M	-	M	M
	1.5	HMI	-	-	U	-	-
	1.6	SINEC NMS	-	U	-	-	-
XM-400 (2)	1.1	Trunk XC-200	T	T	T	T	T
	1.2	Trunk XM-400	T	T	T	T	T
	1.3	Uplink XR-500	M	M	M	M	M
	1.4	W-1700	-	M	-	M	M
XC-200 (1)	0.1	Trunk XM-400	T	T	T	T	T
	0.2	Trunk XC-200	T	T	T	T	T
	0.3	SC-600	-	U	-	-	-
XC-200 (2)	0.1	Trunk XM-400	T	T	T	T	T
	0.2	Trunk XC-200	T	T	T	T	T
	0.3	SC-600	-	U	-	-	-
	0.4	SC-600	-	U	-	-	-
SC-600 (1)	0.1	XC-200	-	U	-	-	-
SC-600 (2)	0.1	XC-200	-	U	-	-	-
SC-600 (3)	0.1	XC-200	-	U	-	-	-

T: Tagged port, U: Untagged port, T: Trunk port, M: Member

VLAN table for Aggregation 1-2

Table 2-18

Device	Port	Function	VLAN ID 1	VLAN ID 200	VLAN ID 210	VLAN ID 220	VLAN ID 230
XR-300 (1)	0.1	Trunk XR-300	T	T	T	T	T
	0.2	Trunk XR-300	T	T	T	T	T
	0.3	Uplink XR-500	M	M	M	M	M
	0.4	W-1700	-	M	-	M	M
	0.5	HMI	-	-	U	-	-
	0.6	SINEC NMS	-	U	-	-	-
XR-300 (2)	0.1	Trunk XR-300	T	T	T	T	T
	0.2	Trunk XR-300	T	T	T	T	T
	0.3	Uplink XR-500	M	M	M	M	M
	0.4	W-1700	-	M	-	M	M
SC-622 (1)	0.1	XR-300	-	U	-	-	-
SC-622 (2)	0.1	XR-300	-	U	-	-	-

T: Tagged port, U: Untagged port, T: Trunk port, M: Member

2.4.4 Scalability

Due to the chosen ring topology, it is easy to scale on the aggregation level by adding more switches to the ring, for example in order to encompass more cells. The HRP ring supports up to 50 switches for this purpose.

When doing so, make sure not to overload the bandwidth of the uplink to the backbone with too many connected cells or systems. An overbooking factor of 1:20 may be used here as a rule of thumb, but it will depend on the specific application. The term "overbooking factor" refers to the ratio of uplink bandwidth to the sum of the possible access port bandwidth.

2.4.5 Components used

The aggregation network has been designed and validated with the following components.

Table 2-19

Components	Description
XC-200 XR-300WG XM-400	Coupling switches for use in the aggregation level can come from the XC/XF/XB/XP-200, X/XR-300, XM-400 and XR-500 series.
W-1700	WLAN components in the aggregation level can come from the W-700 and W-1700 series.

2.4.1 Configuration of components

Aggregation 1-1

Parameter	Value	Value	Value	Value
System name	XM400-1	XM400-2	XC200-1	XC200-2
IP address	10.0.100.10/24	10.0.100.11/24	10.0.100.12/24	10.0.100.13/24
Default gateway / DNS/NTP server	10.0.100.1	10.0.100.1	10.0.100.1	10.0.100.1
FQDN	xm400-1. aggregation11. factory	xm400-2. aggregation11. factory	xc200-1. aggregation11. factory	xc200-2. aggregation11. factory

Parameter	Value	Value	Value	Value
System name	W1788-1	W1788-2	SC600-1	SC600-2
IP address	10.0.100.20/24	10.0.100.21/24	10.0.100.30/24	10.0.100.40/24
Default gateway / DNS/NTP server	10.0.100.1	10.0.100.1	10.0.100.1	10.0.100.1
FQDN	w1788-1. aggregation11. factory	w1788-2. aggregation11. factory	sc600-1. aggregation11. factory	sc600-2. aggregation11. factory

Aggregation 1-2

Parameter	Value	Value	Value	Value
System name	XR300-1	XR300-2	W1788-1	W1788-2
IP address	10.0.200.10/24	10.0.200.11/24	10.0.200.20/24	10.0.200.21/24
Default gateway / DNS/NTP server	10.0.200.1	10.0.200.1	10.0.200.1	10.0.200.1
FQDN	xr300-1. aggregation12. factory	xr300-2. aggregation12. factory	w1788-1. aggregation12. factory	w1788-2. aggregation12. factory

Parameter	Value	Value
System name	SC600-1	SC600-2
IP address	10.0.200.30/24	10.0.200.40/24
Default gateway / DNS/NTP server	10.0.200.1	10.0.200.1
FQDN	sc600-1. aggregation12. factory	sc600-2. aggregation12. factory

2.5 Network structure in the backbone level

2.5.1 Requirements for the backbone level

One task of the backbone network is to interface the aggregation networks. Another is to ensure the link to the industrial datacenter, the industrial DMZ as well as to the enterprise network.

The backbone network must do the following:

- Via the enterprise firewall, it control communication into the enterprise network.
- It redundantly couples all lower-level aggregation network together.
- Via the DMZ firewall, it controls the communication into the DMZ and the datacenter.
- It redundantly connects the DMZ and datacenter network.
- It controls the communication using the DMZ / enterprise firewall.

Positioning and physical separation

The backbone is often at a central point in the industrial network, for example in the place where the lines connecting the various halls or buildings come together and it is possible to guarantee a connection to the industrial datacenter, DMZ and enterprise network.

Depending on the necessary physical separation within the industrial network, both electrical (up to 100 m) as well as optical connections (e.g. 1 Gbit multimode up to 750 m, singlemode up to 120 km) may be used.

Industrial datacenter

The industrial datacenter is an integral part of the industrial network; it serves to host applications essential for manufacturing/production, such as:

- Automation software
- Network management system
- Central user management
- Manufacturing execution system
- Visualization

The design of the industrial datacenter provides availability, security, scalability and flexibility.

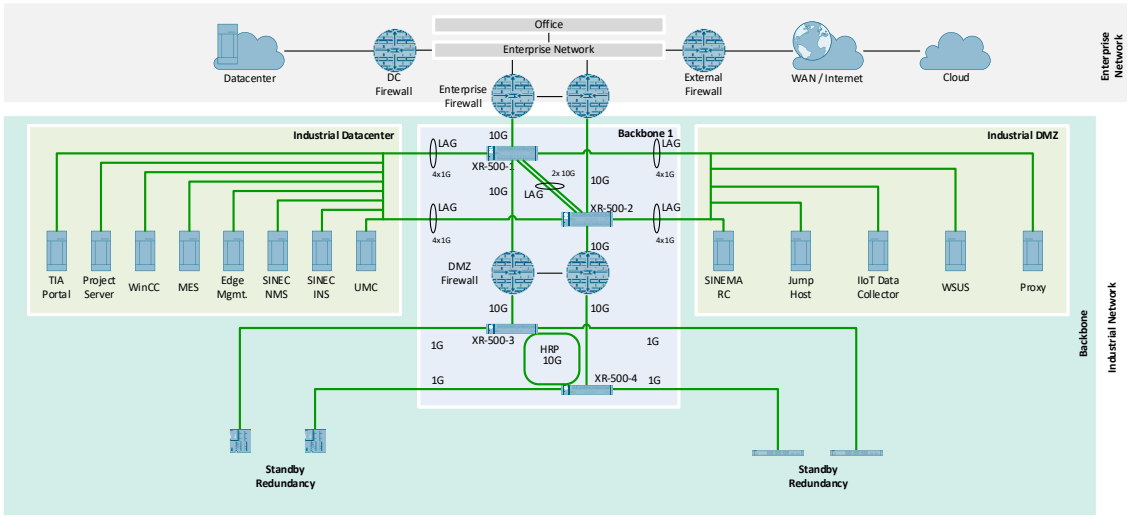
DMZ

The industrial DMZ refers to a specially controlled network. It represents a buffer zone and facilitates secure communication between the industrial network and the enterprise network. The communication connections in this case are controlled by the enterprise firewall or the DMZ firewall. The industrial DMZ contains applications and systems for remote access, communications forwarding (proxy) and software update.

2.5.2 Topology

The Figure below shows the redundant structure of the backbone network.

Figure 2-26



Redundancy in the backbone network

The redundancy mechanisms used in the backbone network are Link Aggregation (LAG) and HRP.

The upper backbone switches are redundantly coupled to one another with LAG. LAG is a method by which multiple (here, two) physical LAN ports are combined to make one logical channel. LACP (Link Aggregation Control Protocol) is used to guard against faults due to misconfigurations or incorrect cable connection.

The lower backbone switches are coupled to one another with HRP and, in the aggregation direction, with standby redundancy. This enables a predictable (deterministic) failover time of at most 300 ms in the event of an error. Here, standby redundancy is configured on the aggregation switch side, which facilitates independent switchover between the various aggregation networks in the event of a fault.

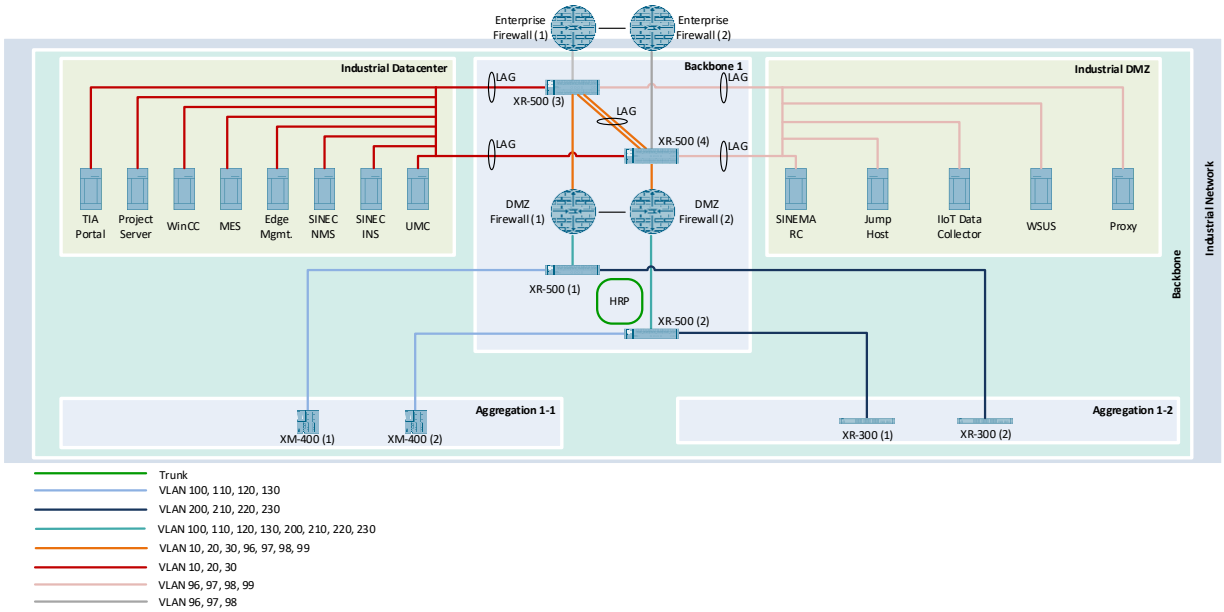
Bandwidth

All backbone switches are connected with fiber-optic cable to each other (and in the DMZ direction and enterprise firewall direction) with 10 Gbit/s of bandwidth. To connect the hosts in the virtual datacenter, in the datacenter proper and in the DMZ, 4 LAG ports of 1 Gbit/s each are used. The aggregation networks are connected via 1 Gbit/s ports.

2.5.3 VLAN segmentation

The following schematic diagram shows the necessary settings and VLAN assignments for both the terminal devices as well as the network ports in order to facilitate the layer-3 concept from chapter 2.2.

Figure 2-27



The following Tables show in detail which VLAN settings are necessary on each device and port, as well as their function.

Note

The VLAN table for the XR-500 (3) and XR-500 (4) may vary.

If the applications are not managed in a virtualized server, then set the ports as untagged member (U) of the VLAN. Telegrams sent from this VLAN are forwarded without a VLAN tag.

If the connection is made via a virtual switch or if the operating system has an 802.1Q driver, then the port is a member of a VLAN.

VLAN tables for the backbone

The following Table shows the VLAN settings when using a virtualized server.

Table 2-20

Device	Port	Function	VLAN ID 1	VLAN ID 100	VLAN ID 110	VLAN ID 120	VLAN ID 130	VLAN ID 200	VLAN ID 210	VLAN ID 220	VLAN ID 230
XR-500 (1)	0.1	Trunk XR-500-2	T	T	T	T	T	T	T	T	T
	0.2	Trunk XR-500-2	T	T	T	T	T	T	T	T	T
	0.3	Trunk uplink, DMZ firewall	T	T	T	T	T	T	T	T	T

Device	Port	Function	VLAN ID 1	VLAN ID 100	VLAN ID 110	VLAN ID 120	VLAN ID 130	VLAN ID 200	VLAN ID 210	VLAN ID 220	VLAN ID 230
	1.1	Downlink XM-400-1	M	M	M	M	M	-	-	-	-
	1.2	Downlink XR-300-1	M	-	-	-	-	M	M	M	M
XR-500 (2)	0.1	Trunk XR-500-1	T	T	T	T	T	T	T	T	T
	0.2	Trunk XR-500-1	T	T	T	T	T	T	T	T	T
	0.3	Trunk uplink, DMZ firewall	T	T	T	T	T	T	T	T	T
	1.1	Downlink XM-400-2	M	M	M	M	M	-	-	-	-
	1.2	Downlink XR-300-2	M	-	-	-	-	M	M	M	M
DMZ firewall (1)	1	Downlink XR-500-1	-	M	M	M	M	M	M	M	M
DMZ firewall (2)	1	Downlink XR-500-2	-	M	M	M	M	M	M	M	M

T: Tagged port, U: Untagged port, T: Trunk port, M: Member

Table 2-21

Device	Port	Function	VLAN ID 10	VLAN ID 20	VLAN ID 30	VLAN ID 96	VLAN ID 97	VLAN ID 98	VLAN ID 99
XR-500 (3)	0.1	Trunk downlink, DMZ firewall	T	T	T	T	T	T	T
	0.2	Trunk LAG XR-500	T	T	T	T	T	T	T
	0.3	Trunk LAG XR-500	T	T	T	T	T	T	T
	0.4	Uplink, enterprise firewall	-	-	-	M	M	M	-
	1.1-1.4	LAG datacenter	M	M	M	-	-	-	-
	1.5-1.8	LAG DMZ	-	-	-	M	M	M	M
XR-500 (4)	0.1	Trunk downlink, DMZ firewall	T	T	T	T	T	T	T
	0.2	LAG XR-500	T	T	T	T	T	T	T
	0.3	LAG XR-500	T	T	T	T	T	T	T
	0.4	Uplink, enterprise firewall	-	-	-	M	M	M	-
	1.1-1.4	LAG datacenter	M	M	M	-	-	-	-
	1.5-1.8	LAG DMZ	-	-	-	M	M	M	M
DMZ firewall (1)	2	Uplink XR-500-3	M	M	M	M	M	M	M
DMZ firewall (2)	2	Uplink XR-500-4	M	M	M	M	M	M	M
Enterprise firewall (1)	1	Downlink XR-500-3	-	-	-	M	M	M	-
Enterprise firewall (2)	1	Downlink XR-500-4	-	-	-	M	M	M	-

T: Tagged port, U: Untagged port, T: Trunk port, M: Member

2.5.4 Scalability

The design of the backbone network provides scalability and flexibility. The number of aggregation networks that can be connected initially scales with the number of uplink ports available from the backbone switches. This can be up to 48 ports depending on the model chosen. If even more aggregation networks need to be connected, then the HRP ring between the backbone switches can simply be expanded with additional devices.

HRP supports up to 50 devices for this. Using the combination of HRP and standby redundancy, multiple aggregation rings can be redundantly coupled to a backbone ring, depending on port availability. HRP and standby redundancy are feasible with small to very large networks.

For smaller networks, it is also possible to combine backbone and aggregation, for instance with a large ring that assumes the function of connecting to the DMZ firewall as well as of connecting directly to the cells.

2.5.5 Components used

The backbone network has been designed and validated with the following components.

Table 2-22

Components	Description
XR-500	Coupling switches for use in the backbone can come from the XR-500 series.
DMZ firewall Enterprise firewall	The firewalls used here meet the requirements for performance and safety in the event of a failure.

2.5.6 Configuration of components

Backbone 1

Parameter	Value	Value	Value	Value
System name	XR500-1	XR500-2	XR500-3	XR500-4
IP address	10.0.10.10/24	10.0.10.11/24	10.0.10.12/24	10.0.10.13/24
Default gateway / DNS/NTP server	10.0.10.1	10.0.10.1	10.0.10.1	10.0.10.1
FQDN	xr500-1. backbone.factory	xr500-2. backbone.factory	xr500-3. backbone.factory	xr500-4. backbone.factory

Parameter	Value	Value	Value	Value
System name	Enterprise-Firewall-1	Enterprise-Firewall-2	DMZ-Firewall-1	DMZ-Firewall-2
IP address	10.0.10.20/24	10.0.10.21/24	10.0.10.30/24	10.0.10.31/24
Default gateway / DNS/NTP server	10.0.10.1	10.0.10.1	10.0.10.1	10.0.10.1
FQDN	enterprise-firewall-1. backbone.factory	enterprise-firewall-1. backbone.factory	dmz-firewall-1. backbone.factory	dmz-firewall-2. backbone.factory

2.6 Central network services

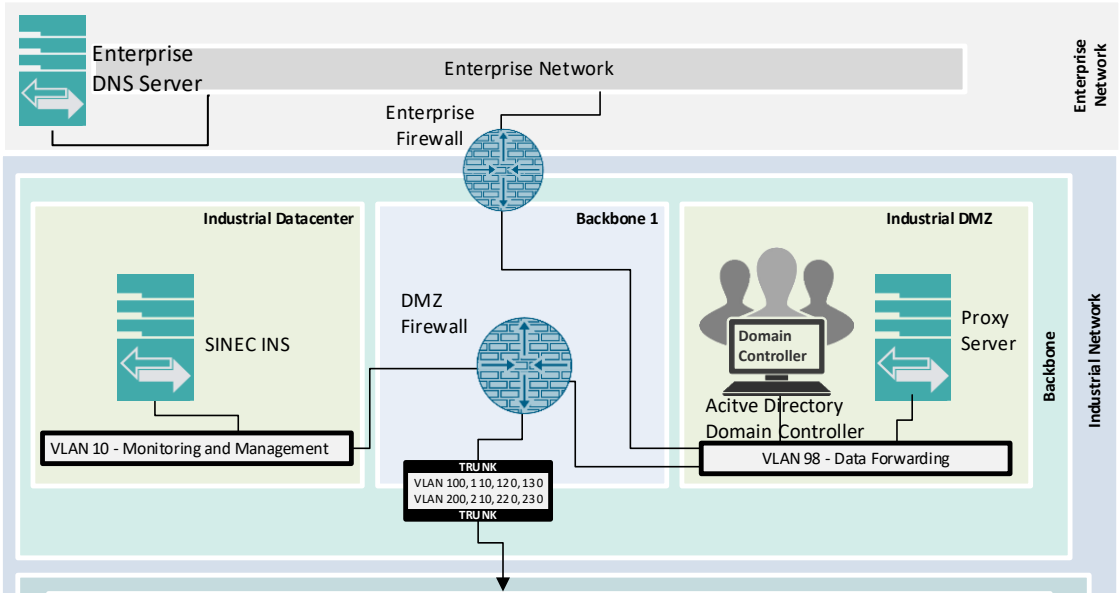
The following chapter explains the establishment of basic services in the network. For supplemental information on this topic, please refer to Appendix VIII – Basic configuration of the firewalls.

Components for services

To provide these services, components used include SINEC INS and a Microsoft Active Directory domain controller as a management instance and a DNS server for the PC stations. The industrial DMZ also contains a proxy server for management and monitoring of connections into higher-level enterprise networks and/or the internet.

The diagram below shows an overview of where these core services are placed in the backbone and the overlying enterprise network.

Figure 2-28



Other services are central network monitoring, update services and Windows update services. These components and services are explained in greater detail in the chapters that follow.

Required firewall rules

The DHCP, DNS and NTP services are provided for all connected devices centrally in each subnet via the corresponding firewall. The following rule sets must be defined in the firewalls for this purpose:

Table 2-23

Service	Source	Destination	Destination port
DHCP	All subnets on the internal interfaces of the firewall	Internal interfaces of the firewall	UDP, 67 + 68
DNS			UDP / TCP, 53
NTP			UDP 123

Base configurations

The following interface configurations are recommended as basic settings for these services.

SINEC INS

Table 2-24

Parameter	Value
IP address	10.0.10.110/24
Default gateway / DNS/NTP server	10.0.10.1
Hostname	SINECINS
Active Directory integration	None, Linux system
FQDN (defined in SINEC INS)	sinecins.datacenter.factory (statically defined in SINEC INS or domain controller)

SINEC NMS

Table 2-21

Parameter	Value
IP address	10.0.10.120/24
Default gateway / DNS/NTP server	10.0.10.1
Hostname	SINECNMS
Active Directory integration	Yes
FQDN (via domain controller or SINEC INS)	sinecnms.datacenter.factory

Microsoft Active Directory domain controller

Table 2-25

Parameter	Value
IP address	10.0.98.10/24
Default gateway / DNS/NTP server	10.0.98.1
Hostname	FACTORYDC
FQDN	factorydc.factory

Proxy server

Table 2-26

Parameter	Value
IP address	10.0.98.20/24
Default gateway / DNS/NTP server	10.0.98.1
Hostname	PROXYSERV
Active Directory integration	Depends on operating system
FQDN (via domain controller or SINEC INS)	proxyserv.dmz.factory (statically defined in SINEC INS or domain controller)

Corporate update server

Table 2-27

Parameter	Value
IP address	10.0.98.30/24
Default gateway / DNS/NTP server	10.0.98.1
Hostname	UPDATESERVER
Active Directory integration	Yes
FQDN (via domain controller or SINEC INS)	updateserver.dmz.factory

WSUS server

Table 2-28

Parameter	Value
IP address	10.0.98.40/24
Default gateway / DNS/NTP server	10.0.98.1
Hostname	WSUS
Active Directory integration	Yes
FQDN (via domain controller or SINEC INS)	wsus.dmz.factory

2.6.1 Microsoft Active Directory domain controller

Architecture description

It is common to use a Microsoft Active Directory to centrally manage Microsoft Windows stations.

As a central management instance, the domain controller facilitates functions such as the following:

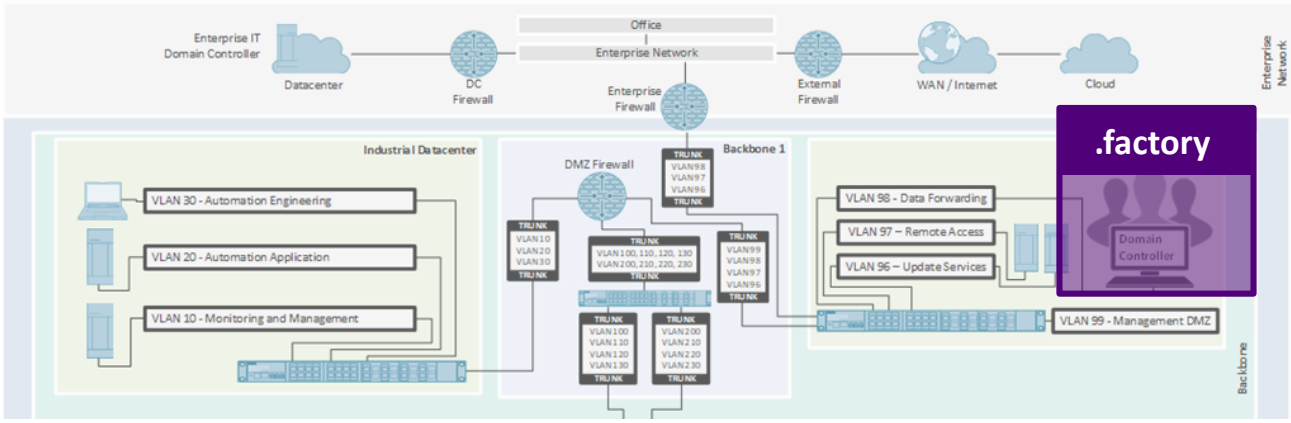
- Central management of user accounts for MS Windows PC stations
- DNS resolution of PC station FQDNs (e.g. TIA project server)
- Provision of a RADIUS server for authentication requests from systems without a MS Windows operating system
- Central management of MS Windows system settings

Because Active Directory user accounts are often imported from higher-level domain controllers of the enterprise network, it is suggested to place the domain controller for the automation stations in the DMZ.

Besides importing users from higher-level domain controller, all manufacturing PCs should be integrated into the domain at this point as well. In this way it is possible to manage all Windows settings centrally, for example.

For the sake of simplicity, the domain ".factory" will be used as a starting point in the following.

Figure 2-29



Configuration of firewall rules in the network components

Besides the aforementioned firewall rules for DHCP, DNS and NTP, the following should be allowed in the DMZ firewall in the local network:

- DNS server access from SINEC INS to the domain controller (default port: UDP/TCP, 53)
- RADIUS access from all network components to the domain controller (default port: UDP, 1812)

The following connection should be allowed in the cell firewalls:

- RADIUS access from the network components in the cell to the domain controller (default port: UDP, 1812)

If the domain controller in the DMZ imports user accounts from a domain controller in the enterprise network, then a corresponding rule set should be stored in the enterprise firewall.

Additional information on the Microsoft Active Directory domain controller:

- Installation and operation of WinCC in a Microsoft domain environment \44\
- User management for SCALANCE devices with RADIUS protocol (Network Policy and Access (NPS) role) \48\ -
- Microsoft Knowledge Base article "How to configure a firewall for Active Directory domains and trusts" \4\

2.6.2 SINEC INS

Architecture description

SINEC INS provides the following basic services in the network:

- **DNS server**
  Not all components support central administration and management with the MS Active Directory. To nevertheless facilitate name-based reachability of, for example, CPUs or HMI Panels, static entries are typically stored in a DNS server.
  The SINEC INS DNS server makes it possible to manage these entries with a web interface that is easy for OT personnel to operate.

- **NTP server**
  SINEC INS serves as a central time server. Time synchronization can be configured centrally in the web interface and is passed down hierarchically to all lower-level NTP servers (DMZ and cell firewalls). See chapter 2.6.6 for more information.

- **Syslog server**

  Syslog is a protocol, common in IT, for distributing log messages. SINEC INS provides a central Syslog server. This server is used by all systems that support Syslog, thus enabling central retention of the log history for network components which are typically linked natively.

- **RADIUS server**
  Network components often use the RADIUS protocol for user authentication. SINEC INS provides a central RADIUS server and, with a UMC client, provides integration into the UMC domain (see chapter 3.6).
  This makes it possible for UMC or Active Directory users to log into the web interfaces of the network components.

Configuration of firewall rules in the network components

To provide the aforementioned services with SINEC INS, the following rule sets should be defined and allowed in the DMZ firewall:

- NTP access from SINEC INS to the enterprise firewall
  (default port: UDP/TCP, 123)
- Syslog from all supported components (e.g. network components, CPUs) to SINEC INS
  (default port: TCP/UDP, 514)
- RADIUS access from all network components to SINEC INS
  (default port: UDP, 1812)

The following rule sets should be defined and allowed in the cell firewalls:

- Syslog from all supported components in the cell to SINEC INS (default port: TCP/UDP, 514)
- RADIUS access from all network components in the cell to SINEC INS
  (default port: UDP, 1812)

Additional information

- SINEC INS function manual - Network management SINEC INS \46\
- Application example: Sending SYSLOG messages with a SIMATIC S7 CPU \45\

2.6.3 Proxy server

Architecture description

The purpose of the proxy server is to control access into and out of the enterprise networks and the internet.

To do this, the proxy server first terminates any session and in its place it establishes its own session to the addressed destination for the system making the query. With this substitution principle, there is no longer a direct connection between the lower-level networks (considered safe) and the higher-level networks (considered potentially unsafe).

The connections are typically made with user context. This means that the system in question must authenticate itself at the proxy server before the connection is established. Proxy servers usually offer numerous options for restricting traffic to the application level. For example, it is possible to restrict access to the internet to such an extent that only appropriate user accounts may access a heavily restricted number of URLs.

In this concept, the proxy server takes central control of internet access. Thus, the proxy server contains unrestricted access into all higher-level networks, including the internet.

Note Alternatively, this service can be implemented with the use of appropriate DMZ and enterprise firewalls with OSI layer-7 functionality.

Configuration of firewall rules in the network components

In order to use the proxy server, the following rule set must be defined and allowed in the enterprise firewall:

- Outgoing access into enterprise networks and the internet without further port restriction

The following rule sets must be defined and allowed in the lower-level DMZ and cell firewalls:

- All connections from systems that need to have access to the enterprise networks or the internet must be allowed to the proxy. These connections are described in the corresponding chapters on each of the components.

2.6.4 DHCP server

Architecture description

The DHCP gives the option of automatically distributing interface parameters to network participants.

Typically, the following parameters are passed to devices making requests:

- IP address
- Subnet mask (DHCP option 1)
- Default gateway (DHCP option 3)
- DNS server (DHCP option 6)
- NTP server (DHCP option 42)

A corresponding DHCP range is defined for each subnet (see chapter 2.2.5 IP address assignment). The addresses of the network components are assigned statically. With respect to remote access, the IP addresses of SINEMA RC and the jump hosts are also statically configured.

Configuration of firewall rules in the network components

Each firewall serves as a DHCP server for the locally connected, internal subnets. If needed and depending on the hardware used, it is possible to bind DHCP leases statically to the client ID (DHCP option 61) or MAC address of the devices.
In such case, the DMZ firewall offers a DHCP server for each subnet in the datacenter, DMZ and aggregation level.

The cell firewalls provide the DHCP servers for the cell networks.

No DHCP server is available below a CPU.

As a rule, by using DNS update mechanisms the DHCP servers also ensure the provision of corresponding records in the DNS server. In this way, FQDN-based addressing of the DHCP clients in the network is then possible.

2.6.5 DNS server

Architecture description

A hierarchical approach is chosen for the resolution of DNS queries. The following DNS servers are always available in the network:

- **Cell firewalls**
  The cell firewalls provide the DNS server service for the devices in the cells; in this role they are configured as DNS proxies. Incoming requests are forwarded via the Transfer&Management-Aggregation subnets and the DMZ firewall.

- **DMZ firewall**
  The DMZ firewall provides the DNS server service for the subnets in the datacenter, DMZ and aggregation level. The DNS queries from the cell firewalls are also received here. In addition, the DMZ firewall is a DNS forwarder and forwards its queries to SINEC INS.

- **SINEC INS**
  SINEC INS provides a simple way to define static DNS entries. Here it is thus possible to facilitate the FQDN-based reachability of the automation components.
  As a DNS forwarder, SINEC INS receives the queries from the DMZ firewall and resolves them directly if possible. If FQDNs need to be addressed which are not stored in the configuration, then forwarding to the domain controller will be the result.

- **Domain controller**
  The DNS server role of the domain controller provides for the resolution of the FQDNs of the PC stations in the domain and receives the DNS queries of the SINEC INS server. In case the requested FQDN is not in the domain, the request will be forwarded to the enterprise firewall via the DNS forwarder feature.

- **Enterprise firewall**
  As a DNS proxy, the enterprise firewall receives queries from the domain controller and forwards them to a DNS server in the enterprise network.

  This DNS server is configured either statically or in the enterprise firewall using DHCP.

- **DNS server in the enterprise network**
  This DNS server is managed by enterprise IT or by the internet service provider (ISP); it resolves queries with destinations outside of the automation networks.

To increase safety in the event of a failure, it is recommended to define the domain controller as the second DNS server in the DMZ firewall and the enterprise firewall as the third. This ensures that, in the event of a failure of SINEC INS or the domain controller, it will still be possible to resolve DNS queries via the enterprise firewall.

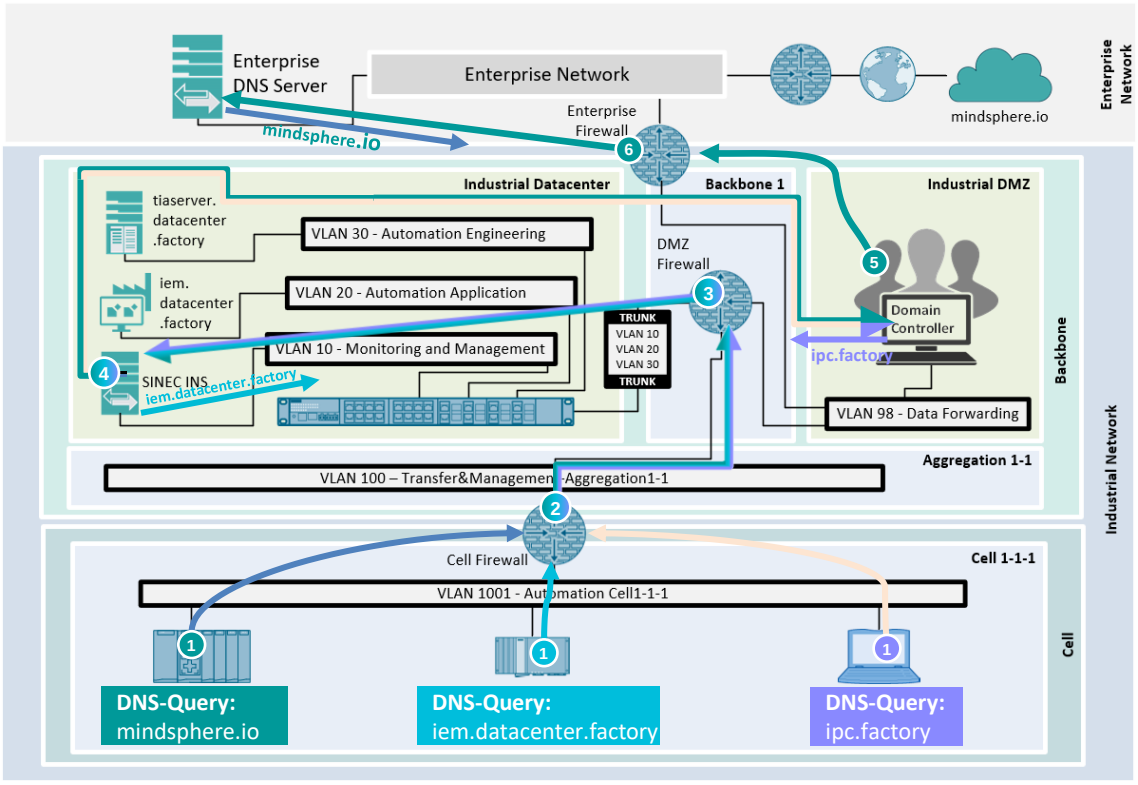
In the same vein, it is recommended to set the enterprise firewall as the second DNS server in SINEC INS.

Furthermore, caching should be enabled in all of the aforementioned DNS servers if possible.

The diagram below shows an example of the hierarchical interplay of the individual DNS servers with the following queries originating from the cell level:

- **mindshere.io**
  The destination of this query is in the internet. Therefore, the enterprise DNS server responds.
- **iem.datacenter.factory**
  The FQDN for this query is statically defined in SINEC INS. Therefore, SINEC INS responds.
- **ipc.factory**
  This is a PC station in the Active Directory. Therefore, the domain controller responds.

Figure 2-30



DNS zones

For easier identification of FQDNs, it can be expedient to divide the systems into individual DNS zones. The following zones are taken as a basis in the passages below:

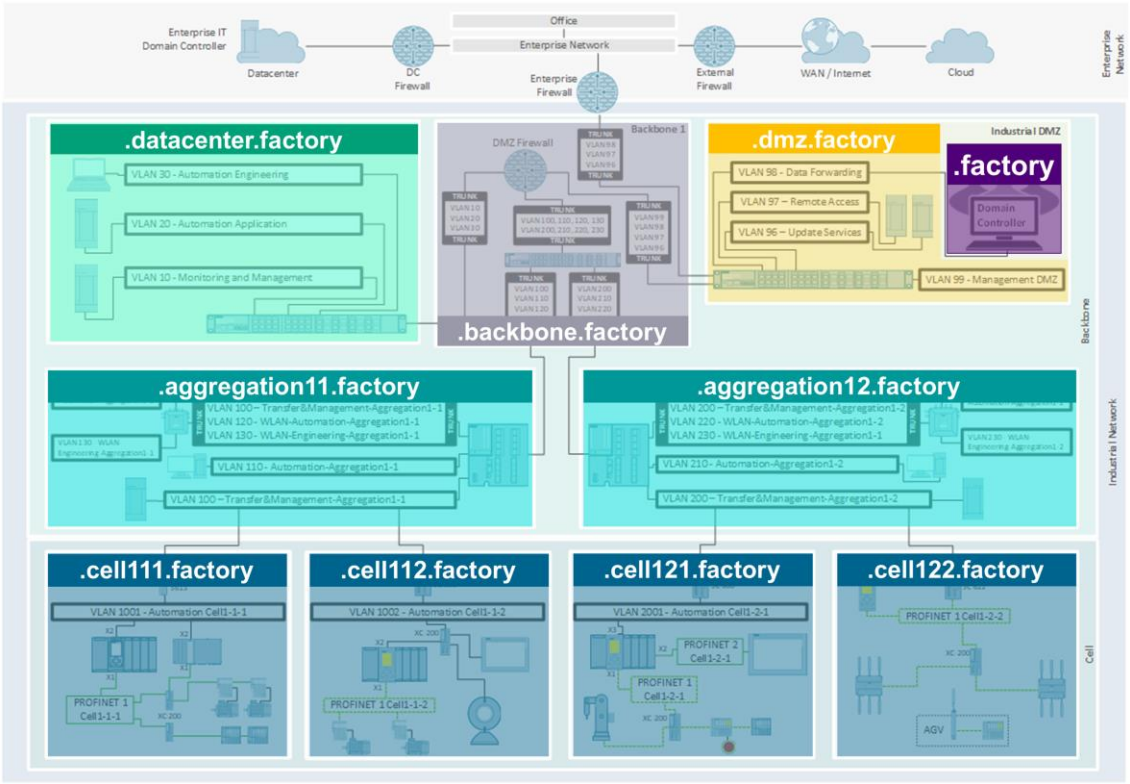
- **.backbone.factory**
  This domain contains all systems in the backbone network between the datacenter subnets, DMZ subnets, aggregation subnets and enterprise subnets.

- **.datacenter.factory**
  All systems physically located in the datacenter are assigned to this subdomain. For example, this pertains to the TIA project server with corresponding engineering VMs. Due to their mobility through all network levels, Field PGs represent a special case. However, due to the engineering context, it is sensible to assign these systems to the datacenter domain as well.
- **.dmz.factory**
  All systems in the DMZ are assigned to this subdomain. For example, these include update servers, proxy servers or jump servers for remote access.
- **.aggregation11.factory, .aggregation12.factory**
  These subdomains contain all systems in the aggregation networks. For example, they are WinCC clients or servers installed in the aggregation level which provide central services for the cells (e.g. SINEC NMS Operation or UMC server).
- **.cell111.factory, .cell112.factory, .cell121.factory, .cell122.factory**
  These subdomains contain all systems in the individual automation cells. Systems typically integrated into the Active Directory are WinCC PC stations, for example.

Note The names for the zones can be extended to include any additional domains as desired.

The diagram below highlights the division of the network segment into different subdomains.

Figure 2-31



Configuration of firewall rules in the network components

Besides the firewall rules for DHCP, DNS and NTP in the local network as described in the chapters above, the following rule sets should be defined and allowed in the DMZ and enterprise firewalls:

DMZ firewall

- Allows DNS traffic from SINEC INS to the domain controller (default port: TCP/UDP, 53)
- Allows DNS traffic from domain controller to the enterprise firewall (default port: TCP/UDP, 53)

Enterprise firewall

- Allows inbound DNS traffic from the domain controller (default port: TCP/UDP, 53)
- Allows inbound DNS traffic from SINEC INS (default port: TCP/UDP, 53)

Cell protection firewalls

- In the cell protection firewalls, the DMZ firewall should allow inbound DNS connections (default port: TCP/UDP, 53) for the application described in chapter 4.3.3.

2.6.6 NTP server

Architecture description

Comprehensive time synchronization is a core component of the network concept.
For example, an accurate clock time and time synchronization are indispensable for plant-wide time stamping of log files and alarms, as well as for the verification of certificates.

The time synchronization is based on an architecture with multiple hierarchically ordered NTP clients and NTP servers.

In this case, SINEC INS, in its role as the central time source in the automation networks, is connected as an NTP client with the NTP server of the enterprise firewall. The enterprise firewall in turn, as NTP client, obtains its system time from the enterprise network.

SINEC INS then provides an NTP server for the DMZ firewall. The DMZ firewall functions as an NTP server for the subnets in the datacenter, DMZ and aggregation.

The cell firewalls obtain their time from the DMZ firewall and then, acting as NTP servers, provide the time for the lower-level devices in the cells.

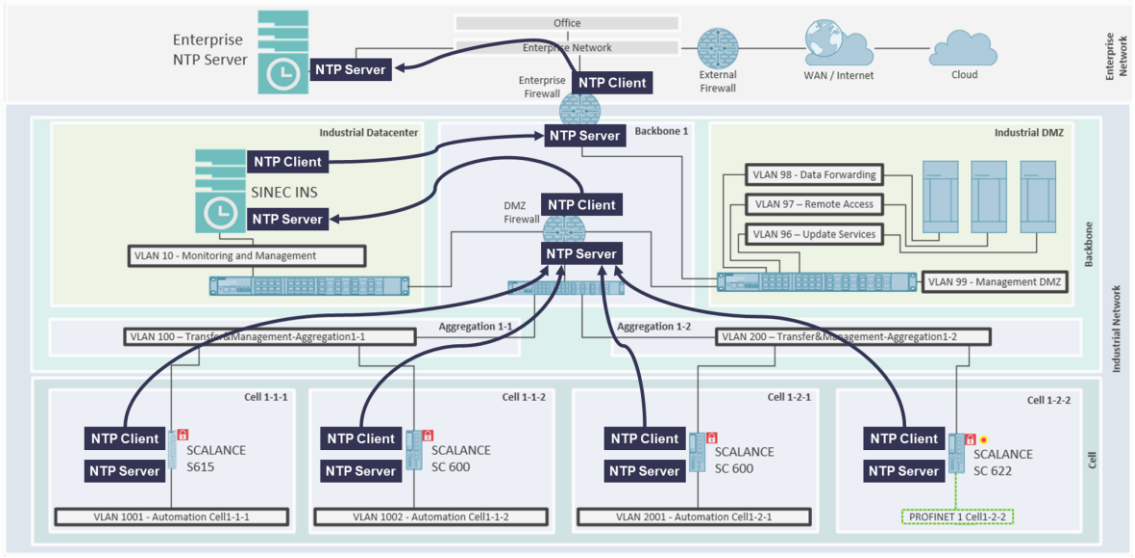
This architecture ensures that no NTP traffic must be routed. This saves firewall configuration effort and ensures that even devices without a configured default gateway can synchronize their system time locally in the network.

Routing system time via SINEC INS also guarantees independence from higher-level enterprise networks. If the time cannot be synchronized via the higher-level NTP server for a longer period of time, then a manual intervention can be performed in the SINEC INS web interface.

All systems that support NTP time synchronization should always obtain their time from the nearest firewall.

The diagram below shows the hierarchical approach to time synchronization.

Figure 2-32



Configuration of firewall rules in the network components

Besides the firewall rules for DHCP, DNS and NTP in the local network as described in the chapters above, the following rule set should be defined and allowed in the DMZ and enterprise firewalls:

- NTP communication between SINEC INS and the enterprise firewall (default port: TCP/UDP, 123)

3 Technical topics

3.1 Visualization

Introduction

Traditional HMIs (human-machine interfaces) are used in automation both to simply and comprehensibly display plant states to plant operators as well as to provide control options. The progressive spread of digital technologies is leading to ever more intelligent, complex and networked automation facilities and machines. In this context, the requirements for human-machine interactions are also changing.

When considering the owner of the plant/factory (end customer), higher-level aspects of the system – for example, operating the plant from multiple control stations, automatic sending of report emails or sending of SMS messages with current information in critical plant situations – plays an increasingly important role.

Against this background, central collection and analysis of data from the field level as well as the integration of cross-device functions with supplemental services (e.g. edge apps, smart watches or tablets) are becoming ever more important. It must be possible to flexibly and securely integrate new maintenance concepts from machine manufacturers (OEMs) into the network.

User management is an especially sensitive aspect from a security perspective. If, for example, the "administrator password" is known, user data on an operator device can be modified. To prevent this, you should always work with a user management system and keep it up to date. Chapter 3.6 describes the options available for this purpose and how they can be implemented.

3.1.1 Components and application

Components in the cell level

If the user needs to be provided with monitoring & control functions close to the machine, it is recommended to use an HMI Panel right on the machine. Besides the traditional communication features (S7 communication/secure S7 communication, etc.), versatile network interfaces make it possible to offer higher-level services such as web access, remote access via Sm@rtServer (VNC) or communication via edge apps.

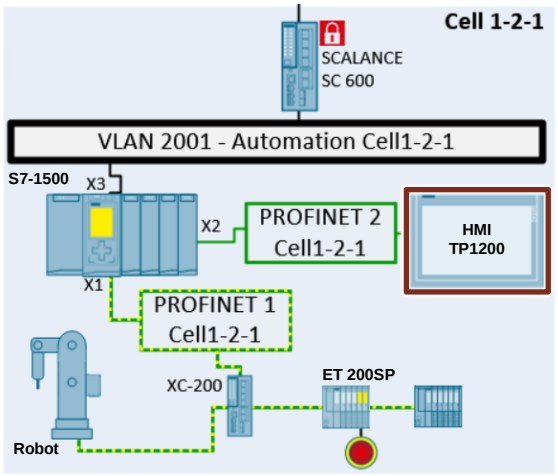
For example, the latest SIMATIC HMI Unified Comfort Panels provide two independent network interfaces that can be used for various communication tasks.

For use of OPC UA, the latest generation of SIMATIC Unified Comfort Panels offer the option of functioning as an OPC UA server. In this case, the panel provides configurable data points that can be queried by OPC UA clients. Traditionally, an OPC UA client is located outside of the cell.

The following layer-2 architectures are typically used on the cell level:

Conventional design

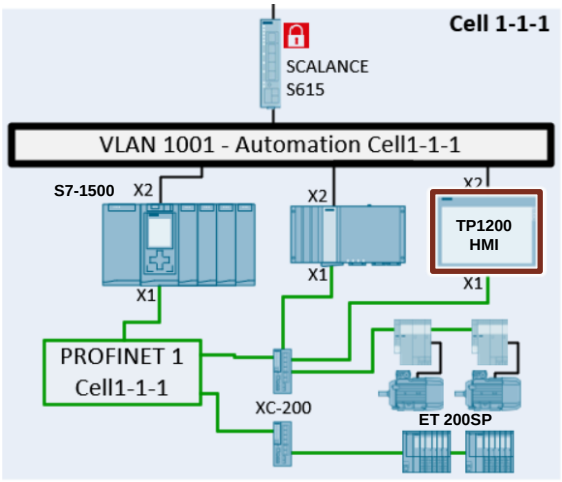
Figure 3-1



To avoid any performance losses at the X1 interface of the S7-1500 CPU (and in case larger amounts of data from various CPUs in the machine cell must be collected and processed), it is recommended to connect the HMI Panel with the X2 interface of the CPU.

Advanced design

Figure 3-2



This type of connection is fundamentally the most versatile solution. Here, the X1 interface of the HMI Panel is used primarily for S7 communication/secure S7 communication with the process. The X2 interface of the HMI Panel is used for communication that crosses cell boundaries (e.g. FTP, web client access, Sm@rt server, OPC UA, etc.).

Components in the aggregation level

If monitoring and control activities extend over a larger spatial area, or if data must be centrally collected, analyzed and displayed, it is recommended to use a WinCC client/server system.

In this system, a WinCC Server handles communication via the process bus with the system controllers and provides the user data and visualization data for the WinCC Clients.

There are two types of WinCC clients:

- Windows-based WinCC clients
- web-based clients (WebNavigator, WebUX, WinCC Unified client)

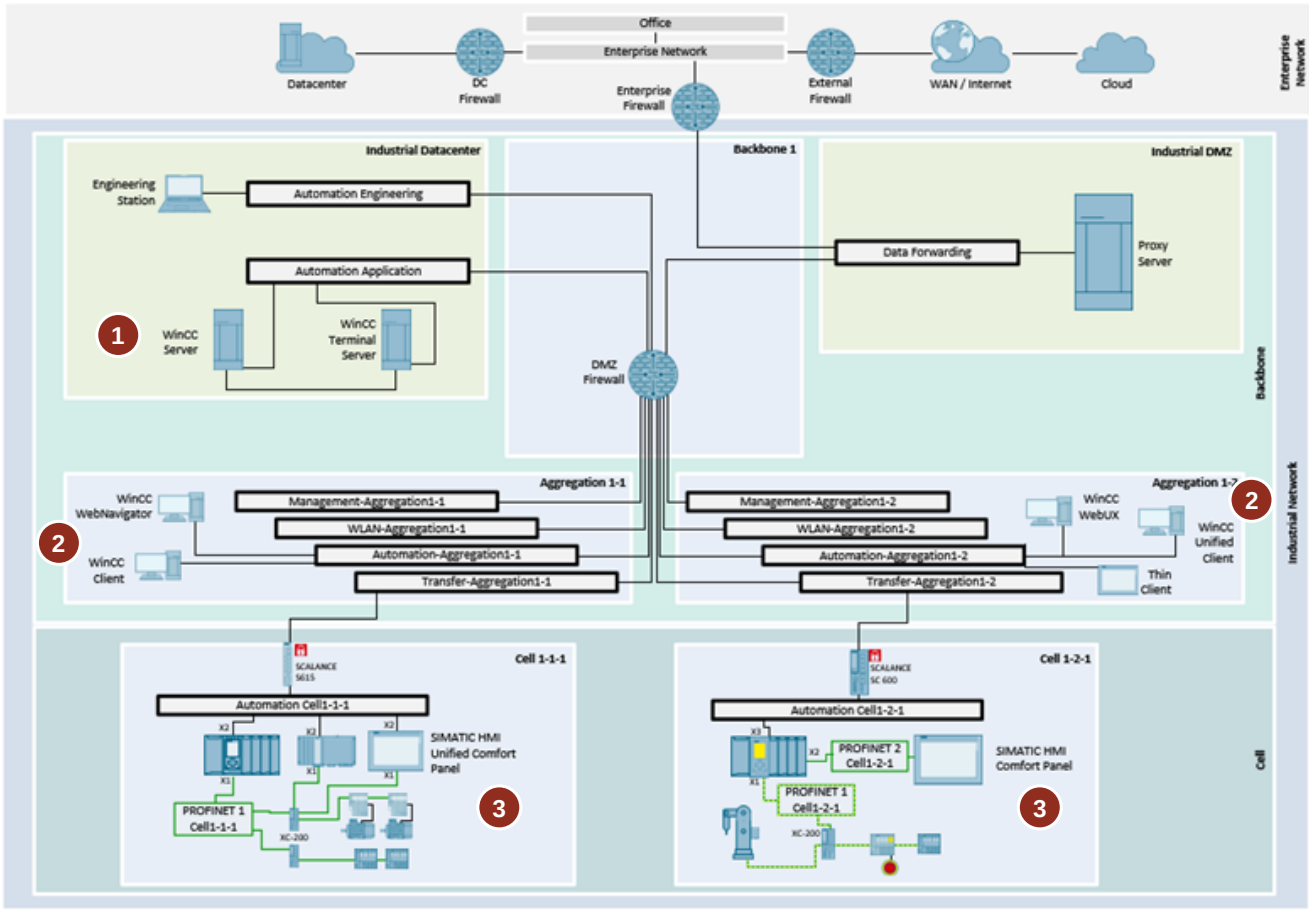
If decentralized HMI solutions will be implemented with client/server architectures, SIMATIC industrial thin clients are a good option for monitoring and control functions. In this case, communication with a dedicated WinCC terminal server runs via Remote Desktop Protocol (RDP).

Placement in the network concept

The following diagram shows the placement of the components in the network concept.

1. Components in the backbone – datacenter
   - WinCC server
   - WinCC terminal server
2. Components in the aggregation level
   - WinCC WebNavigator
   - WinCC client
   - WinCC WebUX
   - WinCC Unified Client
   - thin client
3. Components in the cell level
   - SIMATIC Unified Comfort Panel
   - SIMATIC Comfort Panel

Figure 3-3



3.1.2 Access permission requirements in the network concept

The following communication-related requirements obtain for the communication relationships in the network concept:

Communication from HMI Panels to the CPUs

Because an HMI Panel is located in the cell together with the CPU, no further network requirements must be observed.

Communication from HMI Panel to the engineering stations

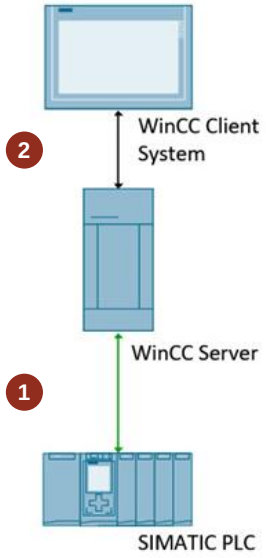
An access permission from the engineering stations from the industrial datacenter is required in order to configure the HMI Panels.

Communication from HMI Panel to higher-level services

For onward communication across cell boundaries (e.g. web client access, Sm@rt server, OPC UA, etc.), the HMI Panel requires access to the industrial datacenter. If the HMI Panel is used as an OPC UA server, for example, it requires a connection to an OPC UA client (TCP/port 4890).

Communication links in a WinCC client/server system

Figure 3-4



1. **WinCC server to the CPUs**

   The WinCC server needs the access permission to the lower-level CPUs. If the CPUs are Siemens automation systems, the S7 protocol is used by default. In this case, TCP port 102 is necessary and must be enabled.
   If third-party systems will be connected, WinCC can be operated as an OPC UA client, for example. The appropriate TCP port for the OPC UA server must be enabled for this. For an S7-1500 controller, for example, this port is TCP port 4840.

2. **WinCC server to each of the WinCC client systems**

   If web-based WinCC client systems will be used, communication between WinCC server and the clients runs over HTTPS as a rule. TCP port 443 is used for this by default.

   Windows-based WinCC clients communicate via the TCP-based terminal bus. The corresponding TCP port (default: TCP port 8910) can be set by the user as desired; accordingly, it must be allowed in the DMZ firewall. If industrial thin clients are used as client systems, TCP port 3389 for the RDP connection must be allowed in the DMZ firewall.

3.1.3 Configuration of the network components

The following configurations in the network components are necessary to run the solution described above. Appendix IX – Firewall rule engineering - chapter 5.9.4 contains a more precise presentation of the necessary communication connections.

- **Configuration of the cell firewalls**
  The following rule sets must be enabled for these communication connections:
  - HTTPS- and SSH-encrypted communication to the HMI Panel (TCP port 443)
  - OPC UA-specific port (TCP port 4840) from the OPC UA client to the HMI Panel
  - If the HMI Panel needs internet access, it is recommended to only allow the communication needed by each app to the proxy server.
  - TCP port for S7 communication from the WinCC server to the CPU (TCP port 102).

  - OPC UA-specific port (TCP port 4840) for OPC UA communication to third-party controllers

- **Configuration of the DMZ firewall**
  The following rule sets must be enabled for these communication connections:
  - NTP access (UDP port 123) and DNS access (UDP port 53) from HMI Panels or WinCC clients and WinCC servers to the cell firewall or SINEC INS (see chapter 2.6.2).
  - OPC UA-specific port (TCP port 4840) from the OPC UA client to the HMI Panel or OPC UA communication from the WinCC server to third-party controllers
  - User-specific TCP port for the communication between WinCC server and WinCC client
  - HTTPS port (TCP port 443) for communication from web-based WinCC clients to the WinCC server
  - *Optional:*
    RDP protocol (TCP port 3389) for communication from the industrial thin client to the terminal server
- **Configuration of the proxy server**
  - If internet access is required (e.g. for cloud connectors), it is recommended to route all internet connections via the proxy server and to create an account for each app with URL whitelisting.
- **Configuration of the enterprise firewall**
  - Thanks to the use of the proxy server, no further configuration is necessary at the enterprise firewall. In case no proxy server is being used, the rules for the connections to the internet must be configured accordingly.

3.1.4 Configuration of the HMI stations

The following parameters are suggested for setting up the HMI/SCADA stations:

HMI Panel configuration

Parameter	Value
IP addresses	10.1.10.202/24
Default gateway / DNS/NTP server	10.1.10.1
Computer name	HMIPANELXXX
Active Directory integration	Recommended to central user management, domain: *.factory*

Configuration of the WinCC server

Parameter	Value
IP address	10.0.20.10/24
Default gateway / DNS/NTP server	10.0.20.1
Computer name	WINCCSERVER
Active Directory integration	Recommended to central user management, domain: *.factory*
FQDN	*winccserver.datacenter.factory* (statically defined in SINEC INS or domain controller)

Configuration of the WinCC clients

Parameter	Value
IP address	10.0.110.100/24 to 10.0.110.200/24
Default gateway / DNS/NTP server	10.0.110.1
Computer name	WINCCCLIENTxxx
Active Directory integration	Recommended to central user management, domain: *.factory*
FQDN	*winccclientxxx.aggregation11.factory* (statically defined in SINEC INS or domain controller)

Note If IP addresses are assigned with DHCP, then this can only occur in connection with a static lease. The reasoning is that WinCC and WinCC runtime V17 and earlier do not support addressing using FQDN.

3.2 Network management

Efficiently monitor networks with SINEC NMS

SINEC NMS is a new generation of network management system (NMS) for Digital Enterprise geared for the ever more complex network structures of an increasingly digital world. With this system, networks containing tens of thousands of nodes can be monitored, managed and configured centrally and at any hour of the day. This makes SINEC NMS the first choice for complex network structures and a pioneer for the digital transformation in the industry – in all sectors and independent of the network size. Thanks to its scalability, SINEC NMS will grow with the network as it continues to expand and becomes more complex.

Changes in industrial networks must be detected early and faults prevented in order to ensure productivity of industrial facilities and minimize downtimes. The solution is SINEC NMS. This system monitors the entire network round the clock and displays a live view of the network devices' diagnostic statuses. It is also possible to display and analyze statistics for any period in time. One advantage of this is early detection of undesired errors thanks to the color-coded diagnostic display. Additionally, email notifications deliver timely information about changes in the network.

What events can be diagnosed?

Using SNMP, the S7 protocols and the protocols in the PROFINET standard, it is possible to detect various events in the network nodes being monitored. Each event provides valuable information for the first diagnosis.

- **SNMP**

  The Simple Network Management Protocol (SNMP) provides information from all SNMP-capable infrastructure components and products.

- **PROFINET**

  PROFINET-capable devices use their own protocol ("read data record" – see chapter 3.7.1) to provide standardized and channel-precise diagnostic information such as short circuits or overvoltage.

- **S7 protocol**

  The proprietary Siemens SIMATIC S7 protocol provides information such as the cycle time or the operating mode of S7-300/400/ET200 CPUs. The status (maintenance requested, erroneous, missing) can also be read from the assigned I/O devices. Moreover, all events and alarm messages from "Report system errors" can be received and displayed by the network management station.

  Note Not possible for S7-1200/1500.

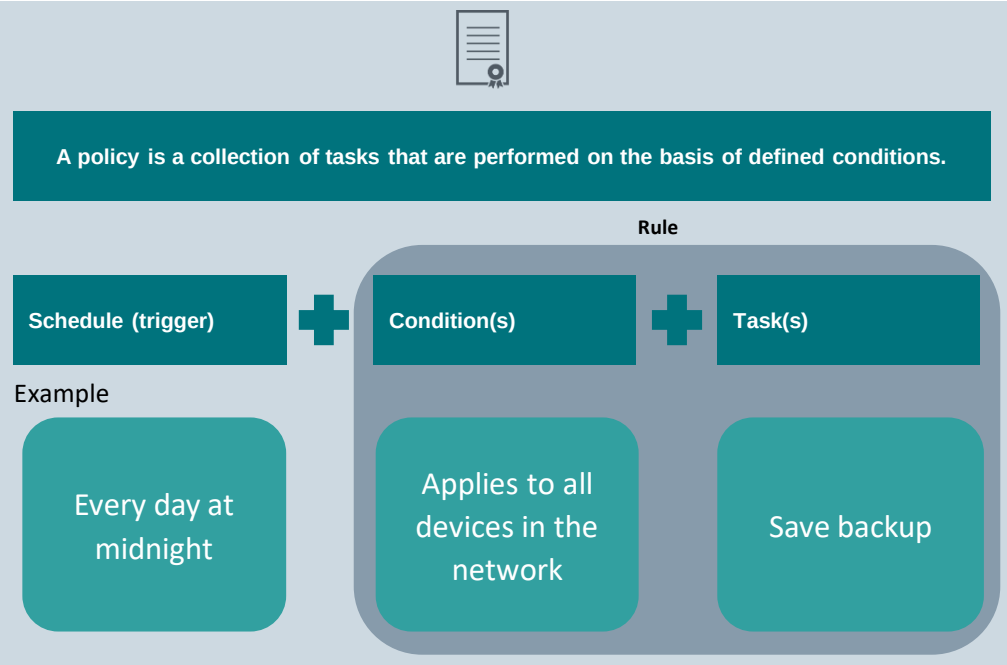
Figure 3-5

SNMP	PROFINET	SIMATIC
Standardized network diagnostics Remote control and configuration Notification in case of faults (Traps)	Open PNO Industrial Ethernet standard Cross-manufacturer data analysis Standardized diagnostics	Diagnostics of CPUs and their assigned devices via S7 protocol Seamless connection to CPU reporting system
· Device recognition · Topology · I&M data · VLAN · Redundancy (HRP, MRP, Standby, Passive listening, STP, RSTP, …) · Uptime · C-PLUG · Power supply · TRAPs · Interfaces · Statistical data (Util., CRC, dropped) · Diagnostic information · Custom OIDs	· Device recognition · Topology · I&M data · Redundancy (MRP) · Controller device assignments · Interfaces · Diagnostic information · Channel diagnostics · Default diagnostics · Statistical data (Util., CRC, discarded frames) · POF diagnostics	· Operating status of PLC · Cycle times + limits · Assigned PROFINET devices · Status of all assigned PROFINET devices · Receipt of all diagnostic alarms (system error reporting) · Readout of message texts stored in CPU · Monitoring of redundant PCS 7 architectures (R1, S2)

Efficiently manage networks with SINEC NMS

A policy can be used to plan and perform tasks for configuring and managing SCALANCE devices. The devices and tasks of a policy can be freely combined within the scope of the existing permissions. The range of devices that can be configured is determined by the conditions. Policies can be rolled out either on a schedule or manually. Before executing a policy, SINEC NMS uses the available device functions to determine which tasks can be executed on which devices. Using policy simulations, this information can be determined without having to execute the policy.

Figure 3-6



You can find policy execution examples in chapters 3.4 and 4.1 on firmware management and backup.

Advantages of SINEC NMS

- SINEC NMS detects all devices in the network. This provides a constantly updated overview of all installed components including all essential properties in the network.
- Plant topologies are automatically read out, displayed and monitored for changes.
- Diagnostic data is collected from all network participants and stored centrally. Diagnostic data are analyzed via data records for the SNMP, S7 communication and PROFINET protocols. The overall state of the network is displayed via a central dashboard.
- Statistics can be displayed and evaluated over any period of time. Historical events can also be easily evaluated in this manner.
- Configurable test patterns enable essential network properties to be repeatedly checked and documented.
- A variety of interfaces (e.g. HTTPS, OPC UA) make it possible to display network and diagnostic data and forward this data to higher-level systems.
- Policy-based configuration of various network functions
- Batch operation for firmware update of single or multiple SCALANCE components
- Central management of network device roles and rights in the entire system. (for more information, see chapter 3.6).
- Central firewall management and NAT management for SCALANCE components

Note

SINEC NMS provides the network component monitoring function for Siemens and 3rd-party devices. However, the network component management function is available exclusively for network components from the SCALANCE and Ruggedcom series.

Further information with examples, demonstration material and more can be found online at \69\.

The software can be downloaded from Siemens Industry Online Support \70\.

The software license can be obtained from the Siemens Industry Mall.

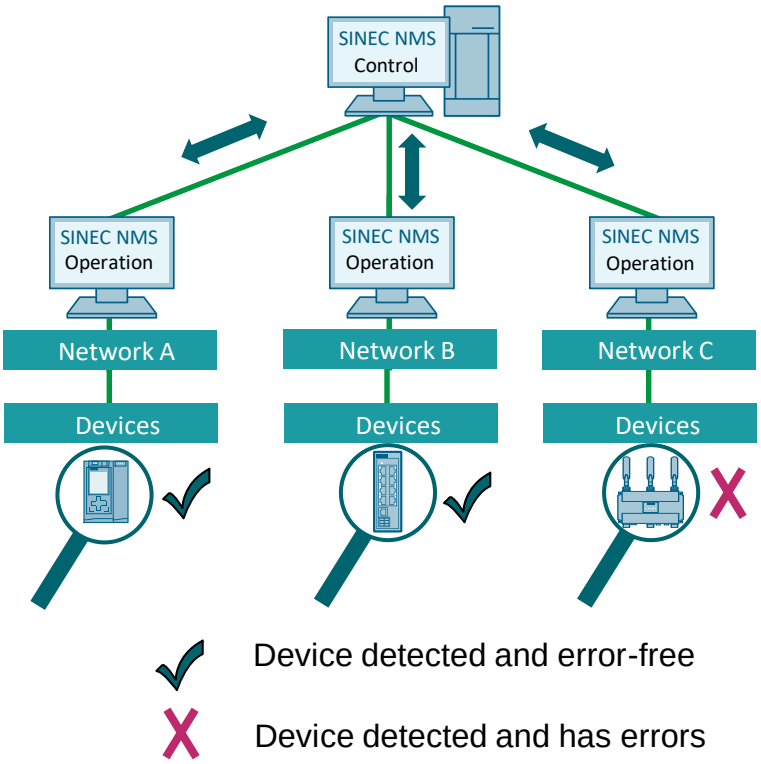
3.2.1 Components and application

Thanks to the distributed approach of SINEC NMS, the network management system can be dynamically adapted to the network requirements of each customer facility. The SINEC NMS network management system consists of one Control and one or more Operations.

Table 3-1

Component	Description
SINEC NMS Control	The Control is the central instance in SINEC NMS; it displays the overall condition of the network. It very quickly gives the user an overview of the overall network status. Furthermore, the distributed SINEC NMS Operations are centrally managed in the Control. The Control is responsible for firmware management, network management and user management.
SINEC NMS Operation	The tasks of the Operations are to detect the network devices and read the respective diagnostic information from the devices. In addition, the SINEC NMS Operations distributed throughout the network implement the configuration parameters (policies) from the Control to the devices.

Figure 3-7



Placement in the network concept

There are essentially two ways of placing the SINEC NMS components in the network.

Centralized approach

Control and Operation are located in the industrial datacenter.

Figure 3-8

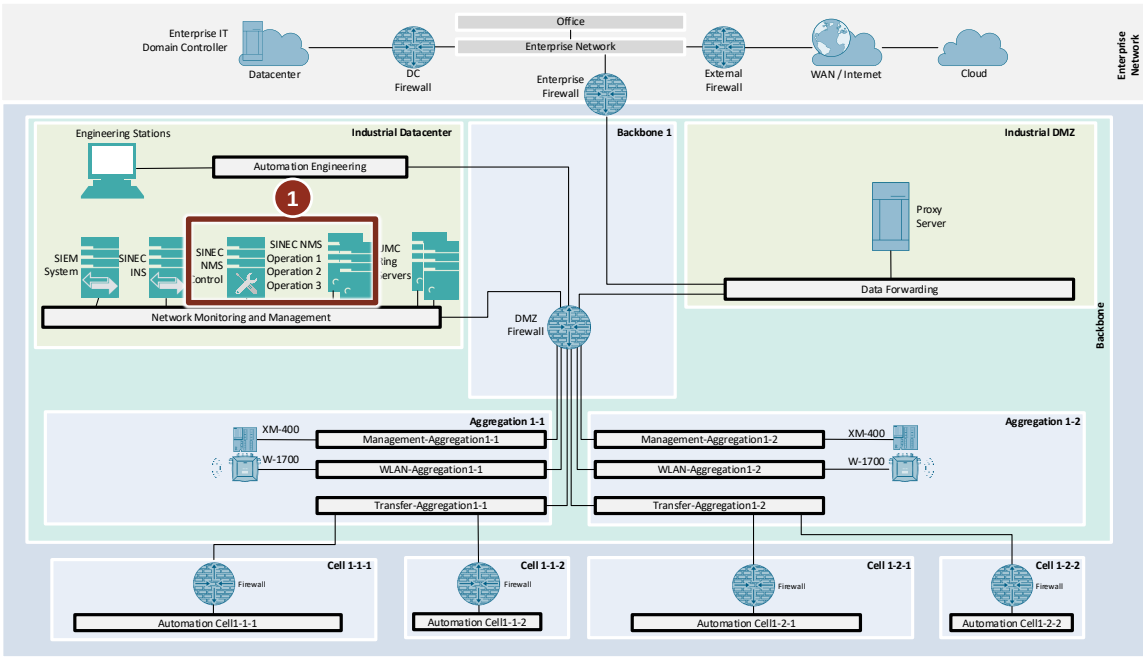


Table 3-2

Advantages	Disadvantages
Easy scalability of additional Operations with virtualization.	Large volumes of diagnostic data (arising from SNMP, S7 communication and PROFINET) are transmitted to the central Operations and must therefore be routed through the entire network.

Decentralized approach

1. The SINEC NMS Control is located in the industrial datacenter.
2. The Operations are located in the aggregation level above the automation cell.

Figure 3-9

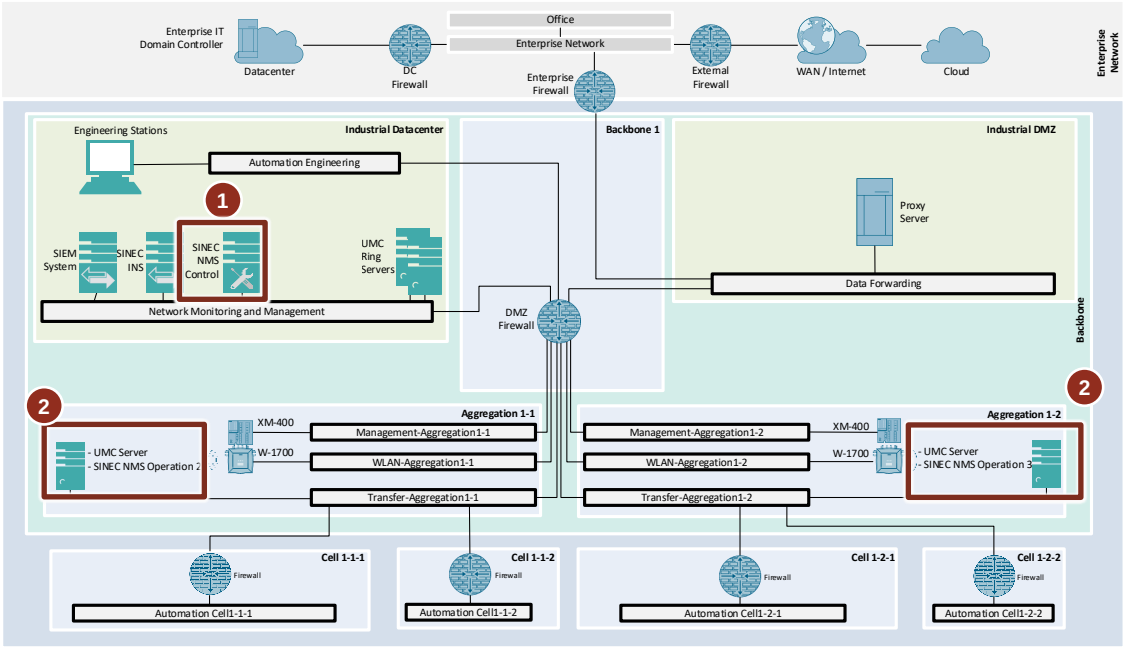


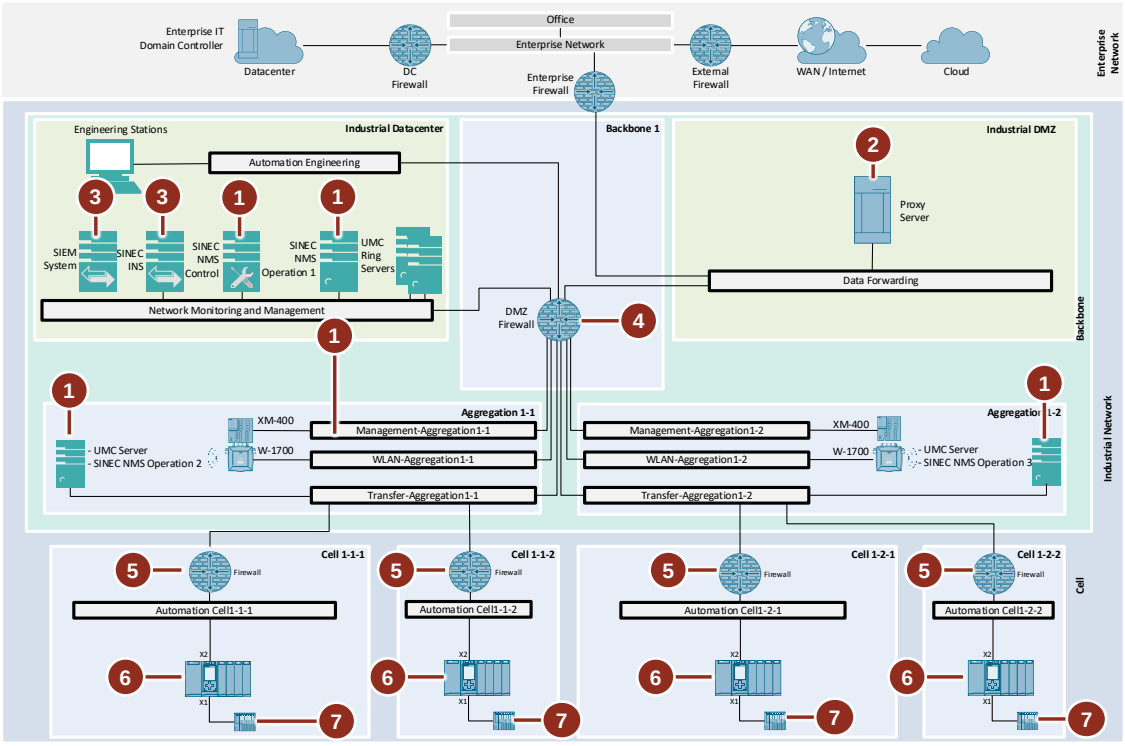
Table 3-3

Advantages	Disadvantages
Diagnostic data from SNMP, S7 communication and PROFINET are analyzed locally in the Operations. The Control receives the compressed data volume.	Additional IPC hardware required for Operations

3.2.2 Configuration and implementation in the network concept

SINEC NMS Control and Operation are installed in the industrial datacenter and on various IPCs in the aggregation level in a decentralized fashion.

Figure 3-10



The following configurations are required to install and run SINEC NMS:

1. IP address assignment
   The Control and Operations must be accessible via static IP addresses. Do not use IP address configuration via a DHCP server. This applies to single node and multiple node installations.

2. Proxy server
   If you need current firmware files for updating your SCALANCE devices, it is recommended to establish your internet connection via a proxy server.

3. SINEC INS services DNS, NTP and Syslog
   Define a static DNS record in SINEC INS (for name-based accessibility of Control and Operation web servers)

   In this example, Control and Operation are installed on Windows operating systems and pull their clock time from SINEC INS.

   Syslog messages are forwarded from the SINEC NMS client to a Syslog server (SINEC INS or SIEM system). The realtime analysis of the network components is done in SIEM (Security Information and Event Management).

4. Configuration of the DMZ firewall
   The following firewall rules must be put in place for network monitoring between SINEC NMS Control and Operation.

Table 3-4

From	To	Port	Protocol	Service
Control	Operation	8443	TCP	HTTPS (Web server)
Control	Operation	5671	TCP	Data exchange (RabbitMQ)
Control	Operation	49131	TCP	Firmware update file synchronization (SFTP)
Operation	Control	443	TCP	HTTPS (Web server)
Operation	Control	5671	TCP	Data exchange (RabbitMQ)
Operation	Control	49113	TCP	Heartbeat (reachability test)
Operation	Control	49114	TCP	Version check

5. Configuration of the cell firewall
   The following firewall rules must be put in place for network monitoring between the Operation and the end device in the cell:

Table 3-5

From	To	Port	Protocol	Service
Operation	Device	161	UDP	SNMP polling
Operation	Device	102	TCP	SIMATIC diagnostics
Operation	Device	ICMP echo req.	IP service	Network scan
Operation	Device	22	TCP	SSH connection
Operation	Device	34,964 & 49.152-65.535	UDP	PROFINET diagnostics
Operation	Device	443	TCP	Backup/restore config
Device	Operation	162	UDP	SNMP Traps
Device	Operation	69	UDP	Firmware update (TFTP)

6. IP forwarding
   IP forwarding is used to forward IP packets between 2 connected subnets via the CPU.

7. Monitoring of network devices
   Using SNMP, S7 communication and the protocols in the PROFINET standard, it is possible to detect various events in the monitored network nodes and display them in SINEC NMS.

3.3 Engineering and configuration with TIA Portal

3.3.1 Components and application

TIA Portal is the central engineering tool for SIMATIC automation components, such as:

- CPUs
- HMI Panels
- SCADA stations
- I/O devices
- Drives

Engineering components

The TIA Portal engineering environment contains the following essential components:

Table 3-6

Component	Description
Project server	The TIA project server acts as the central management server for the TIA Portal projects. All projects are stored here as a rule. Each engineering station has the ability to check out these projects from the server, edit them and check in changes. The TIA project server then saves the corresponding change history with the option for a rollback. Microsoft Windows mechanisms are used to authenticate access to this server. A coupling to the Active Directory of the domain controller is implicitly possible because of this fact. Additional information: \30\ - SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16 - Working with the TIA project server
License server	The software component "Automation License Manager" is responsible for license management in the TIA Portal context. By installing this component on the project server, it is possible to add central license management for the engineering systems to the project server. This enables you to install floating licenses at a central point which can then be used by all the other engineering systems installed in the network. Alternatively, licenses may also be installed locally on the individual stations. This practice is common especially with systems that are deeply integrated into the automation solution (such as HMI stations). A local license installation can also make sense for Field PGs or engineering VMs that continuously remain in use. Additional information: \31\ - Manual - Automation License Manager
Engineering VM	TIA Portal can also be installed on virtual machines when using virtualization servers. These VMs provide significant advantages from an administration standpoint. These virtual machines, hosted in the datacenter for engineering purposes, are referred to hereinafter as engineering VMs.

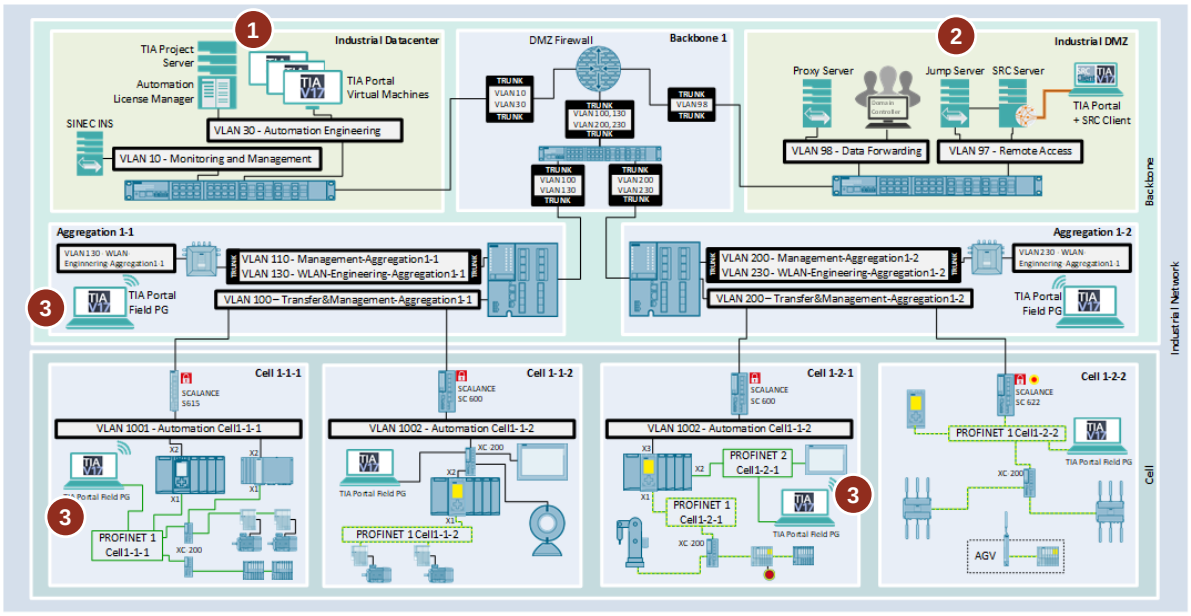
Component	Description
Field PG	A TIA Portal installation on laptops or SIMATIC Field PGs is common for mobile engineering with TIA Portal in the production hall or directly at the machine. These mobile engineering stations are referred to in the following as Field PGs.

Placement in the network concept

The following diagram shows the placement of the components in the network concept.

1. The project/license server and the engineering VMs are placed in the Automation-Engineering subnet of the datacenter.
2. The jump server for the remote access solution described in chapter 4.2 is located in the Remote-Access subnet of the DMZ.
3. The Field PGs can be used on the fly in the WLAN-Engineering-Aggregation subnets, the Automation Cell subnets or directly in the PROFINET subnets.

Figure 3-11



Access paths

Various access paths to the modules are possible for configuration purposes using the components described above. Each of the access paths is explained below.

- **Access from the datacenter**
  The recommended path is access from an engineering VM in the datacenter to the automation components in the cell. The advantage in this case is that the engineering stations can be managed centrally in the virtualization server. As a rule, the VMs are integrated into the Automation-Engineering subnet.
  In such case, the automation components are accessed via routed networks. This means that OSI layer-2 protocols, for example for topology scans, do not work here.

- **Access via SINEMA Remote Connect**
  Access with SINEMA Remote Connect can be structured in two ways:

  a. A user accesses the jump server in the DMZ via a SINEMA RC client. The jump server then uses a remote desktop connection to connect itself to one of the engineering VMs dedicated for remote service.
  Full access to the infrastructure is then possible through this VM. This includes the project/license server, for example.

  b. A user accesses the cell directly via the SINEMA RC client with the VPN tunnel of the SINEMA RC server.
  Direct access is possible with appropriate configuration of the SINEMA RC server and cell firewalls. An access method of this kind is common for a machine manufacturer, for example.
  If this is the case, however, access to the infrastructure in the datacenter should be prevented for security reasons.
  The machine manufacturer thus requires TIA Portal with the corresponding project on his engineering station and does not access the infrastructure hosted in the datacenter.

  Remote access with SINEMA RC is likewise structured via routed networks.
  For more details, see chapter 4.2.

Note

Activation of the VPN tunnel can be secured with a key-operated switch as an additional security measure. This would restrict remote access to only the time actually needed.

- **Access via WLAN on the aggregation level**
  The WLAN engineering VLAN on the aggregation level is available as a convenient access path.
  Owing to the spatial extent across the whole production line, easy engineering and diagnostic access is possible on site.
  Access occurs on OSI layer 3 due to the placement in the aggregation level above.

- **Direct access to the cell level**
  Especially during the commissioning phase it is common to connect the programming device to the cell network directly. This way the cells can be commissioned independently of how the higher-level network is implemented.
  Connecting the programming device directly to the cell facilitates communication between the engineering tools directly on OSI layer 2. This allows for topology scans, device initialization and component searches in the local network.
  In subsequent plant operation, a service port for on-site diagnosis can be set up at a local switch.
  Access can be structured wither via the corresponding automation cell network (as shown in Figure 3-11 for cells 1-1-2 and 1-2-2) or directly on the PROFINET network (as shown for cells 1-1-1 and 1-2-1).
  Bear in mind the following for a connection on a PROFINET network that is isolated with the CPU:

  a. There is usually no DHCP server available in these network segments. Therefore, interface configuration of the Field PGs must be done manually or with TIA Portal mechanisms.

b. Access to the project server routed via the CPU should be avoided and blocked in the cell firewall. TIA Portal projects can reach hundreds of megabytes in size. This data transfer places unnecessary load on the CPU due to IP forwarding. If communication with the project server and OSI layer-2 access to PROFINET is necessary, it is recommended to connect the field PG to the PROFINET network using an Ethernet interface and at the same time use the WLAN engineering VLAN for access to the datacenter.

- **Remote desktop access to engineering VMs**
  Remote desktop access (RDP) from the WLAN-Engineering-Aggregation networks or the automation cell networks is a plausible option for engineering from the datacenter.
  In this case, an engineering VM is used for the project engineering. The laptop or field PG used in this case does not require any special software.

3.3.2 Configuration of the PC stations

- **Configuration of the project/license server**
  Because this station is an infrastructure service, a static configuration of the Ethernet interface is used.

  Internet access, configured via the proxy server, is required to download web licenses through the Automation License Manager.

  Central user management requires that these PC stations be integrated into the Active Directory of the domain controller. Active Directory groups can then be given appropriate permissions in the project server configuration.

  The following parameters are recommended when setting up the PC station:

Table 3-7

Parameter	Value
IP address	10.0.30.10/24
Default gateway / DNS/NTP server	10.0.30.1
Computer name	TIASERVER
Active Directory integration	Recommended to central (AD-based) user management, domain: .factory
FQDN	tiaserver.datacenter.factory (statically defined in SINEC INS or domain controller)
Other	Configuration of the proxy server (DMZ) for internet access

- **Configuration of the engineering VMs**
  As a rule, the engineering VMs receive their interface configuration via DHCP.
  For remote access via RDP from the jump server or lower-level networks, it is nevertheless recommended to give a certain number of VMs a static interface configuration.
  Remote desktop access should also be enabled on these static engineering VMs.
  Integration into the Active Directory is recommended here as well. This enables administration tasks, such as patch management, in a more coordinated manner.

Additionally, these VMs can be addressed with the corresponding FQDN or computer name in case of RDP access.

The following configuration is recommended for all VMs that need to be reachable outside of the virtualization server:

Table 3-8

Parameter	Value
IP address	10.0.30.100/24 to 10.0.30.200/24
Default gateway / DNS/NTP server	10.0.30.1
Computer name	TIAVMxxx
Active Directory integration	Recommended, domain: .factory
FQDN	tiavmxxx.datacenter.factory (statically defined in SINEC INS or domain controller)
Other	Enable RDP access for domain users

The following configuration is sufficient for VMs that only need to be reachable within the virtualization server:

Table 3-9

Parameter	Value
IP address	DHCP
Default gateway / DNS/NTP server	DHCP
Computer name	TIAVMxxx
Active Directory integration	Recommended, domain: .factory

- **Configuration of the Field PGs**
  The Field PGs receive their interface configuration via DHCP. Integration into the Active Directory is recommended, but optional in this case.

  The following configuration parameters are suggested for Field PGs:

  Table 3-10

Parameter	Value
IP address	DHCP
Default gateway / DNS/NTP server	DHCP
Computer name	TIAPGxx
Active Directory integration	Recommended, domain: .factory

3.3.3 Access permission requirements in the network concept

With respect to engineering communication with TIA Portal, the following requirements for the network concept obtain:

- **Communication between PC stations and domain controller**
  All PC stations must be able to communicate with the domain controller in the Data-Forwarding subnet of the DMZ.

For the Field PGs, this access is typically sufficient when outbound from the WLAN-Engineering-Aggregation subnets. Active Directory access from the automation cell networks can therefore be omitted.

- **Communication from the project/license server to the internet**
  To download licenses from the internet, the project/license server requires HTTPS access (TCP port 443) to the following URL: "https://www.automation.siemens.com/swdl"

- **Communication between engineering VM and project/license server**
  The engineering VMs need access to the projects stored on the TIA project server as well as HTTPS access (TCP, default port 8735) to the project/license server.
  Additionally, to use floating licenses, the engineering VMs need access to the Automation License Manager (TCP, default port 4410).
  If you also need the option of distributing fixed licenses to the engineering VMs from the license server, then this outbound connection (TCP, default port 4410) is also necessary from the project/license server for the engineering VMs.

- **Communication between Field PG and project/license server**
  The Field PGs require access from the WLAN-Engineering-Aggregation networks to the project/license server (TCP, default ports 8735 and 4410).
  PROFINET networks are an exception in this case. To prevent excessive load on the CPUs from IP forwarding, access to the project/license server is blocked here in the cell firewall. If the Field PGs connect directly to PROFINET, licenses and projects can be obtained via a parallel WLAN connection from one of the WLAN-Engineering-Aggregation subnets.

- **Communication between jump server and engineering VMs**
  The jump server requires RDP access (TCP/UDP, default port: 3389) to the engineering VMs dedicated for remote access.

- **Communication between RDP clients (laptops without engineering software) and engineering VMs**
  To access engineering VMs from the production environment, RDP access (TCP/UDP, default port: 3389) from the WLAN-Engineering-Aggregation and cell automation subnets is required.

3.3.4 Configuration of the network components

The following configurations in the corresponding network components are necessary in order to operate the engineering solution with TIA Portal described above. Appendix V – Static IP addresses – contains an exact listing of the necessary communication connections.

- **Configuration of the proxy server**
  Access to the URL "https://www.automation.siemens.com/swdl/" is required to download licenses from the internet. A dedicated system account should be created for this access at the proxy server (see Appendix X – Proxy configuration).

- **Microsoft Active Directory**
  It is always recommended, and sometimes even necessary to add the Windows machines to the Active Directory.

- **Configuration of the DMZ firewall**
  The following rule sets are needed in the DMZ firewall:
  - Access from the project/license server to the proxy server
    TCP (default port: 8735)
  - Access from the engineering VMs in the Automation-Engineering subnet and Field PGs in the WLAN-Engineering-Aggregation subnets to the domain controller (see \4\)
  - RDP access from the jump server to dedicated engineering VMs
    (TCP/UDP, default port: 3389), see chapter 4.2 - Remote access
  - Access from the WLAN-Engineering-Aggregation networks to the project/license server
    (TCP, default port: 8735, 4410)
  - RDP access from the WLAN-Engineering-Aggregation networks to dedicated engineering VMs (TCP/UDP, default port: 3389)
  - Access from the automation cell networks to the project/license server
    (TCP, default port: 8735, 4410)
  - License management access from the project/license server to all Field PGs and engineering VMs (TCP, default Port 4410)
  - RDP access from the automation cell networks to dedicated engineering VMs
    (TCP/UDP, default port: 3389)

- **Configuration of the cell firewalls**

  The following rule sets are needed in the cell firewalls:
  - Access from the automation cell networks to the project/license server
    (TCP, default ports: 8735, 4410)
  - License management access from the project/license server to the Field PGs in the cell
    (TCP, default port: 4410)
  - RDP access from the automation cell networks to dedicated engineering VMs
    (TCP/UDP, default port: 3389)

- **Configuration of the enterprise firewall**
  When using the proxy server for internet access, the enterprise firewall does not need to be configured.

Note

It is recommended to prevent access to the datacenter from the VPN interface of the cell firewalls.

The jump server in the DMZ should be used for remote access to the datacenter.

Further details can be found in chapter 4.2 Remote access.

For each system, the chapters below contain a description of the access mechanisms and a recommendation for the configuration of the network components. An example firewall configuration is described in Appendix IX – Firewall rule engineering.

3.3.5 Configuration of access to SIMATIC S7-1200/1500 CPUs

Overview of necessary communication services

Engineering

The S7 protocol (ISO-on-TCP protocol to TCP port 102) is used as a rule for engineering the SIMATIC S7 CPUs.
This protocol is used for:

- Uploading/downloading the configuration
- Diagnostics via the TIA Portal "Go Online" function
- Firmware updates

The web server (TCP port 80 / 443) is a common tool for performing diagnostics without engineering software.

The following access methods are also available if needed:

Access to OPC UA server

The OPC UA server (TCP, default port: 4840) contains hardware information. This way it is possible to read serial numbers, hardware versions and firmware versions as part of an asset management exercise, for example.

Access to SNMP V1 server

An SNMP V1 server (port: TCP 161) is available on the modules for diagnosing the IP and Ethernet stack. This SNMP server is typically used by asset management systems such as SINEC NMS (see chapter 3.2 Network management).

More information on the communication services employed can be found in chapter 3.2 of the following manual:

SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication \40\

Recommended firewall configurations

It is recommended to enable the protocols ISO-on-TCP, HTTPS and OPC UA for engineering access to the SIMATIC CPUs between engineering networks and CPU. All of these protocols provide security in the form of authentication and encryption.

Access paths that entail increased risk due to lack of authentication and encryption should not be allowed as a rule for all engineering networks. This applies here to the SNMP and HTTP server. In this case, authentication can be accomplished via the SINEMA Remote Connect server on the network level. Therefore it can be expedient to only allow such access through the VPN tunnel with the appropriate authentication and on-site activation on the machine (e.g. with a key-operated switch) (see chapter 4.2 Remote access). The engineering systems then connect themselves with the SINEMA Remote Connect server in the DMZ for this access.

The network component configuration recommendations with regard to engineering the SIMATIC CPUs are listed below.

- **Configuration in the DMZ firewall**
  - Allow ISO-on-TCP, HTTPS and OPC UA access from the Automation-Engineering subnet to the IP addresses of the CPUs in the Automation-Cell subnets (TCP ports 102, 443, 4840)
  - Allow ISO-on-TCP, HTTPS and OPC UA access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the CPUs in the Automation-Cell subnets (TCP ports 102, 443, 4840)

- **Configuration in the cell firewalls**
  - Allow ISO-on-TCP, HTTPS and OPC UA access from the Automation-Engineering subnet to the IP addresses of the CPUs in the Automation-Cell subnets (TCP ports 102, 443, 4840)
  - Allow ISO-on-TCP, HTTPS and OPC UA access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the CPUs in the Automation-Cell subnets (TCP ports 102, 443, 4840)
  - Allow ISO-on-TCP, HTTPS, SNMP V1 and OPC UA access from the SINEMA Remote Connect VPN to the IP addresses of the CPUs in the Automation-Cell subnets (TCP ports 102, 443, 161, 4840)

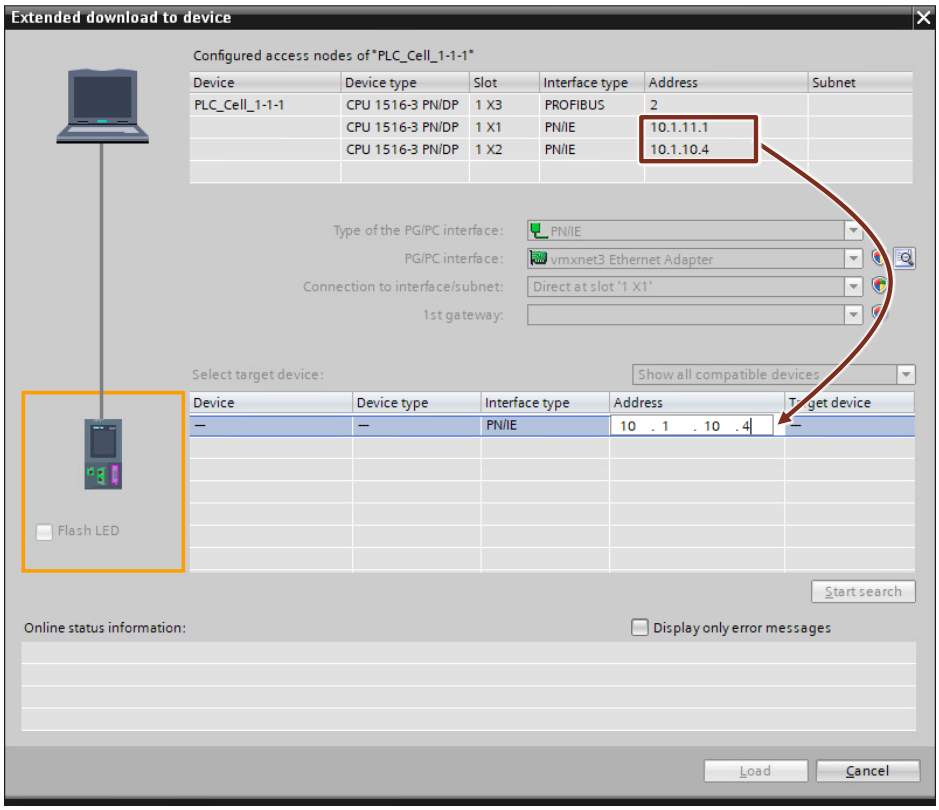
Restrictions for access via routed networks

TIA Portal uses OSI layer-2 protocols to search for devices in the network, initialize devices and perform topology scans. Because these protocols are not capable of routing, it is not possible to search for devices or read the network topology into TIA Portal Network Editor across subnet boundaries, for example.

Access to the CPU from the datacenter or the WLAN-Engineering-Aggregation networks must therefore be structured via the S7 protocol (ISO-on-TCP protocol, port: 102) directly to the IP address of the module.

This direct ISO-on-TCP access can be granted in TIA Portal in the "Extended Download to Device" dialog or the "Go online" dialog with a manually specified IP address. This IP address only has to be entered once. After the connection is established successfully, TIA Portal will save this information in the project context. If you click the "Go online" button or the "Download" button to connect again, then the dialog will not appear a second time. In case the access IP address needs to be changed, open the advanced "Go online" or "Download" dialog again.

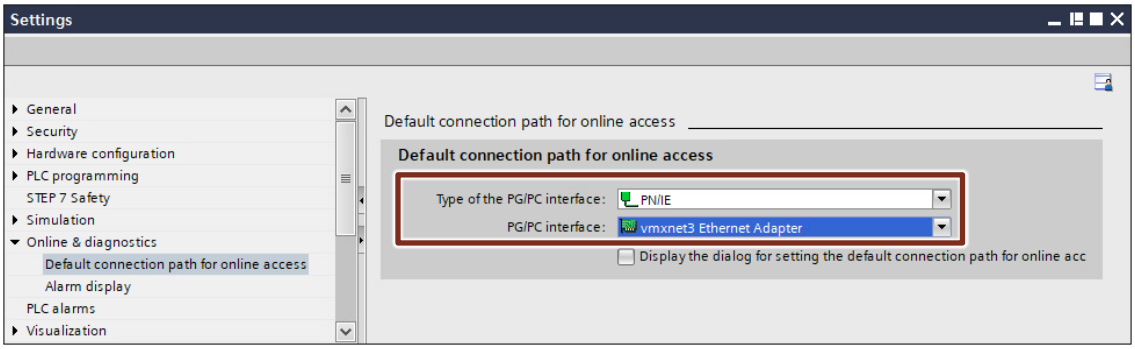
Figure 3-12



There is also the option of defining a preset connection path for online access in the TIA Portal settings.

This preset will cause the network adapter to be pre-populated in the dialogs. For the virtual machines in the datacenter, it is recommended to select the network adapter in the Automation-Engineering subnet. For the Field PGs, the WLAN interface can be preset. If access is being granted with a Field PG right at the cell via Ethernet, the adapter can be reconfigured each time the dialog appears.

Figure 3-13



Device initialization is typically performed when commissioning using TIA Portal right in the cell network.

For service cases, for example when replacing a module, the initialization can be performed via the DCP discovery feature of the network components as an alternative. However, this requires access to the web server of the switch or router.

For more information on this topic, refer to chapter 4.5.15 in the following manual:

SIMATIC NET: Industrial Ethernet Security SCALANCE S615 Web Based Management - \41\

Note

It is always recommended at the start of commissioning to configure the components' hardware with on-site access using a Field PG.

Once the components are reachable via an IP address in the network, configuration and programming can be accomplished from the engineering VMs in the datacenter.

After the network is fully commissioned, a device initialization required when replacing a module on a service call can also be performed via the DCP proxy feature of the SCALANCE components.

Cascaded CPU architectures

CPUs in cascaded network architectures with more than one level are reachable from the datacenter and the aggregation level exclusively via S7 routing (see chapter 2.2.4). This requires that all subnets between the CPUs are configured in the corresponding TIA Portal project.

Access to the web server, OPC UA server or SNMP V1 server is not possible from higher-level networks.

For more information on routed access to the CPUs, please refer to the following FAQ: "How do you configure and enable S7 Routing in STEP 7 (TIA Portal)?" \42\

3.3.6 Configuring access to SIMATIC Unified Comfort Panels/Comfort Panels

Overview of necessary communication services

Engineering

The TCP protocol on TCP port 5001 is always used for engineering the SIMATIC Unified Comfort Panels and SIMATIC Comfort Panels.

This protocol is used for:

- Uploading/downloading the configuration
- Firmware/image updates

The web server (TCP port 443) is a common tool for performing diagnostics without engineering software.

The following access methods are also available if needed:

Access to OPC UA server

The OPC UA server (TCP, default port: 4840) contains hardware information. This way it is possible to read serial numbers, hardware versions and firmware versions as part of an asset management exercise, for example.

Access to SNMP V1 server

An SNMP V1 server (port: TCP 161) is available on the modules for diagnosing the IP and Ethernet stack.

Recommended firewall configuration

For engineering access, it is recommended to allow the HTTPS and OPC UA protocols as well as TCP port 5001 between engineering networks and the SIMATIC panel. All of these protocols provide security in the form of authentication and encryption.

Access paths that entail increased risk due to lack of authentication and encryption should not be allowed as a rule for all engineering networks. This applies here to the HTTP server. In this case, authentication can be accomplished via the SINEMA Remote server on the network level. Therefore it can be expedient to only allow such access through the VPN tunnel with the appropriate authentication and on-site activation on the machine (e.g. with a key-operated switch) (see chapter 4.2 Remote access). The engineering systems then connect themselves with the SINEMA Remote Connect server in the DMZ for this access.

Here are the network component configuration recommendations for engineering the SIMATIC Unified Comfort Panel:

- **Configuration of the DMZ firewall**
  - Allow HTTPS and OPC UA access from the Automation-Engineering subnet to the IP addresses of the Panels in the Automation-Cell subnets (TCP ports 5001, 443, 4840)
  - Allow TCP, HTTPS and OPC UA access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the Panels in the Automation-Cell subnets (TCP ports 5001, 443, 4840)

- **Configuration of the cell firewalls**
  - Allow TCP, HTTPS and OPC UA access from the Automation-Engineering subnet to the IP addresses of the Panels in the Automation-Cell subnets (TCP ports 5001, 443, 4840)

- Allow TCP, HTTPS and OPC UA access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the Panels in the Automation-Cell subnets (TCP ports 5001, 443, 4840)
- Allow TCP, HTTPS, SNMP and OPC UA access from the SINEMA Remote Connect VPN to the IP addresses of the Panels in the Automation-Cell subnets (TCP ports 5001, 443, 161, 4840)

Restrictions for access via cascaded networks

The following SIMATIC Panel generations do not support S7 routing and therefore downloading via the HMI Panel is not possible:

- Basic first-generation Panels (KP300 Basic mono PN, KP400 Basic Color PN, KTP400 Basic Color/mono PN, KTP600 Basic mono PN, KTP600 Basic Color DP/PN, KTP1000 Basic Color DP/PN, TP1500 Basic Color PN)
- Basic 2nd generation Panels support the procedure with device version 14.0.0.0 or later.

3.3.7 Configuration of access to drives

Note

All descriptions in this chapter refer to SINAMICS

- V90 PN
- G120 *
- S120
- S210

* only Control Units with a PROFINET or PROFIBUS interface

Overview of necessary communication services

Engineering

The S7 protocol (ISO-on-TCP protocol on TCP port 102) is used for the Startdrive/STARTER SINAMICS drive engineering system.

This protocol is used for:

- Uploading/downloading the configuration
- Diagnostics and parameter assignment via Startdrive/STARTER "Go Online" function

Web server

The web server (TCP port 80 / 443) is a common tool for performing diagnostics or commissioning without engineering software. The web server can also be used for a firmware update with SINAMICS S120 and S210 drives.

(see also for S120: \57\ or for S210: \58\).

The following access methods are also available if needed:

Access to SNMP V1 server

An SNMP V1 server (TCP port 161) is available on the modules for diagnosing the IP and Ethernet stack. This SNMP server is typically used by asset management systems such as SINEC NMS (see chapter 3.2 Network management).

Recommended firewall configuration

For web server access to the SINAMICS drives between engineering networks and the drive, it is recommended to enable the HTTPS protocol. This protocol provides security in terms of authentication and encryption.

Access paths that entail increased risk due to lack of authentication and encryption should not be allowed as a rule for all engineering networks. This applies here to the engineering access (ISO-on-TCP) and the SNMP server. In this case, authentication can be accomplished via the SINEMA Remote Connect server on the network level. Therefore it can be expedient to only allow such access through the VPN tunnel with the appropriate authentication and on-site activation on the machine (e.g. with a key-operated switch) (see chapter 4.2 Remote access). The engineering systems then connect themselves with the SINEMA Remote Connect server in the DMZ for this access.

Depending on the variant, the following configuration recommendations apply to the network components with regard to the engineering of the SINAMICS drives:

Cell with network separation by the PLC and S7 routing

PROFINET and PROFIBUS drives that are connected to the PLC can be reached by the engineering system via S7 routing. The web server and SNMP-V1 server (PROFINET only) are not accessible via S7 routing.

The S7 access is only configured up to the first network transition (PLC) in the firewall.

- Configuration of the cell firewalls
  - Allow ISO-on-TCP access from the SINEMA Remote Connect VPN to the IP addresses of the drives in the Automation-Cell subnets (TCP ports 102).

Cell with network separation by the PLC and IP forwarding or flat cell

By means of IP forwarding in the SIMATIC PLC or through a flat cell, the PROFINET drives can be reached via OSI Layer 3 and thus also the web server and SNMP V1 server.

- Configuration of the DMZ firewall
  - Allow HTTPS access from the Automation-Engineering subnets to the IP addresses of the drives in the Automation-Cell subnets
    (TCP port 443)
  - Allow HTTPS access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the drives in the Automation-Cell subnets (TCP port 443)

- Configuration of the cell firewalls
  - Allow HTTPS access from the Automation-Engineering subnets to the IP addresses of the drives in the Automation-Cell subnets (TCP port 443)
  - Allow HTTPS access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the drives in the Automation-Cell subnets (TCP port 443)
  - Allow ISO-on-TCP, HTTPS and SNMP V1 access from the SINEMA Remote Connect VPN to the IP addresses of the drives in the Automation-Cell subnets (TCP ports 102, 443, 161)

Restrictions for access via routed networks

The restrictions for SINAMICS drives are the same as those with SIMATIC CPUs (see chapter 3.3.5).

Cascaded drive architectures

Drives in cascaded network architectures with more than one level are reachable from the datacenter and the aggregation level exclusively via S7 routing (see chapter 2.2.4). This requires that all subnets are configured in the corresponding TIA Portal project.

Access to the web server and SNMP V1 server is not possible from higher-level networks.

For more information on routed access to the drives, please refer to the following FAQ: "How do you configure and enable S7 Routing in STEP 7 (TIA Portal)?" \42\

Overview S7 protocol/web server

SINAMICS drives can be configured with the engineering systems Startdrive or STARTER. One exception is the SINAMICS V90 PN drive which is configured in TIA Portal with HSP 0185.

All SINAMICS drives described here support the S7 protocol. SINAMICS S120 and S210 additionally have an integrated web server.

Table 3-11

	V90 PN	G120	S120	S210
S7 protocol (ISO-on-TCP, port 102)	X	X	X	X
Integrated web server (https, port 443)	-	-	X	X

3.3.8 Configuration of access to I/O devices

Overview of necessary communication services

Engineering

The I/O devices are typically integrated below the CPU as PROFINET devices. The CPU is usually responsible for configuration and monitoring of these components. This means that the S7 protocol (ISO-on-TCP protocol on TCP port 102) to the CPU is used here as a rule when engineering the I/O devices.

The I/O devices are initialized with the DCP protocol.

The following direct access methods to the I/O device are also available if needed:

Access to SNMP V1 server

An SNMP V1 server (port: TCP 161) is available on the modules for diagnosing the IP and Ethernet stack.

More information on the communication services employed can be found in chapter 3.2 of the following manual:

SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication \40\

It is generally a good idea to enable access from engineering systems to the web servers of the I/O devices:

Note If I/O Link devices are used, UDP ports 34964 and 49152 to 65535 must be allowed because the I/O Link devices are commissioned and diagnosed by reading/writing PROFINET data records.

Recommended firewall configurations

The following configuration is recommended for access to the web interfaces of the I/O modules:

Appendix IX – Firewall rule engineering – contains a detailed list with IP addresses.

- **Configuration of the DMZ firewall**
  - Allow HTTPS access from the engineering VMs to the I/O devices in:
    - Monitoring and Management subnet
    - Management-DMZ subnet
    - Transfer&Management-Aggregation subnets
    - Automation-Cell subnets
    - PROFINET subnets
  - Allow HTTPS access from the Field PGs in the WLAN-Engineering-Aggregation subnets to the I/O devices in:
    - Monitoring and Management subnet
    - Management-DMZ subnet
    - Transfer&Management-Aggregation subnets
    - Automation-Cell subnets – PROFINET subnets
  - Allow HTTPS access from the Field PGs in the Automation-Cell subnets to the I/O devices in:
    - Monitoring and Management subnet
    - Management DMZ subnet
    - Transfer&Management-Aggregation subnets
- **Configuration of the cell firewalls**
  - Allow HTTPS access from the engineering VMs and from the Field PGs in the WLAN-Engineering-Aggregation subnets to the I/O devices in:
    - Automation-Cell subnets
    - PROFINET subnets
  - Allow HTTPS access from the Field PGs in the Automation-Cell subnets to the I/O devices in:
    - Monitoring and Management subnet
    - Management DMZ subnet
    - Transfer&Management-Aggregation subnets

Restrictions for access via routed networks

It is always recommended at the start of commissioning to configure the components' hardware with on-site access using a Field PG.

Once the components are reachable via an IP address in the network, configuration and programming can be accomplished from the TIA Portal VMs in the datacenter.

After the network is fully commissioned, a device initialization required when replacing a module on a service call can also be performed via the DCP proxy feature of the SCALANCE components. In case of network isolation, the gateway is the CPU. If there is no network isolation, the gateway is the SCALANCE component (see cell 1-2-2 for an example).

3.3.9 Configuration of access to SIRIUS industrial controls

The following setup is restricted to the following components:

- SIRIUS Control (circuit breakers, contactors, overload relays, load feeders)
- SIRIUS Hybrid (motor starters, soft-starters)
- SIRIUS Command (command/reporting/recording devices)
- SIRIUS Monitor (protection, monitoring and control functions)

For the PROFINET/PROFIBUS devices in the SIRIUS Hybrid and SIRIUS Monitor product families, the same requirements apply as with the I/O devices per chapter 3.3.8.

Chapter 3.3.5 describes the necessary access to the web servers and OPC UA servers of the communication-enabled products from the SIRIUS Hybrid family.

Some products from the SIRIUS Control, Command and Monitor families have I/O Link or AS-i/ASIsafe communications capability on the field level.

3.3.10 Configuration of access to Industrial Edge

Overview of necessary communication services

Edge components are engineered with web interfaces. Here there is an option for an Industrial Edge device (IED) to establish an SSH tunnel to the Industrial Edge Management (IEM), allowing all relevant configuration data from the IED to appear in the web interface of the IEM.

This method is always recommended. This makes it possible to engineer from a central location, the IEM. However, especially for configuration of the installed apps, there can be cases in which direct access to the web server of the IED is required. Therefore it is recommended to allow outbound HTTPS access from the engineering systems to all Edge components.

Recommended firewall configurations

The firewall configuration recommendation below follows from the communication architecture described previously:

- **Configuration of the DMZ firewall**
  - Allow HTTPS access from the Automation-Engineering subnet to the IP addresses of the IEM and IEDs (TCP port: 443)
  - Allow HTTPS access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the IEM and IEDs (TCP port: 443)
  - Allow HTTPS access from the DHCP ranges of the Automation-Cell subnets to the IP address of the IEM (TCP port: 443)
- **Configuration of the cell firewalls**
  - Allow HTTPS access from the Automation-Engineering subnet to the IP addresses of the IEDs (TCP port: 443)
  - Allow HTTPS access from the WLAN-Engineering-Aggregation subnets to the IP addresses of the IEDs (TCP port: 443)
  - Allow HTTPS access from the DHCP ranges of the Automation-Cell subnets to the IP address of the IEM (TCP port: 443)

3.3.11 Configuration of access to network components

The network components in the aggregation level and in the Automation-Cell subnets are managed centrally with SINEC NMS in this concept. Chapter 3.2 contains additional details and information on the necessary communication connections here.

Switches under the CPU are typically integrated as PROFINET devices. The CPU is thus responsible for configuration and monitoring of these components.

However, it is a good idea to allow access from engineering systems to the web servers of the switches for the following reasons:

- Access to the web interfaces of the switches in the automation cell networks / PROFINET networks is necessary in order to use the DCP proxy functionality.
- The web interfaces often receive important information for diagnosing network faults (e.g. ARP tables, port statistics).

To simplify the addressing of the web interfaces, the appropriate DNS records can be created in SINEC INS.

Recommended firewall configurations

The following configuration is recommended for access to the web interfaces of the network components:

Appendix IX – Firewall rule engineering – contains a detailed list with IP addresses.

- **Configuration of the DMZ firewall**
  - Allow HTTPS access outbound from the engineering VMs to the network components in:
    - Monitoring and Management subnet
    - Management DMZ subnet
    - Transfer&Management-Aggregation subnets
    - Automation-Cell subnets
    - PROFINET subnets
  - Allow HTTPS access from the Field PGs in the WLAN-Engineering-Aggregation subnets to the network components in:
    - Monitoring and Management subnet
    - Management DMZ subnet
    - Transfer&Management-Aggregation subnets
    - Automation-Cell subnets
    - PROFINET subnets
  - Allow HTTPS access from the Field PGs in the Automation-Cell subnets to the network components in:
    - Monitoring and Management subnet
    - Management DMZ subnet
    - Transfer&Management-Aggregation subnets
- **Configuration of the cell firewalls**
  - Allow HTTPS access from the engineering VMs and from the Field PGs in the WLAN-Engineering-Aggregation subnets to the network components in:
    - Automation-Cell subnets

- PROFINET subnets

- Allow HTTPS access from the Field PGs in the Automation-Cell subnets to the network components in:
  - Monitoring and Management subnet
  - Management DMZ subnet
  - Transfer&Management-Aggregation subnets

- **Configuration of SINEC INS**

  In case the DNS records are not automatically generated through the use of DHCP, there is the option of creating manual DNS records in SINEC INS.

3.4 Update management

3.4.1 Components and application

Introduction

An update is a process by which existing software is replaced with a new version. This newer version can contain fixes for security holes and/or improve general functionality, user-friendliness or performance of the software.

To increase efficiency and reduce the time and work spent on updating plant devices and systems, a central update management solution must be integrated into the plant.

Update management refers to the scheduled method of installing updates on machines and systems. Update management includes not only technical implementation but also the relevant organizational measures, such as when, how often and in what way which updates are rolled out to the plant.

Central user management provides additional security by deploying the latest security patches for all exposed devices. It also helps maintain system uptime by keeping software and applications up to date and ensuring smooth operation. Another important point is the observance of officially mandated security standards where cyberattacks are concerned.

The update management system is located in the datacenter and in the DMZ. It is recommended to connect the server to the internet via a proxy server. In this way it is possible to download the latest firmware and roll it out to the devices and systems in the plant while at the same time ensuring that all automation cells are isolated from the internet. The IT department is responsible for maintaining the update management system. They will ensure that the latest updates and firmware versions are available on the update management system for the end devices.

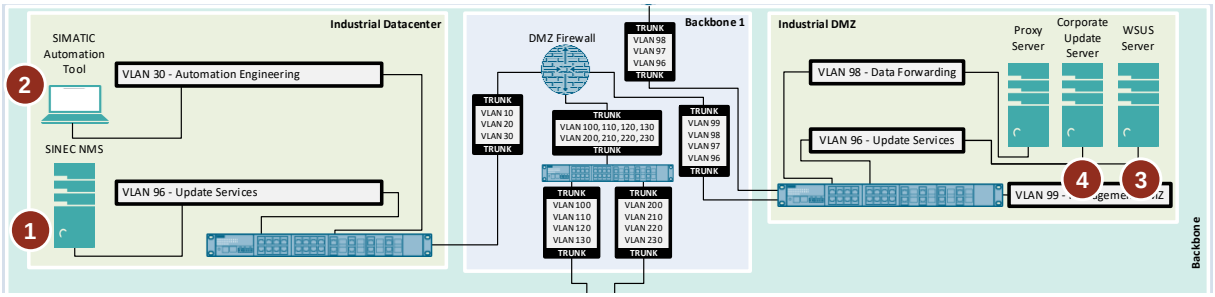
Besides the engineering stations, the update process in the plant also includes the updating of network components, CPUs and HMI stations. The update management system must be able to deploy updates for all these devices and systems in the plant.

Components and placement in the network concept

This system can be broken down into 4 parts:

1. SINEC NMS for updating the network components.
2. SIMATIC Automation Tool (SAT) installed on a Windows machine to update CPUs and HMI stations. This tool has an internet connection via the proxy server so that it can download firmware update files.
3. Windows Server Update Services (WSUS) to update Windows machines and HMI systems.
4. Corporate update server for updating TIA Portal software.

Figure 3-14



3.4.2 Updates for network components via SINEC NMS

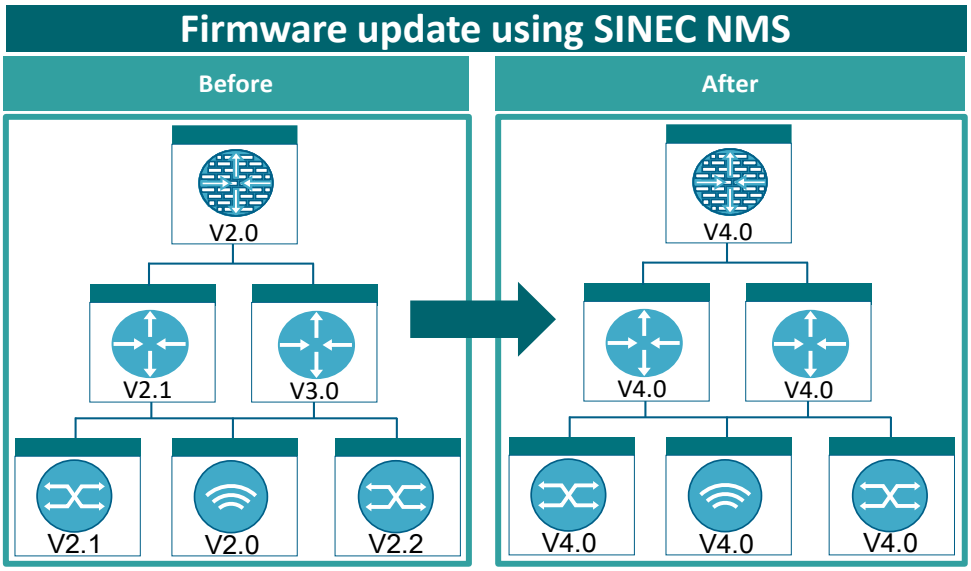
Network components like those from the SCALANCE or RUGGEDCOM series can be updated centrally using SINEC NMS.

The SCALANCE devices load firmware update files (available on SINEC NMS) via the SFTP protocol.

Task description and principle

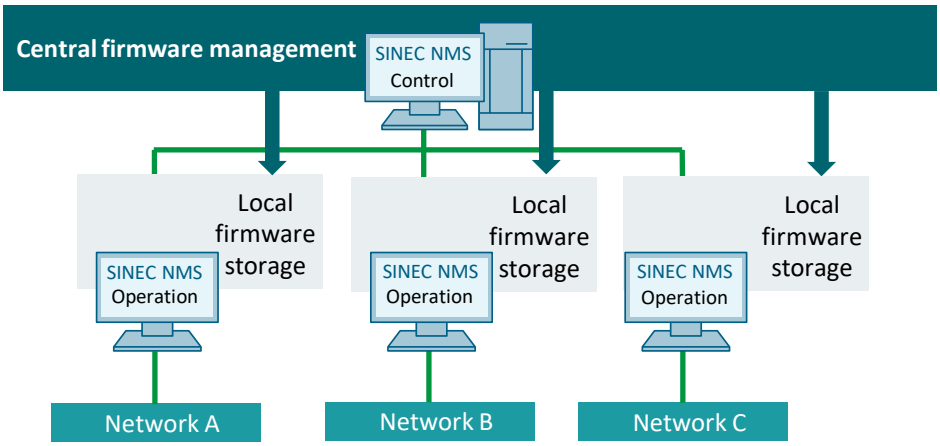
A network administrator may need to adjust the firmware versions of network components to reflect new features or global company policies. SINEC NMS gives the administrator the ability to manage firmware versions centrally to reduce effort and ensure that firmware versions are up-to-date.

Figure 3-15



SINEC NMS provides the ability to download firmware files to SCALANCE/RUGGEDCOM components. In the SINEC NMS system, the firmware files are managed centrally in firmware containers in the Control and can be rolled out plant-wide via policies. Each change to the firmware containers in the Control is automatically synchronized with the Operations. When major changes are made to the firmware containers, synchronization with the Operations can take some time.

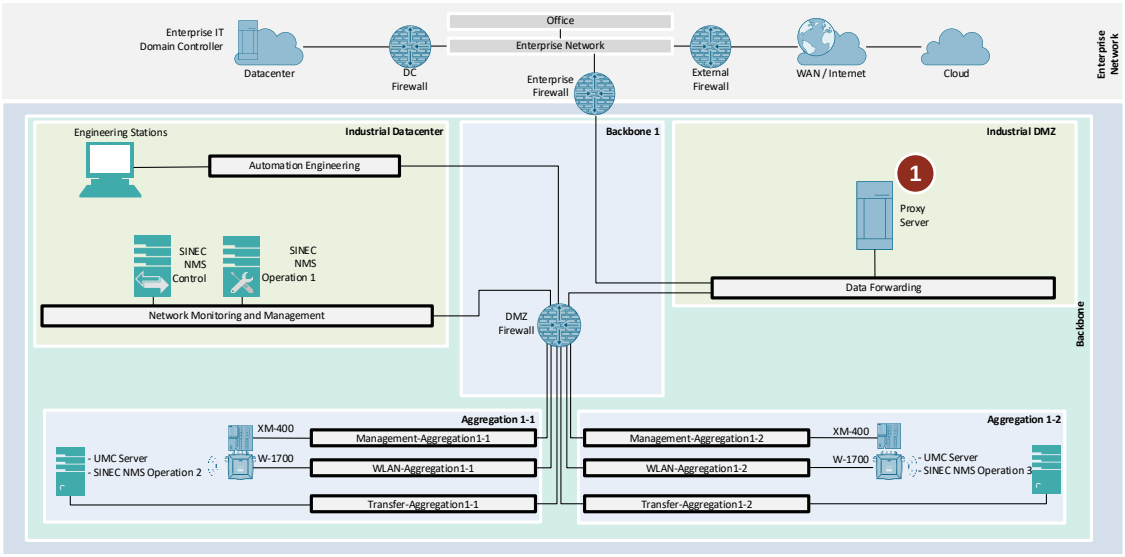
Figure 3-16

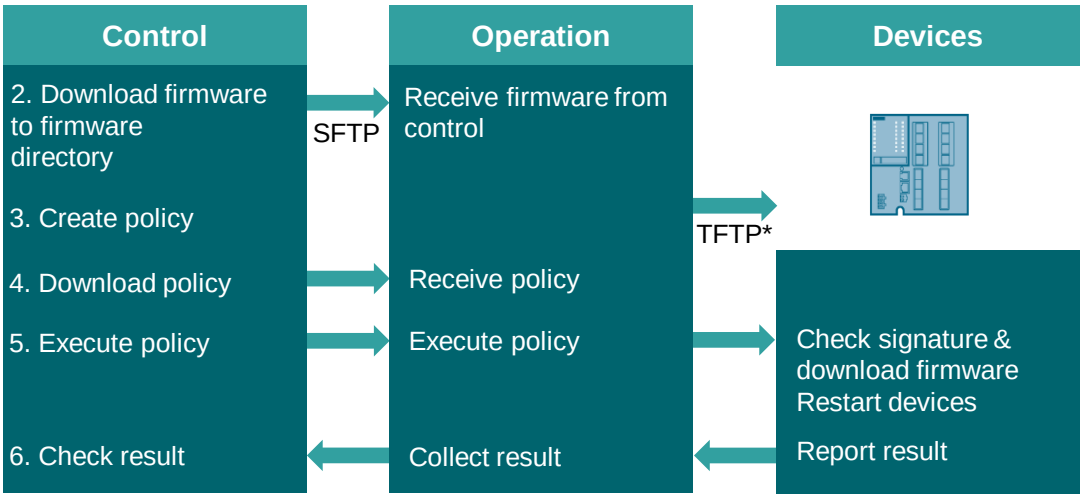


The update process

The diagrams below explain the essential sequence of a firmware update to a SCALANCE XM-400 switch.

Figure 3-17





1. It is recommended to connect to the internet via a proxy server. This will provide the latest firmware files for upgrading the SCALANCE devices. Current firmware versions are provided by SIOS.
2. First, the firmware file must be stored in the SINEC NMS Control. The system then transfers the file to all Operations via SFTP (TFTP). The appropriate devices are assigned using their item numbers.
3. To perform a firmware update, a policy must be created. In the policy you will specify a time for the firmware update and which devices it affects. Here, SINEC NMS takes into account the topology to provide for a smooth update process.
4. The firmware update policy is loaded to the Operations. Then the policy must be activated.
5. While executing the policy, the Operation communicates with the devices. A restart, triggered by the policy, is required to activate the firmware.
6. Once the policy has been executed, the result (successful, unsuccessful, error) will be displayed for each device.

Note

SINEC NMS requires SNMP write access to the devices in order to perform the firmware update.

The devices will be inaccessible for a period of time when you restart them. Therefore, in linear network topologies, the order in which the devices will restart must be taken into consideration. In this case we recommend a path-based strategy in which the most remote device is restarted first.

Additional information

You can find further information on firmware updates via SINEC NMS in SIOS under the article ID: 109762792.

3.4.3 Access configuration for SINEC NMS

A firmware update to SCALANCE network components requires SINEC NMS to have access to these components via the SNMP protocol.

Conversely, the components must have SFTP access to SINEC NMS in order to download the firmware update files.

SINEC NMS must also have internet access so that it can download the firmware update files.

Configuration of the DMZ firewall

- Allow SNMP access from SINEC NMS to the network components (TCP port 161).
- Allow SFTP access from the network components to the SINEC NMS server.
- Allow HTTPS access between SINEC NMS and the internet via the proxy server.

Table 3-12

From	To	Port	Protocol	Service
SINEC NMS	SCALANCE	161	TCP	SNMP
SCALANCE	SINEC NMS	22	TCP	SFTP
SINEC NMS	Internet	443	TCP	HTTPS

Configuration of the cell firewalls

- Allow SNMP V1 access from SINEC NMS to the network components (TCP port 161).
- Allow SFTP access from the network components to the SINEC NMS server.

Table 3-13

From	To	Port	Protocol	Service
SINEC NMS	SCALANCE	161	TCP	SNMP
SCALANCE	SINEC NMS	22	TCP	SFTP

3.4.4 Update CPUs and HMI Panels via SAT

The SIMATIC Automation Tool (SAT) is used for central firmware update management of CPUs and HMI Panels.

This tool is installed on a virtual Windows machine. It has connections to the automation cells and to the internet via the proxy server.

The user creates a project in SAT that contains all the IP addresses of the components that will be updated. For this reason it is crucial to have available a complete list of the IP addresses of the devices.

Additional information on SAT can be found in the article ID: 109794330.

3.4.5 Access configuration for SAT

SAT should be able to access the internet so it can download firmware update files. It must also be able to communicate with the CPU and the HMI in the cells. The network requirements for the SAT VM are thus:

- **Communication between SAT VM and internet**
  SAT downloads the firmware update files over HTTPS from the Siemens Industry Online Support website.
- **Communication between SAT VM, CPU and HMI in the cells**
  SAT must access the cells to load the firmware update files to the devices. Here, ISO-on-TCP is used for uploading the firmware files.

Configuration of the DMZ firewall

- Allow HTTPS access between SAT and the internet via the proxy server (TCP port 443).
- Allow ISO-on-TCP access between SAT and the CPUs and HMIs for updating the firmware of these devices (TCP port 102).

Table 3-14

From	To	Port	Protocol	Service
SAT	Internet	443	TCP	HTTPS
SAT	CPU	102	TCP	ISO-on-TCP
SAT	HMI Panel	102	TCP	ISO-on-TCP

Configuration of the cell firewalls

- Allow ISO-on-TCP between SAT and CPU and HMI for updating the firmware on these devices (TCP port 102).

Table 3-15

From	To	Port	Protocol	Service
SAT	CPU	102	TCP	ISO-on-TCP
SAT	HMI Panel	102	TCP	ISO-on-TCP

3.4.6 Update Windows and HMI systems via Windows Server Update Services

Update management for this system should be implemented centrally for administrative as well as security reasons. This means that not every computer downloads its own updates from the internet. Rather, a central server centrally downloads the patches once and provides them to all computers of an automation system for installation.

Windows Server Update Services – WSUS

Use of WSUS is recommended for implementing central update management. This is available from Microsoft free of charge and includes all functions needed for update management.

Requirements for update management with TIA/WinCC

- Update management must not negatively impact process operations in an automation system.
- Microsoft provides updates to close existing security gaps in Windows components. This must happen quickly to protect systems before any hackers exploit these gaps. That is why with PC-based systems (WinCC/engineering stations) it is recommended to install patches immediately after Microsoft publishes them.
- Placement of WSUS:
  Because WSUS requires a connection to the internet (to the Microsoft sites), it should be placed in the DMZ network. It is recommended to use a proxy server to connect the WSUS server with the internet.
- Update groups
  Computers that are supplied with updates at the same time are organized in an update group. Because the installation of a security update generally triggers a restart of the computer, it should be ensured that redundant systems are organized in different update groups. This means that a redundant PCS 7 OS server pair must be split between two different update groups. This is the only way to ensure that patching is possible during operation.
  Among other things, formation of update groups enables the following:
  - Specific updates for different update groups
  - Updating at different times

3.4.7 Access configuration for Windows Server Update Services

The WSUS server must connect to the internet via the proxy server. In addition, it must communicate with the Windows computers, which entails the following requirements:

Configuration of the proxy server

The proxy server must support the HTTPS and SSL protocols; it must use the basic authentication procedure or Windows authentication. (TCP port 80, TCP port 443).

Configuration of the DMZ firewall

Allow the following ports in the DMZ firewall:

- For WSUS 3.2 and earlier: HTTP and HTTPS (TCP port 80, TCP port 443).
- With WSUS 6.2 and higher (at least Windows Server 2012): HTTP (TCP port 8530) and HTTPS (TCP port 8531).

The firewall on the WSUS server must be configured in such a way that it allows inbound data traffic at these ports.

Table 3-16

From	To	Port	Protocol	Service	Version
WSUS server	Windows PCs	80	TCP	HTTP	≤ V3.2
WSUS server	Windows PCs	443	TCP	HTTPS	≤ V3.2
WSUS server	Windows PCs	8530	TCP	HTTP	≥ V6.2
WSUS server	Windows PCs	8531	TCP	HTTPS	≥ V6.2
WSUS server	Internet	443	TCP	HTTPS	All

Configuration of the cell firewalls

Table 3-17

From	To	Port	Protocol	Service	Version
WSUS server	Windows PCs	80	TCP	HTTP	≤ V3.2
WSUS server	Windows PCs	443	TCP	HTTPS	≤ V3.2
WSUS server	Windows PCs	8530	TCP	HTTP	≥ V6.2
WSUS server	Windows PCs	8531	TCP	HTTPS	≥ V6.2

3.4.8 Updates for TIA Portal software via corporate update server

The corporate update server is used to centrally update TIA Portal within a factory. Then you can store selected updates and support packages on a local server and make them available to the users, for example for different production lines.

The advantage of this is that the users do not need to access the internet. Rather, they can install the updates via the intranet. Because the users do not need direct access to the internet, security against trojans or malware that may contact the internet from the internal enterprise network is greatly increased.

A corporate server can only be deployed on a Microsoft Server operating system because the IIS service and a running IIS server are necessary to run the BITS.

Additional information on the corporate update server can be found in the article ID: 109798671.

3.4.9 Access configuration for the corporate update server

All TIA Portal engineering stations must be able to access the corporate update server, which in turn connects via the proxy server with the internet.

Configuration of the proxy server

Allow an HTTPS connection from the corporate update server to the internet.

Configuration of the DMZ firewall

Allow the connection (TCP port 8888) between the TIA Portal PCs/VMs and the corporate update server.

Table 3-18

From	To	Port	Protocol	Service
TIA Portal	Corporate update server	8888	TCP	-
Corporate update server	Internet	443	TCP	HTTPS

Configuration of the cell firewalls

Table 3-19

From	To	Port	Protocol	Service
TIA Portal computer	Corporate update server	8888	TCP	-

3.5 Virtualization

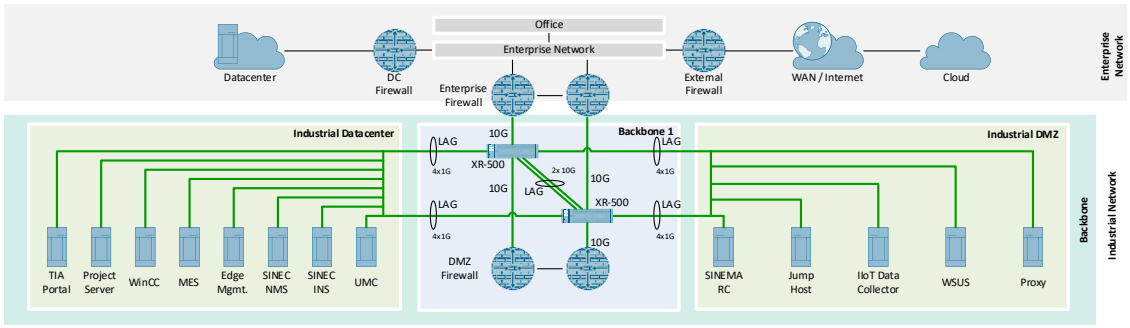
3.5.1 Components and application

Introduction

This chapter describes how to structure the industrial datacenter and the industrial DMZ with or without a virtualization solution.

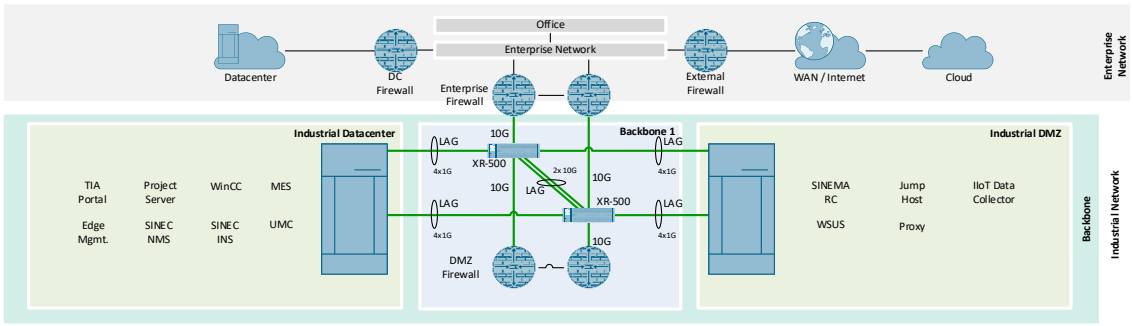
Industrial datacenter without virtualization

Figure 3-18



Industrial datacenter with virtualization

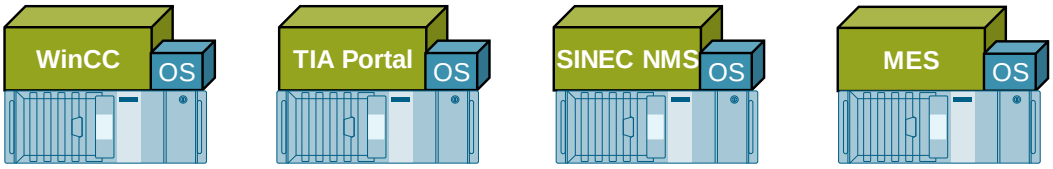
Figure 3-19



Industrial datacenter without virtualization

In the traditional model (without virtualization), each industrial datacenter can add a new server where the operating system and the appropriate user software are installed.

Figure 3-20



Advantages

- Simple troubleshooting in the system
- This solution is preferred in smaller industrial datacenters for cost reasons.
- While IT servers are almost always located in climate-controlled industrial datacenters, industrial PCs in production areas are often exposed to electromagnetic radiation, more extreme temperatures, vibration and shocks, as well as dirty and/or humid air. With the proper hardening, e.g. fanless or designed with a higher protection rating, Siemens devices can run reliably despite their demanding environment.

Disadvantages:

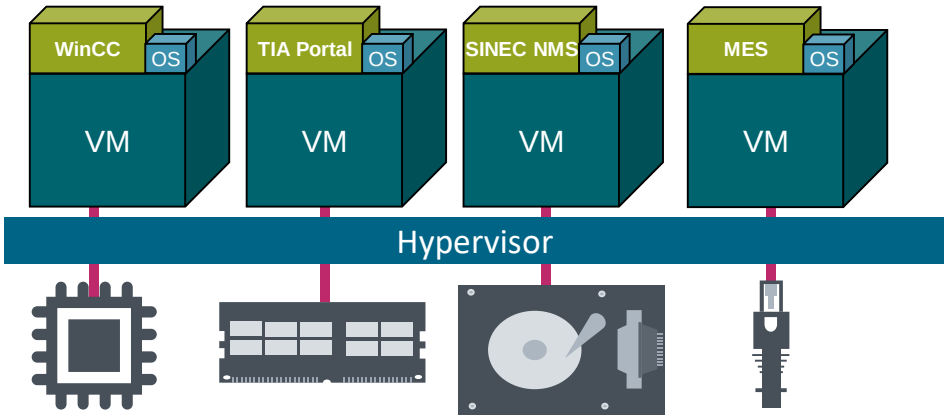
- High energy demand
- High space requirement
- For each new application, a new computer, redundant power supplies and UPS must be ordered. This costs time and money.
- High administrative overhead and maintenance.
- Large number of ports necessary between switch and servers.

Industrial datacenter with virtualization

IT systems that were previously implemented on different physical servers can be bundled together on one hardware platform with the aid of virtualization. Virtualization decouples the operating system and the user software of a computer from its hardware.

The operating system and the user software are provided in the form of a virtual machine (VM). The hypervisor dynamically distributes the hardware resources to the various virtual machines. Common hypervisors are VMware ESXi or Microsoft Hyper-V. The virtual machines run operating systems such as Microsoft or Linux. The operating system runs applications such as WinCC, TIA Portal, SINEC NMS or an MES system.

Figure 3-21



Advantages

- Energy savings
  - Less energy is required thanks to optimized usage of existing hardware.
  - Fewer UPS battery systems are needed to cover temporary power outages.
  - Smaller dimensioning of the backup diesel generator for longer power outages.
- Higher flexibility and availability
  - New virtual machines can be added quickly. IT infrastructure is easily scalable and expandable.
  - Virtual machines can be quickly moved from one server to another.
  - High availability is possible because once a server fails, all virtual machines can be started on another server automatically.
  - Independent of the hardware employed
  - Simple backup with snapshots
  - Simpler redundancy concepts for the hardware (one RAID system for the virtualization computer instead of for each individual computer)
- Low space requirements
  - Administrators do not need to occupy themselves with managing and maintaining standalone computers.
  - Fewer ports required for wiring between switch and virtualization system

Disadvantages

- Longer troubleshooting process due to the complexity of the system. A new software layer is introduced which can contain errors and which must be secured.
- In addition to the virtualized servers, there is typically a virtualized network level as well, which entails additional complexity.

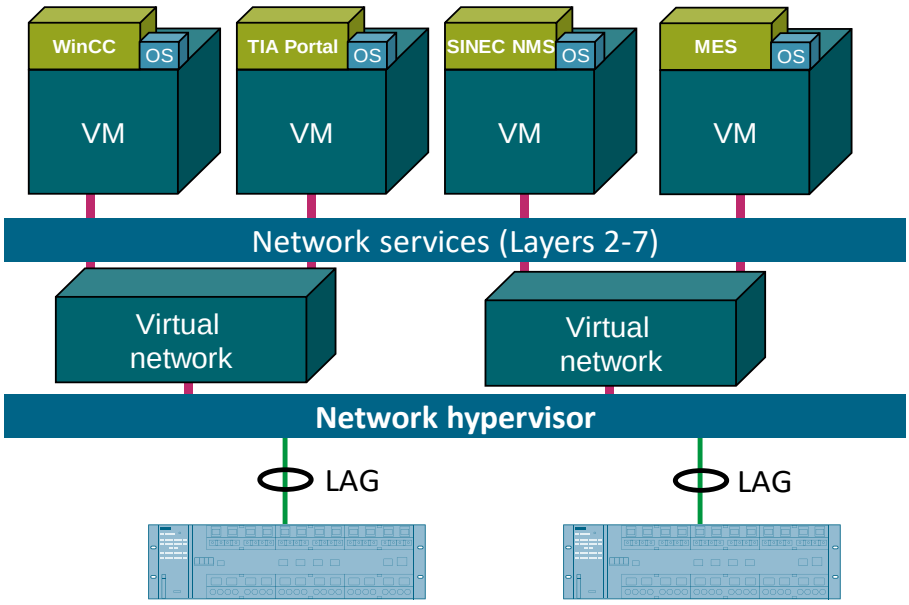
3.5.2 Network virtualization (NFV)

Network virtualization pairs a physical network with a logical virtual layer that decouples the network from physical realities. In this case, the tasks of routers, switches and firewalls are

provided through software components. One example of a network virtualization software program is NSX Data Center from VMWare.

Network virtualization optimizes the performance, reliability, flexibility, scalability and security of the system.

Figure 3-22



The network hypervisor establishes a physical connection to the XR-500 switches to obtain physical access to the network. With network virtualization, virtual routers, firewalls or switches can be configured into a virtual network. Network services such as load balancing and virtual firewalls are available, and network traffic can be measured. The virtual industry applications provided by VMs are connected with the virtual network.

The connection to the virtualization environment is established using Link Aggregation (LAG) / Link Aggregation Control Protocol (LACP). Bundling multiple LAN interfaces increases throughput and resilience to failure.

Additional information

- Information on Link Aggregation: \59\
- Further information on the topic of SIMATIC Virtualization as a Service: \60\.
- Examples of project engineering and configuration of a virtualization solution: \61\

3.6 User management

3.6.1 Components and application

The User Management Component (UMC) facilitates centralized administration of user accounts for many Siemens products, including:

- TIA Portal
- WinCC Unified PC Runtime and Unified Comfort Panels
- WinCC Runtime Advanced and Comfort Panels
- SINEMA Remote Connect
- SINEC NMS
- SINEC INS
- SCALANCE network components (via SINEC INS)

Engineering components

Central user management is based on the following components:	Description
UMC ring server	The UMC ring server represents the central configuration platform for user management. Here, users are defined with the relevant group assignments for the UMC domain. To connect to enterprise IT systems, it is possible to import a user and/or groups from an Microsoft Active Directory. A requirement for this is that the UMC ring server PC has been added to the Active Directory. The UMC ring server can be realized in a redundant configured to increase availability.
UMC server	The UMC server is essentially a stand-in for the ring server. This substitution principle enabled load distribution, for example during a rush of logins at a shift change. The UMC server also supports caching of user accounts in case the connection to the ring server or domain controller is temporarily unavailable. In this case, the UMC server receives updates from the UMC ring server on a cyclic basis. The authentication can occur locally, thus not placing a load on the ring server. For Active Directory users, the UMC server is directly responsible for communication with the domain controller. Therefore, when using the Active Directory, the UMC server PC must also be part of the domain. The UMC server can be installed by itself or in conjunction with additional software. A standalone installation is suitable for the engineering VLAN in the datacenter, for example. If a PC with a Windows operating system needs to be available in the cell level or aggregation level, it is recommended to install a UMC server in this location.

Central user management is based on the following components:	Description
TIA Administrator	Connection to the TIA Portal computer is accomplished with the TIA Administrator tool. There are essentially 2 possible modes in this case: **UMC agent:** The UMC agent represents an authentication client. The agent does not retain a user database. It is configured for access to a UMC server or UMC ring server. Any login made in the UMC context is forwarded to the configured server. Therefore, when using the agent, no integration into the Active Directory is necessary. UMC agents are typically used in systems that are not continuously connected and which are thus not expected to have a current user database (e.g. a Field PG used by a service technician on a temporary assignment). **UMC runtime server:** Unlike the UMC agent, the UMC runtime server retains a user database on the engineering system. Other services such as SLRA can also be provided by the runtime server. This concept favors the runtime server for the engineering systems thanks to caching of users. This way, for example, it is possible to sign in to a TIA project even if there is momentarily no network connection. To use the runtime server, the engineering VM or the Field PG must be integrated into the Active Directory.
UMC-L	UMC-Local (UMC-L) is a software component in the WinCC Unified context. This component is included in any WinCC Unified installation; it is responsible for local user management on the operator device. The main advantage of this component is independence from Microsoft Windows and the Active Directory (for example with Unified Comfort Panels). UMC-L can be configured in 2 modes: • Local User Management (UMC-L-LUM) Users are managed purely locally. No connection to a UMC server or UMC ring server is configured. • Global User Management (UMC-L-GUM) Users are managed purely globally. This mode connects the WinCC Unified installation to a UMC server or UMC ring server. Due to the fact that the UMC-L-GUM service does not support user caching, the additional installation of a UMC server is recommended with all Microsoft Windows-based WinCC Unified stations. Install the UMC server first in this installation sequence. The subsequent installation of WinCC Unified is then coupled directly to the UMC server as part of the installation routine.

Central user management is based on the following components:	Description
SIMATIC Logon Remote Authenticator (SLRA)	The SIMATIC Logon Remote Authenticator can be activated after installation on the ring server and server stations. This service facilitates authentication using the SIMATIC Logon protocol via UMC and thus requires no additional SIMATIC Logon server be provided. Similar to SIMATIC Logon, only authentication of AD users is supported. This applies especially to older visualization systems such as WinCC Runtime Advanced or Comfort Panels. WinCC Runtime Advanced can always be installed together with a UMC server on one PC. The SLRA service can then be used via the localhost address. User caching on the WinCC station is realized with the UMC server. Additionally, this UMC server can then receive authentication requests from the local network.

Note

The installation routine for the UMC server is not available for download. It can be found on TIA Portal DVD 2.

After the installation, the documentation is located in the following folder:
"C:/Program Files/Siemens/Automation/UserManagement/Documentation"

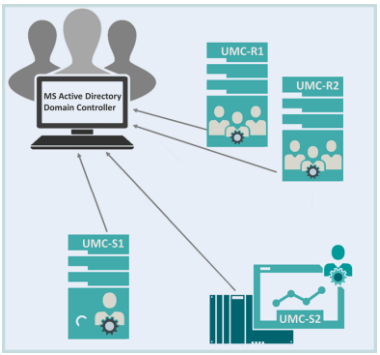
Additional information

As a supplement to the documentation, the configurations of the most important use cases are described in SIOS as an application example: \5\.

3.6.2 Communication links for the UMC components

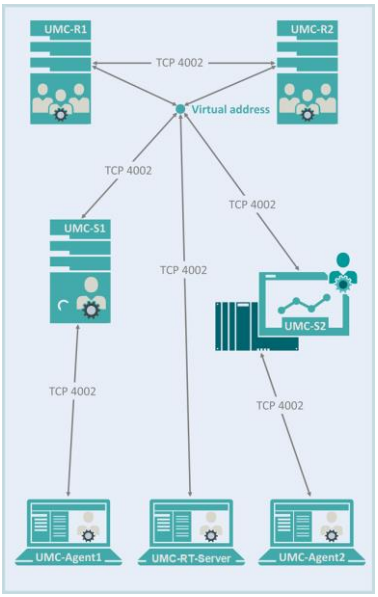
The UMC components require the following connections to run:

Communication between UMC (ring) server and Microsoft Active Directory:



In case users or user groups are imported from an Active Directory, all stations with UMC ring server, UMC server or UMC runtime server services must be integrated into the Active Directory.
To communication connections to the domain controller necessary for this purpose depend on the operating system version you are using.
For more information, refer to the following Microsoft article:
\4\ - "How to configure a firewall for Active Directory domains and trusts"

Communication between UMC agent, UMC server and UMC ring server

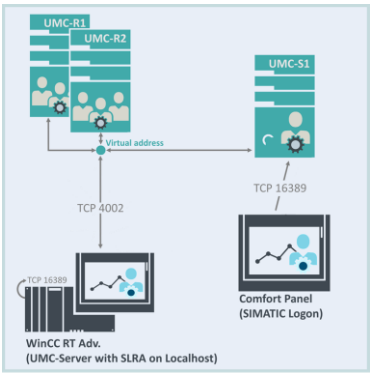


Communication between the UMC agent/RT server, UMC server and UMC ring server takes place through TCP port 4002 in the default configuration. The communication is bidirectional. Therefore, the port be opened for inbound connections for agents, runtime server, server and ring server.

In case of a redundant configuration, the ring servers are reachable at a shared virtual IP. The communication between the two ring servers runs through TCP port 4002 in this case as well.

Depending on its configuration, an agent can connect to a server or a ring server.

Communication between UMC-L-GUM and UMC (ring) server

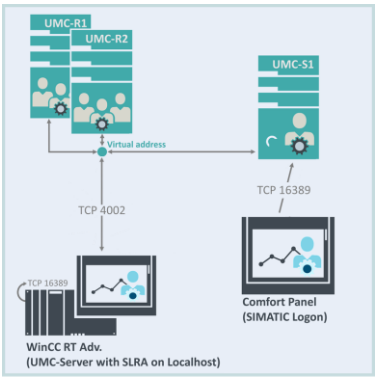


For installations of WinCC Unified without a full-fledged UMC server, the outbound communication from the UMC-L-GUM URL runs over HTTPS. Because in this case the user database is not synchronized, only the outbound connection from the UMC-L-GUM service is necessary.

Depending on the configuration, a UMC-L-GUM service can connect to a UMC-RT server or a UMC ring server.

The TCP port depends on the web server configuration of the UMC server (default: TCP, 443).

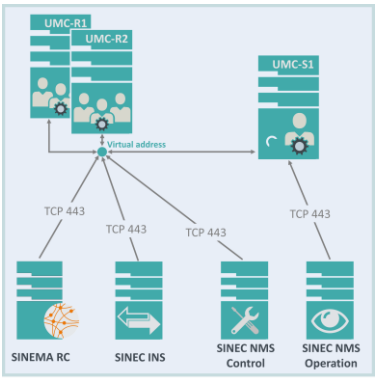
Communication between SIMATIC Logon clients and UMC



A link between WinCC Runtime Advanced and Comfort Panels is possible with the SLRA service. Given the appropriate configuration, the SLRA service can be provided both in the server as well as the ring server. The WinCC instances are configured in the accustomed manner as with SIMATIC Logon. The port is freely configurable (default: TCP 16389, outbound from WinCC).

In case a UMC server runs together with WinCC Runtime Advanced on the same PC, the communication to the ring server runs bidirectionally on TCP port 4002 as described above.

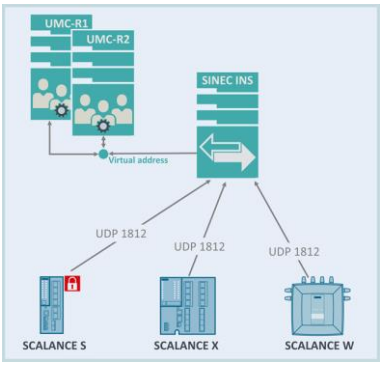
Communication between SINEC NMS, SINEC INS, SINEMA RC and UMC



SINEC NMS, SINEC INS and SINEMA Remote Connect use the remote authentication service of the web server. Therefore, the connection is possible to the UMC server as well as the ring server.

The communication is outbound from the SINEC or SINEMA components. It is HTTPS-based and requires the IP address and web server port of the UMC server (which may be redundant) and/or ring server (default: TCP 443).

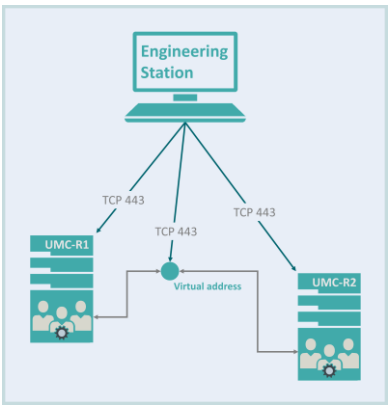
Communication between network components, SINEC INS and UMC



SINEC INS is used to connect network devices to the UMC domain. In this case, SINEC INS provides a RADIUS server (default port: UDP 1812) and forwards the authentication requests, inbound via the RADIUS server, to the configured UMC server or ring server.

These connections make it possible to implement centralized authentication of configuration access with UMC or Active Directory users.

Configuration access



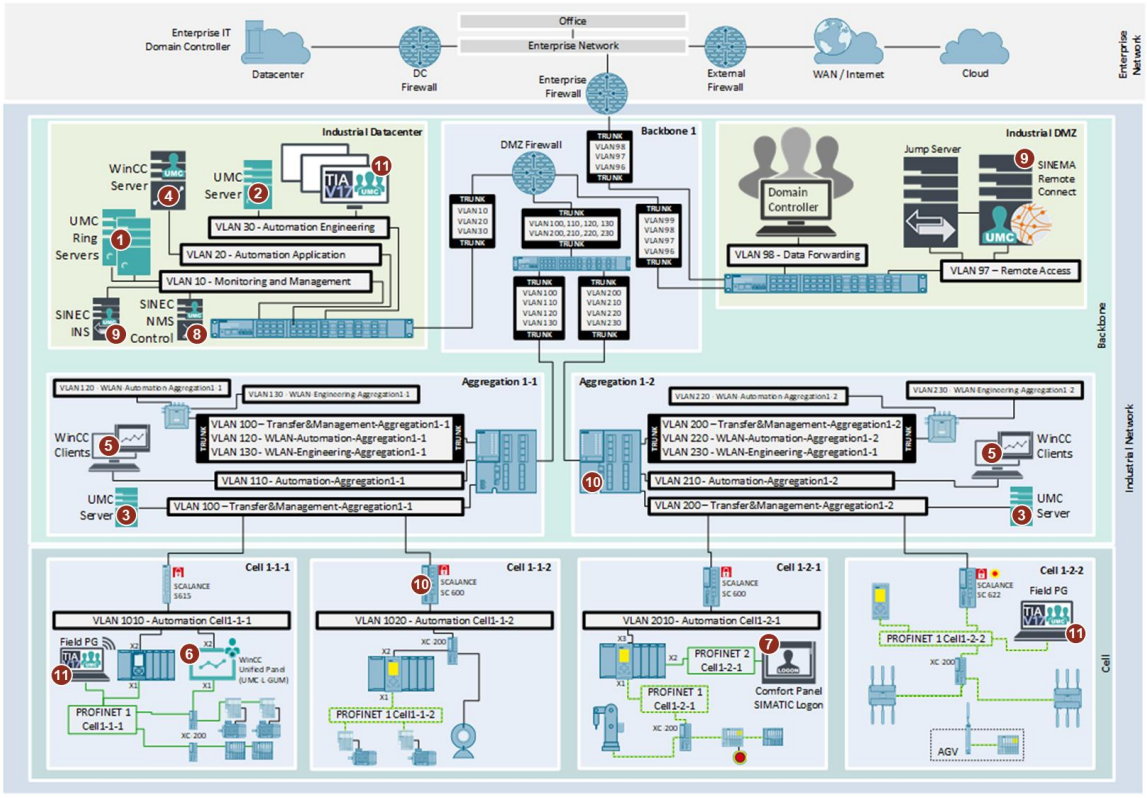
To configure the UMC domain, only the web interface of the ring server is used (default port: TCP 443). Users and/or groups can be imported from the Active Directory in this central location. The configuration is then distributed by the ring server to all other servers.

In case of a redundant design, the engineering station should have access to the virtual as well as physical IP addresses of the servers.

3.6.3 Placement in the network concept

The diagram below shows an example arrangement of the components in the network.

Figure 3-23



1. **UMC ring server in the industrial datacenter**
   A redundant design in the monitoring and management subnet is recommended for the ring servers.

   The PC stations receive the following configuration:

   UMC priority ring server:

   Table 3-20

Parameter	Value
IP address	10.0.10.121/24
Default gateway / DNS/NTP server	10.0.10.1
Computer name	UMCRINGSERVPRI
Active Directory integration	domain: .factory
FQDN	umcringservpri.datacenter.factory (statically defined in SINEC INS or domain controller)

   UMC secondary ring server:

   Table 3-21

Parameter	Value
IP address	10.0.10.122/24
Default gateway / DNS/NTP server	10.0.10.1

Parameter	Value
Computer name	UMCRINGSERVSEC
Active Directory integration	domain: .factory
FQDN	umcringservsec.datacenter.factory (statically defined in SINEC INS or domain controller)

UMC ring server (virtual interface):
The redundant servers are operated in a Microsoft NLB (Network Load Balancing) cluster. This cluster is reachable via a virtual IP address. To ensure reachability with FQDN, a static DNS record should be created in the domain controller. This FQDN is then used for addressing of the redundant UMC ring servers by all other servers and agents.

The following parameters are recommended for cluster IP and FQDN:

Table 3-22

Parameter	Value
Virtual cluster address	10.0.10.120/24
FQDN	umcringserv.datacenter.factory (statically defined in SINEC INS or domain controller)

2. **UMC server in the Automation-Engineering subnet (industrial datacenter)**
It s recommended to host a UMC server for the engineering VMs in the same subnet. Because the connections between UMC server and VMs are then limited to the local subnet, less configuration work is required in the DMZ firewalls.
The following interface configuration is recommended for this server:

Table 3-23

Parameter	Value
IP address	10.0.30.20/24
Default gateway / DNS/NTP server	10.0.30.1
Computer name	UMCSERV
Active Directory integration	Domain:.factory
FQDN	umcserv.datacenter.factory (statically defined in SINEC INS or domain controller)

3. **UMC server in the Transfer&Management-Aggregation subnets**
The UMC server in the Transfer&Management subnets provide authentication services on the aggregation level. Any device located below this level in the cells can use these services. This applies in particular to the HMI Panels in the cells. This way, in the event of a failure in the backbone network, authentication services can still be provided in the individual aggregation networks. The SLRA service is enabled on the corresponding server for aggregation levels containing Comfort Panels.

So that the communication to the cells is not routed through the DMZ firewall, static routes are necessary in the PC stations (see chapter 2.2.6 and subsequent chapters). These routes can be found in the Tables below.

For installing the UMC server, it is recommended to deploy a corresponding application server with a Microsoft Windows operating system in the transfer networks of the aggregation level. Here, for example, a SINEC NMS Operation can be installed in addition to UMC (see chapter 3.2 Network management). Static DNS records in the domain controller or SINEC INS DNS server then facilitate the corresponding FQDN-based addressing of the UMC servers.

The following interface configuration is recommended for the servers:

UMC-Server-Aggregation1-1:
Table 3-24

Parameter	Value
IP address	10.0.100.100/24
Default gateway / DNS/NTP server	10.0.100.1
Static routes	10.1.10.0/24 ➔ 10.0.100.110 10.1.11.0/24 ➔ 10.0.100.110 10.1.20.1/24 ➔ 10.0.100.120 10.1.21.0/24 ➔ 10.0.100.120
Computer name	APPSERVAGGR11
Active Directory integration	domain: .factory
FQDN	umcserv.aggregation11.factory (statically defined in SINEC INS or domain controller)

UMC-Server-Aggregation1-2:
Table 3-25

Parameter	Value
IP address	10.0.200.100/24
Default gateway / DNS/NTP server	10.0.200.1
Static routes	10.2.10.0/24 ➔ 10.0.200.110 10.2.11.0/24 ➔ 10.0.200.110 10.2.12.0/24 ➔ 10.0.200.110 10.2.20.0/24 ➔ 10.0.200.120
Computer name	APPSERVAGGR12
Active Directory integration	domain: .factory
FQDN	umcserv.aggregation12.factory (statically defined in SINEC INS or domain controller)

4. **WinCC server**
   The WinCC server also receives a local UMC server installation. If visualization software is being used which only supports SIMATIC Logon, it is also necessary to enable the SLRA service of the server. The interface configuration of the WinCC server is described in chapter 3.1 – Visualization.

5. **WinCC clients in the Automation-Aggregation subnets**
   User authentication at the WinCC Unified clients in the aggregation level is carried out by the WinCC server in the datacenter.
   If the clients are installed on PCs with a Microsoft Windows operating system, it is recommended to add these PCs to the Active Directory for central management of the operating system accounts.

6. **WinCC Unified Panels**
   The WinCC Unified Panels connect via UMC-L-GUM to the UMC server in the nearest Transfer & management aggregation subnet.
   The interface configuration of these devices is described in chapter 3.1 – Visualization.

7. **WinCC Comfort Panels**

   The Comfort Panels (shown for example in cell 1-2-1) connect via SIMATIC Logon to the SLRA service of the UMC server in the nearest Transfer&Management-Aggregation subnet. The interface configuration of the Panels is described in chapter 3.1 – Visualization.

8. **SINEC NMS**
   A UMC server is a part of the SINEC NMS installation. This server is connected to the ring servers in the datacenter according to the architecture described above.
   The interface configuration is described in chapter 3.3 – Network management.

9. **SINEC INS and SINEMA RC**

   The SINEC INS and SINEMA RC components are connected via HTTPS communication directly to the ring servers in the datacenter. A separate server for caching of users is not available in this context. The interface configurations of these servers are described in the corresponding chapters.

10. **Network components**

    Network components are connected to SINEC INS via the RADIUS protocol for authentication of configuration access. SINEC INS serves as a stand-in to perform authentication at the UMC ring server.

11. **Engineering VMs and Field PGs**
    The engineering systems connect in the UMC runtime server role with the UMC server in the Automation-Engineering subnet.

12. **Microsoft Windows PC systems**
    Central user management of the operating system is performed by the Active Directory as described in chapter 2.6.1.
    The following systems and components utilize the operating system users, and by extension, the Active Directory users:
    - TIA project server
    - TIA Administrator

3.6.4 Configuration of the network components

The following configurations in the network components are necessary to run the engineering solution described above. Appendix III contains a more detailed list of the firewall rules based on the architecture in Figure 3-16.

1. **Configuration of the Microsoft Windows PC stations**
   All PC stations should be added to the Active Directory of the domain controller.
   This is essential for the stations with a UMC server installation. For all other stations (e.g. TIA project server) it offers the advantage of central administration of the operating system's user accounts.

2. **Configuration of the DMZ firewall**
   The following rules are necessary in the DMZ firewall for the operation of the UMC components:

General requirement

- Communication from all PC stations with UMC ring server, UMC server and UMC runtime server to the domain controller for interfacing with the Active Directory (see \4\)

Components in the backbone

- Bidirectional communication between the UMC server in the Automation-Engineering subnet and the ring servers (default port: TCP, 4002)
- Bidirectional communication between the WinCC server and the UMC ring servers (default port: TCP, 4002)
- Bidirectional communication between the SINEC NMS Control and Operation stations and the UMC ring servers (default port: TCP, 443)
- HTTPS communication from SINEC INS to the UMC ring servers (default port: TCP, 443)
- HTTPS communication from the SINEMA Remote Connect server to the UMC ring servers (default port: TCP, 443)
- RADIUS access from all network components in the DMZ (Management-DMZ subnet) to the SINEC INS RADIUS server (default port: UDP, 1812)
- HTTPS configuration access from the engineering VMs to the UMC ring servers (default port: TCP, 443)

Note

In case user permissions need to be configured from the SINEC NMS web server, it is necessary for the engineering PC to receive access (with the appropriate firewall rules) to the web server of the UMC server configured in SINEC NMS.
In this case, SINEC NMS represents the web interface of the UMC server as an HTML inline frame. Thus, in such case a connection is established directly from the engineering station to the UMC server or ring server.

Components in the aggregation level:

- Bidirectional communication between the UMC server in the Transfer&Management-Aggregation subnets and the UMC ring servers in the datacenter (default port: TCP, 4002)
- Bidirectional communication between the Field PGs in the WLAN-Engineering-Aggregation subnets and the UMC server in the Automation-Engineering subnet (default port: TCP, 4002)
- RADIUS access from all network components in the aggregation networks (Transfer&Management-Aggregation subnet) to the SINEC INS RADIUS server (default port: UDP, 1812)
- HTTPS configuration access from the Field PGs in the WLAN-Engineering-Aggregation subnets to the UMC ring servers (default port: TCP, 443)

Components in the cell level:

- Bidirectional communication between the Field PGs in the Automation-Cell subnets and the UMC server in the Automation-Engineering subnet (default port: TCP, 4002)
- RADIUS access from all network components in the cell networks to the SINEC INS RADIUS server (default port: UDP, 1812)

3. Configuration of the cell firewalls

Rules for the following connections are necessary in the cell firewalls:

- Bidirectional communication between the Field PGs in the Automation-Cell subnets and the UMC server in the Automation-Engineering subnet
  (default port: TCP, 4002)
- HTTPS communication from the WinCC Unified Panels to the UMC server in the Transfer&Management-Aggregation subnet (default port: TCP, 443)
- SIMATIC Logon communication from the WinCC Comfort Panels to the UMC server in the Transfer&Management-Aggregation subnet (default port: TCP, 16389)
- RADIUS access from all network components in the cell networks to the SINEC INS RADIUS server (default port: UDP, 1812)

3.7 PROFINET communication

3.7.1 PROFINET – introduction

PROFINET (**Pro**cess **Fi**eld **Net**work) is an open industrial Ethernet standard for automation maintained by the PROFIBUS & PROFINET International (PI) organization (see \33\).

PROFINET uses the Ethernet standard from the IT world in addition to IP-based communication. It supports realtime communication and allows for the integration of other fieldbus systems.

Current information on PROFINET from Siemens can be found in reference \62\.

Advantages of PROFINET

- Open standard for Industrial Ethernet from the organization "PROFIBUS & PROFINET International" (PI)
- Uses Ethernet standard from the IT world
- PROFINET network is open for IP-based protocols from office networks.
- Realtime communication between CPU and decentralized I/O, even redundantly.

Limitations of PROFINET

- I/O communication not possible across router boundaries
- Address assignment not possible across router boundaries
- No integrated security (defense in depth)

Why use Ethernet for a fieldbus?

- Open architecture
- Established and proven standard
- Easy to connect with the existing enterprise network

PROFINET fundamentals

The sections below will provide you with the most important definitions, terms and features surrounding PROFINET. Additional information on the PROFINET protocol can be found in the PROFINET system manual \12\ or from PI \33\.

Device classes

The standard distinguishes between four different device classes in a PROFINET network:

- I/O supervisor: SCADA, engineering station
- I/O controller: CPU
- I/O device: distributed I/O system, field devices
- I-Device: "intelligent" I/O devices (e.g. CPU with I-Device functionality)

Conformity classes (CC)

PROFINET devices are divided into 3 successively more stringent conformity classes that correspond to the certification grade and functionality of the device in question. These CCs make it quick and easy to see the feature set of a device.

A precise description of the conformity classes can be obtained from the PI: \34\.

Figure 3-24

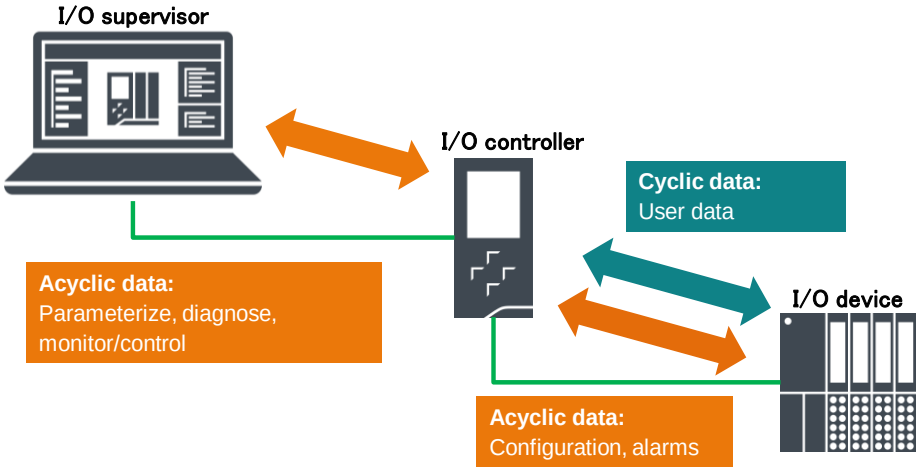
	Class A (CC-A)	Class B (CC-B)	Class C (CC-C)
Basic functions (*=optional)	▪ Cyclic RT comms ▪ Acyclic TCP/IP comms ▪ Parameters ▪ Alarms ▪ Topology info Data transfer cycle ▪ Auto address resolution ▪ Neighborhood detection ▪ Priority data traffic	▪ IT compatible switches ▪ Network diagnostics (SNMP) ▪ Media redundancy (MRP) * ▪ Auto addressing * ▪ Config change during operation *	▪ Reserved bandwidth (IRT comms) ▪ Switches with bus & time sync ▪ Bumpless media redundancy (MRPD) * ▪ Clock synchronicity *
Typical use	▪ Production technology ▪ Building automation	▪ Automation plants	▪ Motion Control ▪ Precise reactions

Types of data transmission

PROFINET uses 2 types of data transmission:

- Cyclic communication:
  prioritized, deterministic data transmission for time-critical applications
- Acyclic communication:
  Parameter assignment, diagnostics, monitoring/control with I/O controllers
  Configuration, alarm handling for I/O devices

Figure 3-25



Cyclic communication

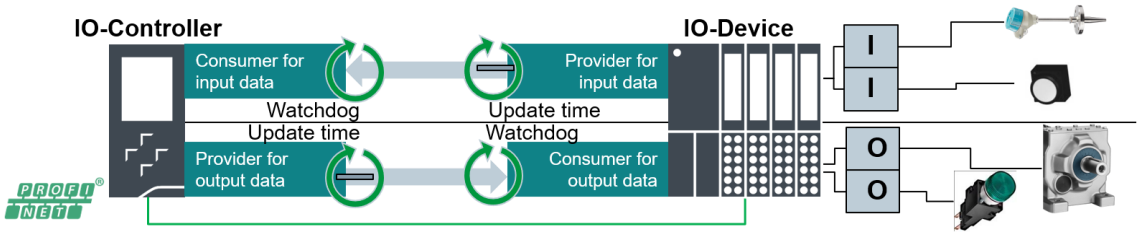
For cyclic data exchange between I/O controller and I/O device, the following 3 conditions must be defined:

- **Update time:**
  Time interval in which the I/O controller and I/O device exchange data. It can be individually configured for each I/O device.
- **Send clock**:
  The smallest possible interval that can be used for the update time. It is set in the I/O controller and therefore applies to all I/O devices assigned in the I/O system.
- **Response watchdog time**:
  The time interval in which I/O controller or I/O device will accept having received no I/O data from the other side. The response watchdog time is a whole number multiple of the update time and can be configured individually for each I/O device.

PROFINET uses the provider/consumer model for cyclic data exchange:

- The provider sends I/O data on a cyclic basis (depending on the update time) without needing an explicit request.
- The consumer receives I/O data without confirmation and monitors the cycle of inbound data with a response watchdog time.
- The controller and the device function simultaneously as provider and consumer (even if there are no user data to transmit).

Figure 3-26



Each I/O device works on its own cycle. As such, I/O devices can have different update times (e.g. ET 200SP 1 ms; HMI 128 ms). Each device sends data on a cyclic basis independently of the others. Because the Ethernet network is fully duplexed, it is possible for it to receive and send at the same time.

What is realtime capability?

Industrial communication, especially in the production automation, requires precise and deterministic data transmission.

This is why, for the cyclic exchange of time-critical I/O user data, PROFINET I/O does not use TCP but instead uses realtime communication (RT) or isochronous realtime communication (IRT) for synchronized data exchange in reserved time intervals.

This deterministic data transmission gives PROFINET the ability to respond to an electrical signal within a specified time span, the response watchdog time. A violation of this response time is treated as an error that can be addressed on a user- or application-specific basis.

The ability to react within the defined time span and the specific error response constitute realtime capability.

How fast is realtime?

The realtime requirements on a system depend on the process that needs to be controlled. The requirements range from multiple seconds in building climate control to a few milliseconds in materials handling.

Realtime with PROFINET

PROFINET I/O is a scalable realtime communication system based on the layer-2 protocol for Fast Ethernet. The RT transmission procedure for time-critical process data and IRT for highly precise and isochronous processes give you 2 performance classes with realtime support:

The RT and IRT transmission methods are standardized in the IEC 61158 international standard.

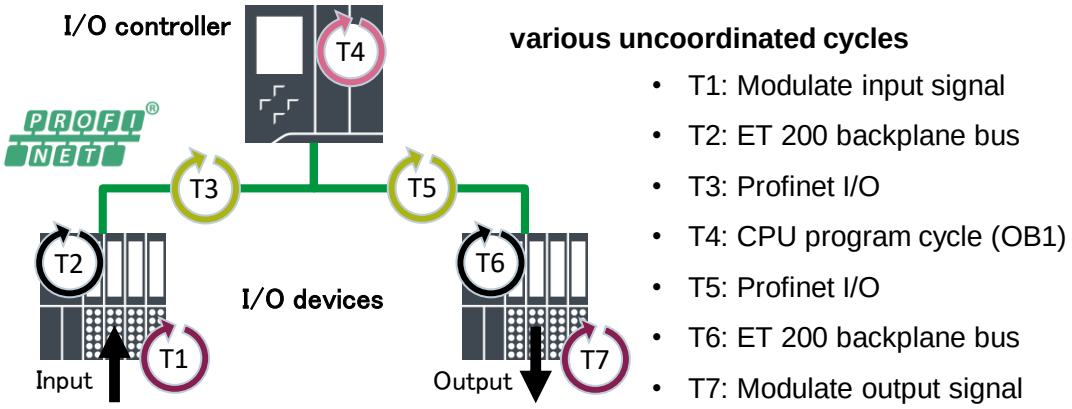
Realtime communication (RT)

PROFINET RT is the standard solution for integrating distributed I/O systems. RT likewise relies on standard Ethernet in devices and commercially available industrial switches as infrastructure components. Special hardware support is not required.

PROFINET I/O telegrams are prioritized over standard telegrams using a VLAN tag according to IEEE802.1Q. This ensures the determinism required in automation engineering. In this method, data are transmitted via prioritized Ethernet telegrams (VLAN 0 priority 6).

In PROFINET RT there is no synchronization between the various cycles required for signal processing and signal forwarding. This yields a best-case terminal-to-terminal response time equal to the sum of all cycles. The worst-case figure is double this time.

Figure 3-27



Isochronous realtime communication (IRT)

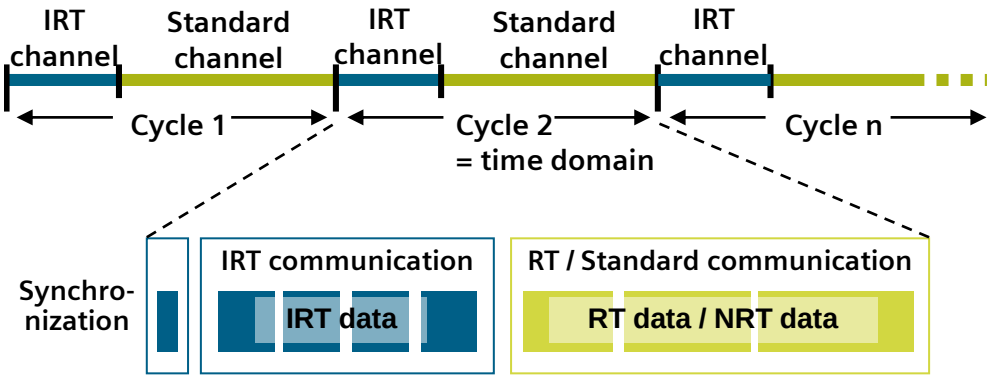
In comparison to RT, IRT is a synchronized transmission method for the cyclic exchange of IRT data between PROFINET devices. A reserved bandwidth within the send clock is available for the IRT data. This guarantees that IRT data can be transmitted without interference at reserved, synchronized intervals even when network load is high (for example, due to TCP/IP communication or other realtime communication).

Special hardware is required for IRT and the functions that rely on it. A topology with the appropriate project engineering is also required.

A prerequisite for IRT communication is that the I/O controller and the I/O devices of the PROFINET sync domain must have a common time basis. For this purpose, a sync master (for example, the I/O controller) dictates the cycle on the basis of which all sync slaves (for example, the I/O devices) will synchronize among themselves. A bandwidth for IRT communication is reserved within this sync domain. RT and NRT data are exchanged outside of this reserved bandwidth.

In addition to the reserved bandwidth, the telegrams are exchanged on defined transmission paths to further optimize data traffic. For this, the topological information from the configuration is used for planning the communication. Transmission and reception points of each individual data telegram at every communication node are thus guaranteed. This enables you to achieve optimal usage of the bandwidth and obtain the best possible performance from the PROFINET I/O system.

Figure 3-28



There are various IRT-based functions that can be used for specific applications along with the devices designed for these applications. More information on IRT can be found in the PROFINET system manual: \12\.

Isochronous mode

The IRT-based isochronous mode function adds an OB to the CPU that is synced up to the synchronized PROFINET cycles. The processing of the I/O data is coordinated here with the PROFINET cycle, granting greater precision and speed. These properties are often required for Motion Control or metrology applications, for example.

More information can be found in the manual on S7-1500 Isochronous Mode: \36\.

Oversampling

The IRT-based oversampling function divides the PROFINET cycle in the module into multiple sampling cycles. The values of the sampling cycles are collected in the module and sent to the I/O controller in the next PROFINET cycle. By dividing the PN cycle into smaller sub-cycles, oversampling allows for extremely accurate recording of measurements and very precise controls.

More information can be found in the application example on oversampling: \37\.

Time-based I/O

The time-based I/O function uses special modules to record signals with a time stamp and, based on this time stamp, to generate highly precise signals.

This function makes it possible to generate ultraprecise signals with no jitter.

More information can be found in the manual on time-based I/O: \38\.

Acyclic data transmission

In addition to cyclic communication, PROFINET also has acyclic communication that is used for non-repeating events.

With PROFINET, these events mainly represent data for diagnostics, parameter assignment, configuration and monitoring.

A distinction is made between data record communication and alarms. Both types of acyclic communication are based on UDP, making them capable of routing.

Data record communication

Data record communication is used by various participants for different purposes.

- **Configuration and parameter assignment:**
  When establishing a connection between an I/O controller and I/O devices, settings parameters are transmitted via data record communication.
- **Diagnostics and identification:**
  With I/O supervisors, tools and I/O controllers, diagnostics/identification information is read acyclically according to "Identification and Maintenance (I&M) Functions".
- **Controller-to-controller communication:**
  With I/O controllers, larger volumes of data are transmitted using the I-Device functionality.

Alarms

In an automation process, events are transmitted as alarms. These must be acknowledged by the user program. A distinction is drawn between various alarm types:

- **Process alarms** notify the I/O controller of an event in the process so that the I/O controller can execute a defined response to it in the user program.
- **Diagnostic alarms** indicate a malfunction of a field device.
- **Maintenance alarms** indicate an impending device failure.

In addition to these alarms, there are also manufacturer-specific alarms that can be used for specific diagnoses of an I/O device, for example.

3.7.2 Requirements for the network concept

While PROFINET networks in the traditional sense are found on the field level, the requirements for OT-IT integration in state-of-the-art networks dictate that they be able to communicate more and more openly with enterprise networks. With standard Ethernet-based communication, PROFINET is able to provide all the necessary tools for these demands. This chapter will present the essential requirements of PROFINET networks.

Topologies in PROFINET networks

Using the Ethernet standard allows PROFINET to offer a wide variety of network design possibilities. Most common network structures are thus possible, offering a great degree of flexibility for the cells.

The following parameters must be observed in the network architecture:

- Topology options: Linear, star, ring, tree, wireless (also in combination)
- Maximum number of nodes:

  - Nodes per network:
    unlimited (only limited by the maximum bandwidth of the network, 100 Mbit/s for PROFINET)
  - I/O devices per I/O controller:
    depends on the I/O controller and the interface used (e.g. technical specs of the S7-1516 X1: 256 I/O devices; X2: 32 I/O devices)
- Unlimited addressing via PN names (max 240 characters)

Redundant networks

Ring structures that facilitate fault-tolerant networks using the MRP and MPRD media redundancy protocols require special hardware. Devices in class CC-B (switch with at least two ports) can support the MRP functionality as an option. In such networks, all devices that do not support MRP must be connected to the ring via a stub.

Note

SIMATIC CPUs do not support RSTP. Relevant frames are passed through, allowing a CPU to be operated in an RSTP network. However, if a path directly to the CPU fails, the path will be deactivated.

A network meshed with RSTP is therefore **not recommended** within a cell.

Networks with hard realtime requirements

While the topology for RT communication can be chosen almost without limitation, IRT communication requires that I/O devices be connected together in linear structures. Such linear structures must not be interrupted by unsynchronized devices such as RT I/O devices or IRT devices assigned in a different context. IRT networks can nevertheless be structured using IRT-capable switches (e.g. SCALANCE X200 IRT, ports of the X1 interface of the S7-1500). In this case, IRT-capable switches help form the logical structure of the network. The ports of the X1 interface can also be used for load distribution.

Note

Especially with a larger number of IRT I/O devices with a rapid update time, the engineer should consider spreading the devices across both ports of the S7-1500 IRT PROFINET X1 interface in order to reduce the network and port load from each of the strings.

The FAQ "Which IO controllers and IO devices support the following functions in STEP 7 (TIA Portal)..." (\7\) provides an overview of which devices support the MRP and MRPD media redundancy protocols, for example, or IRT.

Network and port load distribution with PROFINET

Especially in modern networks that need to meet the requirements of digitalization, utilization of the available bandwidth plays an increasingly important role.

To ensure error-free data transmission over PROFINET and other protocols, it is recommended to check the load on the network during the network's design phase and design it accordingly.

The bandwidth used and the port load are the primary factors in this. The main sources of network load in the cell are typically the cyclic realtime communication between PROFINET nodes (RT) and acyclic, so-called "non-realtime communication" (NRT) that includes, for example, OPC UA communication and IP camera live transmissions.

When structuring network load in the cell network, many factors play a role:

- Form of the network topology (linear, star, ring)
- Line depth between source and target interface
- Type of forwarding in the switches (cut-through, store&forward)
- Number of PROFINET nodes in the same network
- Update time of the PROFINET nodes

Note Diagnostics and parameter assignment likewise require free bandwidth in the cell. Therefore, enough buffer should be ensured when planning the network load.

To prevent overload in the network and ports and thereby prevent packet loss, the network load and port load must be verified before commissioning.

TIA Portal will calculate the network load for the configured PROFINET nodes automatically based on the topology, update time and the type of communication (RT or IRT). If PROFINET nodes are configured with the "Automatically calculate update time" function, the update time will be adjusted based on the parameters listed above. TIA Portal will thus make sure that the network load caused by PROFINET is within acceptable limits.

TIA Portal cannot calculate NRT communication because this is acyclic communication that is used in a manner specific to each user program.

Therefore, it is recommended to use SINETPLAN design program (\39\) to perform advance planning of networks with a higher level of communication traffic from RT and NRT.

Additional details on the PROFINET line depth and load calculation are provided by the PROFINET installation guidelines from PI: \35\.

Topology requirement of the PROFINET services

PROFINET uses protocols for various services which, due to the characteristics of these protocols, entail varying requirements for the network.

The following protocols are used by the respective PROFINET services in the classes CC-A, CC-B and CC-C:

- Connection setup (IOC to IOD): IP, ARP, DCP, UDP, ICMP
- Connection handling (e.g. PROFINET data records): DCE/RPC
- PROFINET data records: UDP
- I/O communication: RT, IRT
- Redundancy: MRP, MRPD
- Diagnostics: SNMP
- Topology: LLDP

Important protocols for cyclic data exchange and connection setup between I/O controller and I/O device require a **flat switched network structure** based on OSI layer 2 without any interruptions from routers.

These protocols include: **DCP**, **ARP**, **RT**, **IRT**, **MRP**, **MRPD** and **LLDP.**

An example of a typical application here is PROFINET name assignment, which is based on the DCP protocol and which can therefore only occur within a switched network. In the same vein, cyclic PROFINET I/O communication via RT and IRT is not possible across routers.

Unlike the protocols listed directly above, the protocols used for diagnostics and PROFINET data records can also be used **in routed networks**. These protocols include: **DCE/RPC**, **UDP** and **SNMP.**

This guarantees, for example, that diagnostics based on these protocols can be performed even on engineering stations that are located behind routers.

S7-1500-specific interface properties

This chapter will address the CPU-specific properties with regard to PROFINET. S7-1500 CPUs have up to three integrated Industrial Ethernet interfaces.

The X1 and X2 interfaces support PROFINET. While the X1, as the dedicated PROFINET interface, supports the larger quantity structure and therefore RT as well as IRT, the X2 supports RT and a smaller quantity structure.

The X3 interface offers transmission speeds of up to 1 Gbit/s, making it especially suitable for linking to higher-level networks.

A detailed description of the feature set of each interface is listed in the technical specifications of each S7-1500.

To add more Industrial Ethernet interfaces and functions to smaller CPUs, the S7-1500 portfolio has so-called communications processors (CPs) and communications modules (CMs). CPs add additional Ethernet interfaces to the CPU with supplemental functions (e.g. security), while CMs add another interface with PROFINET functionality.

The following overview shows which functions are supported by which integrated interface (X1, X2, X3) and by the CM 1542-1:

Figure 3-29

S7-1500 Interfaces	**X1**	**X2** ≥ S7-1515	**X3** S7-1518	**CM 1542-1**
PROFINET	✓	✓	✗	✓
IRT with isochronous mode	✓	✗	✗	✗
Media redundancy	✓	✗	✗	✓
Transmission speed	**100 Mbit/s**	**100 Mbit/s**	**1 Gbit/s**	**100 Mbit/s**

PROFINET requirements for switches

PROFINET relies standard Ethernet in devices and commercially available industrial switches as infrastructure components. Special hardware support is not required.

Even so, PROFINET telegrams are prioritized over standard telegrams by way of a VLAN tag in accordance with IEEE802.1Q to guarantee the determinism required in automation engineering.

In this method, data are transmitted via prioritized Ethernet telegrams (VLAN 0 priority 6).

Switches in PROFINET-relevant network segments, such as the cell, should therefore have a PI certification so that prioritized data transfer can be guaranteed.

The FAQ "Segmenting a Network Using VLANs" (\8\) describes necessary considerations when configuring VLAN switches in a PROFINET RT network.

Note If the switch you are using meets conformity class CC-A, prioritization with VLAN tags is assured. All Siemens SCALANCE switches meet at least the requirements of CC-A.

Realtime communication across cell boundaries

Some cells must exchange data with each other in realtime, for example to transmit handshakes, material handoffs or other safety-related emergency stop signals to other cells.

There are two methods of implementing this realtime communication across cell boundaries:

- **I-Device:**
  A function whereby an I/O controller functions as an I/O device for up to four higher-level I/O controllers. It can be configured either at the integrated X1 and X2 interfaces or on the PROFINET CM 1542-1.
- **PN/PN coupler:**
  An additional device with two separate interfaces that can be assigned as an I/O device to as many as four I/O controllers. At the I/O device, the data are copied to the other side, where they are once again available to I/O controllers in the role of an I/O device.

Chapter 3.9 - M2M communication - contains detailed explanations of realtime communication across cell boundaries.

Wireless networks with industrial WLAN

In PROFINET networks, it is possible to connect devices over WLAN. When doing so, the following PROFINET-related points should be considered in contrast to wired networks:

- The available bandwidth is lower.
- Packet loss is more likely.
  - Roaming of a client across multiple access points requires a certain handover time (e.g. in AGV applications).
  - To use industrial WLAN for PROFINET, suitable signal coverage of the area must be ensured.
- Handover times for standard WLAN are on the order of hundreds of ms. Moreover, collisions limit the maximum number of nodes that can connect.

Deterministic industrial WLAN extension – iPCF and iPCF-MC

To better adapt industrial WLAN to the requirements of PROFINET, the standard has been expanded to include iPCF (industrial Point Coordination Function) and iPCF-MC (iPCF Management Control).

These extensions enable quicker handover times under 100 ms. Clients are also queried deterministically, resulting in fewer collisions.

Additional details on WLAN are explained in chapter 3.13 – WLAN.

The points explained above mean that special attention must be paid to the following parameters during design and configuration:

- Update time
- Response watchdog time
- Number of nodes

Detailed information and recommendations for designing WLAN networks are presented in application example \32\.

3.7.3 Implementation of the requirements for the network concept

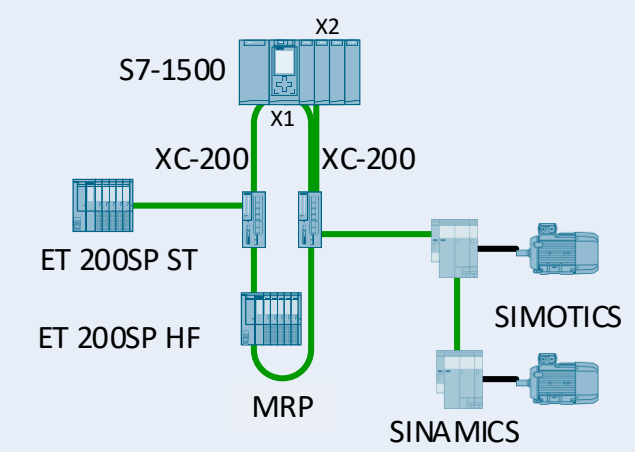
The chapter below aims to describe the implementation of the PROFINET requirements for the network concept, particularly with regard to the cells. Each requirement will be treated using examples of the cells from chapter 2.3 - Network structure in the cell level.

Topologies in PROFINET networks – redundant networks

We will examine first the implementation of the topology requirements of the PROFINET network.

The emphasis of Cell 1 in the PROFINET network is on high availability of the nodes.

Figure 3-30



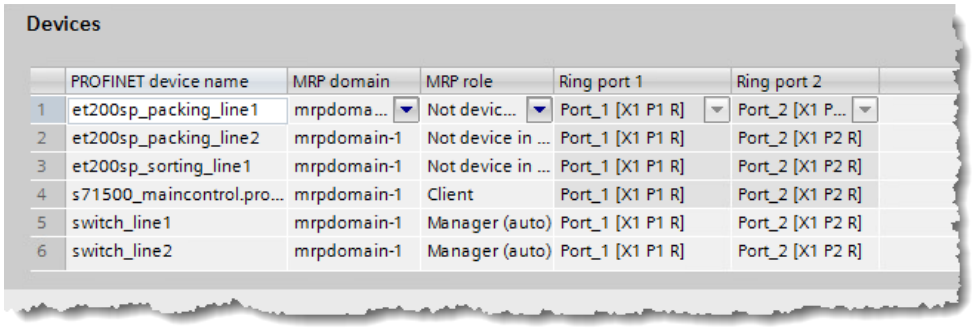
To meet the requirements for high availability, an MRP ring is placed between the I/O controller and the switches. Additional PROFINET nodes are connected via stubs to the switches in the MRP ring. These nodes do not need to support the MRP functionality and can thus be configured as "not participants in the ring" while still benefiting from the increased availability of the network in general.

The SCALANCE XC200 switches employed here meet PROFINET CC-B and the optional MRP functionality.

Note It is also possible to use devices from different manufacturers within a single MRP ring. All devices must support the MRP protocol per IEC 62439.

A switch in the MRP ring is configured as the MRP manager. Siemens MRP-capable devices that support the MRP Manager functionality can also be configured as "MRP Manager (Auto)", which will instruct the network to decide for itself which device will act as the manager.

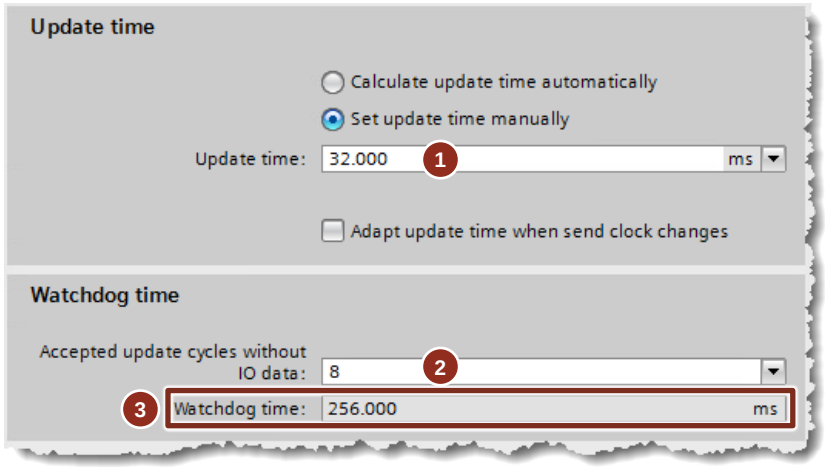
Figure 3-31



With fault-tolerant networks of this kind, MRP guarantees a reconfiguration time of under 200 ms. Due to this reconfiguration time, the watchdog time of the PROFINET RT I/O devices must be set higher than 200 ms. To achieve this, the update time of the I/O device or the number of cycles without PN I/O traffic can be increased. This way, should a network fault occur, the network will function without an error message or failure of communication. The higher-level application must nevertheless be able to handle the programmed watchdog time without any new user data.

In the Figure below, the watchdog time of more than 200 ms is achieved with a combination of an increased update time (suitable for the application) (1) and an increase in the accepted cycles without I/O data (2). The watchdog time achieved in this way (3) is now longer than the maximum expected reconfiguration time, meaning that this I/O device can be operated in an MRP-redundant network without a failure.

Figure 3-32



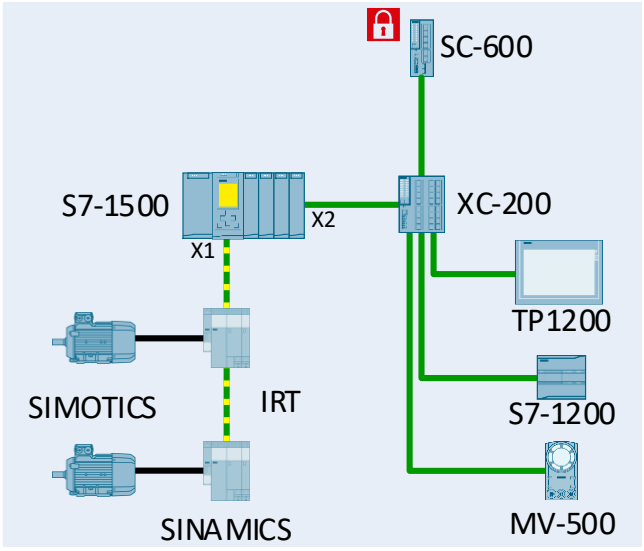
In general, all free ports of the switches in the MRP ring can be used as the starting point of a separate star-shaped network, thereby keeping the line depth as low as possible. In this case, the switch is considered the "single point of failure" for all downstream devices.

More information on the MRP function can be found in the manual "SIMATIC PROFINET PROFINET with STEP 7" (\12\) and in the application example "Configuration of a Ring Topology Based on MRP" (\13\).

Topologies in PROFINET networks – networks with strict realtime requirements

With a Motion application, the PROFINET-side focus of this cell is on strict realtime requirements – and with regard to failsafe operation as well.

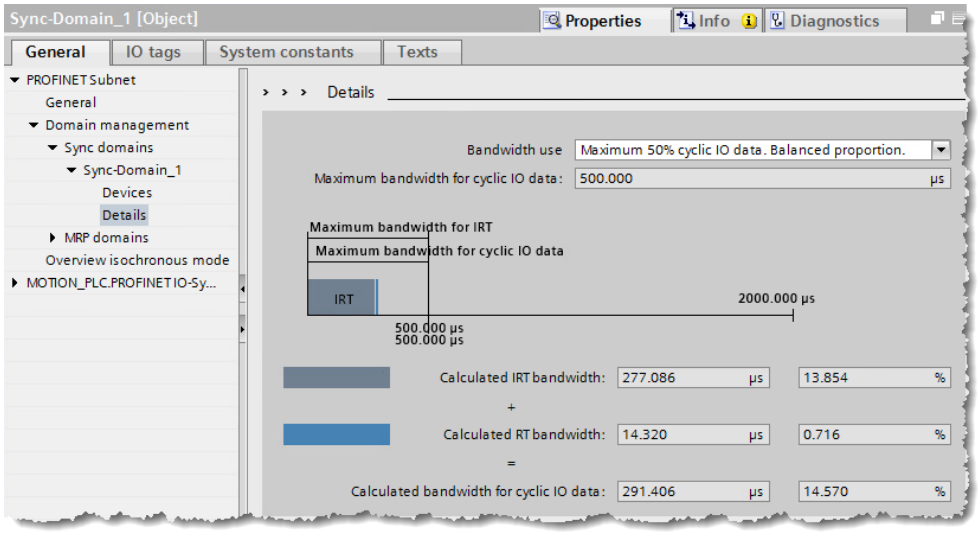
Figure 3-33



Motion applications using PROFINET IRT require a linear topology. It runs on the IRT-capable X1 interface of the S7-1500. The topology in TIA Portal must be identical to the actual setup. If the actual structure differs from the engineered topology, the application will not work and a corresponding entry will be created in the diagnostic buffer. No RT nodes may be connected inside of the IRT linear topology.

A large number of IRT nodes with a fast update time and large data volumes may already use a large proportion of the bandwidth reserved for PROFINET by the X1 interface of the S7-1500. TIA Portal will automatically calculate how much of this bandwidth is currently used for RT and IRT data. When using IRT, this figure can be read from the Properties of the sync domain.

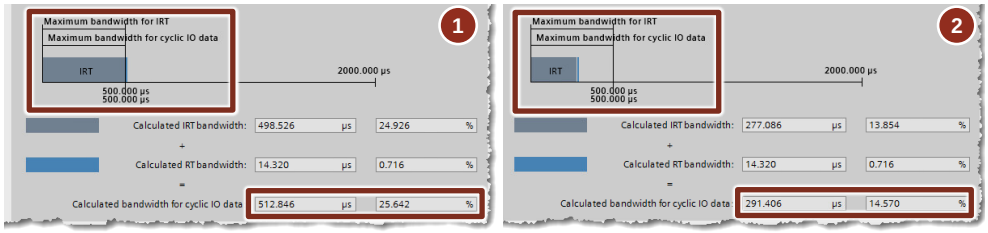
Figure 3-34



To counteract a major bandwidth load on one of the ports, the IRT nodes can be split across the ports X1-P1 and X1-P2.

The figure below shows the difference in the calculated bandwidth between 2 topological methods. On the left (1), all nodes are connected topologically with X1-P1, while on the right (2) the nodes are equally distributed across X1-P1 and X1-P2.

Figure 3-35



A considerable reduction can be seen in the bandwidth calculated for cyclic data exchange. This example shows that network load can be reduced significantly by a prudent choice of topology and distribution of the devices.

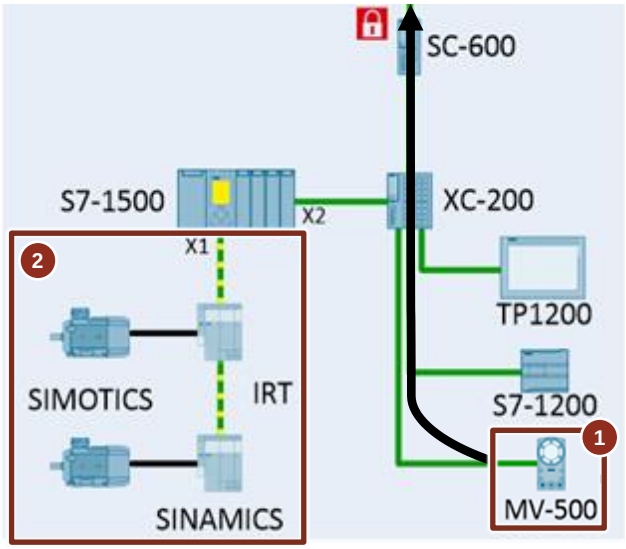
Besides splitting the load across the two-port switch of the X1 interface of the S7-1500 CPU, the IRT-capable switch even makes it possible to design the IRT network – which actually needs to be configured in a rigid linear topology – more freely with a star topology. When doing so, remember that each IRT switch you are using is also considered an IRT device and will therefore reduce the maximum number of IRT I/O devices in the network.

Topologies in PROFINET networks – Network and port load distribution with PROFINET

The topology in the example cells is designed to minimize the network load in the PROFINET network. This prevents packet loss.

This cell's IP camera (1), which usually generates a large volume of data and sends it to other systems, is not integrated in the PROFINET network (2) directly but is instead connected via the X2 interface of the S7-1500. As a consequence, the increased network load from the camera is not routed through the PROFINET network with its high realtime requirements. The camera can thus send data to higher-level systems for analysis without affecting the realtime applications.

Figure 3-36

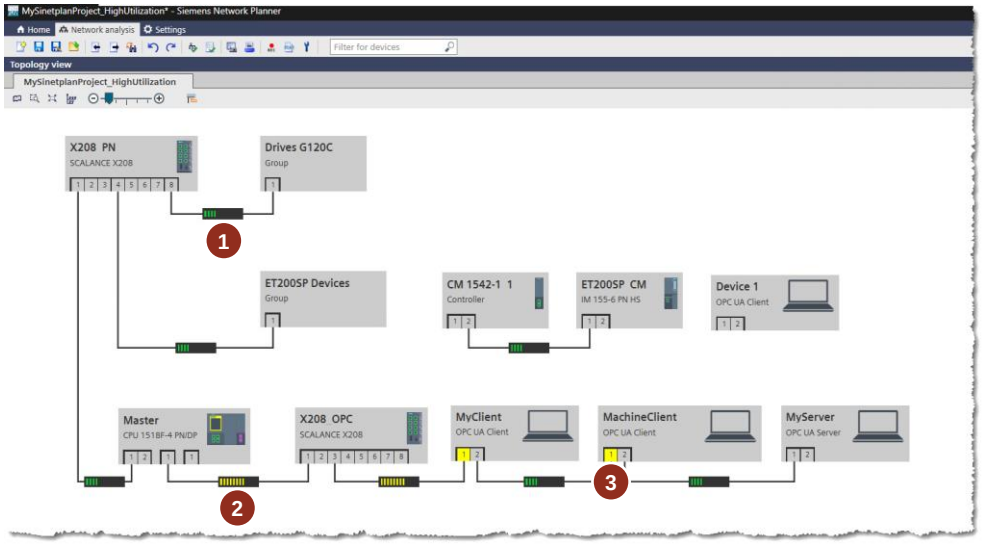


With respect to line depth, the number of PROFINET nodes and the update times of these nodes in the PROFINET network, the network concept adheres to the recommendations of the PROFINET installation guidelines from PI: \35\.

The SINETPLAN tool (\39\) is recommended for a closer look at network and port load.

The example below shows an excerpt from SINETPLAN along with some of the things that can be ascertained from the tool.

Figure 3-37.



1. Green bar: Calculated bandwidth is under the configured limit.
2. Yellow bar: Calculated bandwidth is over the configured bandwidth warning threshold.
3. Yellow port: The port load is over the configured warning threshold. If the port is not colored, the port load is below this threshold.

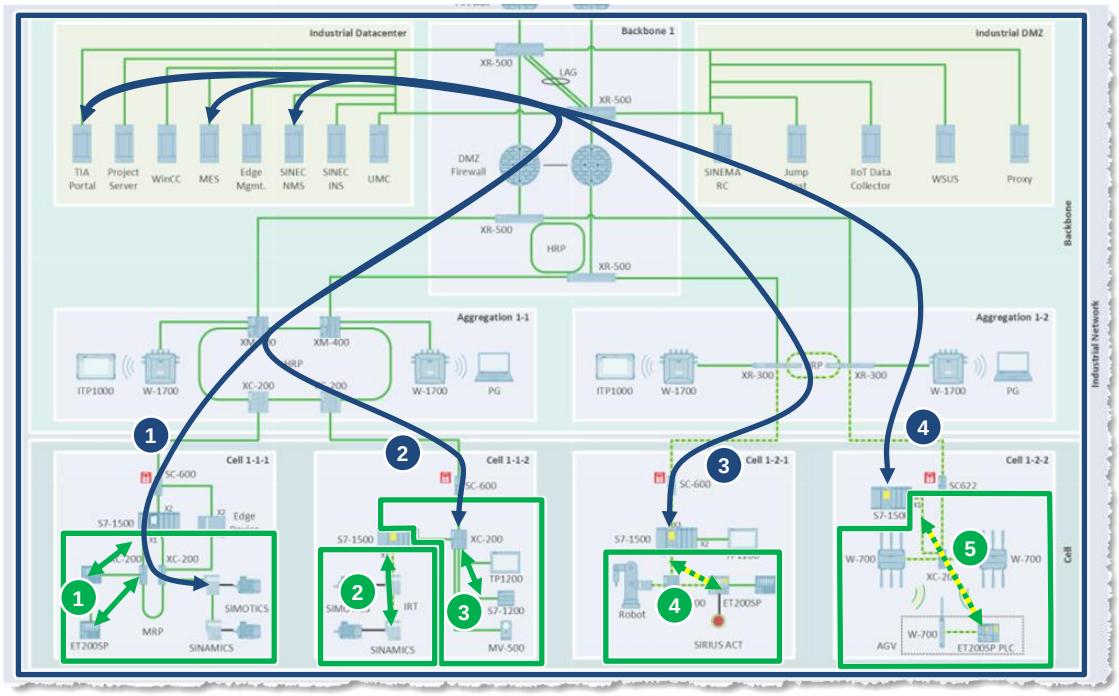
Topology requirement of the PROFINET services

As described in chapter 3.7.2 – "Requirements for the network concept", PROFINET services place different requirements on the network.

This section describes where and which services can be used with the PROFINET nodes in the cells. An excerpt from the master overview diagram of the network concept will serve as a basis for this exercise.

The excerpt is divided into two regions. The first are green areas where OSI layer-2 services can be used. These areas therefore require a flat switched network structure without interruptions from routers. The others are blue areas where services can be used which permit use across router boundaries. The blue region requires routes and firewall rules as described from chapter 2.2.6 "Routing" and chapter 3.3 onward.

Figure 3-38



Access using PROFINET services from higher-level networks (blue numbers)

1. Diagnostics and PROFINET device download utilizing S7 protocol, SNMP and PROFINET data records.
2. Access to the web server of a switch, for example to use the DCP functionality of the switch.
3. Access to diagnostics of an I/O controller.
4. Access from SINEC NMS to PROFINET diagnostics of an I/O controller.

PROFINET access from the flat layer-2 network (green numbers)

1. RT communication between I/O controller and I/O device (ET 200SP)
2. IRT communication between I/O controller and I/O device (drive)
3. DCP name assignment via the WBM of the switch
4. RT and PROFIsafe communication with an I/O device
5. RT and PROFIsafe communication with an I-Device (also via WLAN)

S7-1500-specific interface properties

Thanks to their respective strengths, this network concept uses the interface of the S7-1500 primarily for the following applications:

- X1 interface
  - Main interface for connecting to PROFINET I/O devices (RT, IRT)
  - Integrated 2-port switch for greater topological flexibility (e.g. media redundancy, splitting of IRT devices across 2 lines)
- X2 interface (only on S7-1515 and higher)
  - Network isolation
  - Connection of additional PROFINET I/O devices (RT)
  - Connection to higher-level networks

- X3 interface (only on S7-1518)
  - Network isolation
  - Connection to higher-level networks
  - Requirements of PROFINET communication for switches

For details on how interfaces can be used, please refer to chapter 2.3 "Network structure in the cell level".

3.8 Safety-related communication

3.8.1 PROFIsafe – Introduction

Definitions

PROFIsafe offers the capability of functionally safe communication on the basis of PROFIBUS and PROFINET.

The PROFIsafe protocol, standardized in the international IEC 61784-3-3 standard, can be utilized for safety-related applications up to a Safety Integrity Level SIL 3 according to IEC 61508/IE 62061 or Performance Level PL "e"/category 4 according to ISO 13849.

PROFIsafe uses the so-called "black channel" principle to achieve this. Safety messages are transmitted over the same medium (bus cable) together with the standard messages. This has no effect on the PROFIBUS/PROFINET network or the standard bus protocols. The approach is to ensure maximum possible independence from the transmission channel, regardless of whether it is a copper cable, fiber-optic cable, backplane bus or wireless communication. Transmission rates and the error identifiers implemented in the standard protocol have **no effect**.

Requirements for safety-related communication

PROFIsafe thus offers a safety communication capability **without** additional validation of the specific bus system in accordance with IEC 61508. This is a major advantage for the user because the otherwise laborious safety assessment of the bus system and all the components is no longer necessary. A fresh validation also does not need to be performed when there are changes (e.g. firmware updates) to network components or additions in the network.

For failsafe communication between two partners, the following must be guaranteed:

- Data integrity (data are current and correct)
- Authenticity (correct recipient)
- Prompt transmission (timeliness)

PROFIsafe uses the following four safety mechanisms to secure against possible transmission errors (e.g. loss, repetition, delay, incorrect order):

- Monitoring Number
- Timeout with receipt
- Unique identification (codename)
- Data integrity verification (CRC)

Figure 3-39

Measure: / Error:	Monitoring Number (sign of life)	Time-out (with receipt)	Data Consis-tency Check (CRC)	Codename (for sender and receiver)
Data corruption			X	
Unintended repetition		X		
Incorrect sequence	X			
Loss	X	X		
Unacceptable delay		X		
Insertion	X			X
Masquerade (standard message mimics failsafe)			X	
Incorrect adressing	X			X
Out-of-sequence	X			
Loopback of messages	X			

The codename is also generally referred to as the PROFIsafe address. It serves to uniquely identify the origin and destination. Every F I/O therefore has two address parts (F origin address and F destination address), of which one or both address parts are used for backup. A distinction is made based on:

- **PROFIsafe address type 1**
  The uniqueness of the PROFIsafe address is only ensured by the F destination address. The F origin address has no effect on the uniqueness of the PROFIsafe address. The F destination address must therefore be unique CPU-wide and network-wide. It must be checked for uniqueness in the safety printout.
- **PROFIsafe address type 2**
  The uniqueness of the PROFIsafe address is ensured by combining the F origin address and the F destination address. The PROFIsafe address must be unique CPU-wide and network-wide.

Note

"Network-wide" here means running across subnet boundaries. With PROFIBUS, a network includes all nodes that are reachable via PROFIBUS DP. With PROFINET I/O, a network includes all nodes reachable via RT_Class_1/2/3 (Ethernet / WLAN / Bluetooth, layer 2) and, as the case may be, RT_Class_UDP (IP, layer 3) \18\.

3.8.2 Requirements for the network concept

In larger networks, it is often not possible to guarantee the uniqueness of PROFIsafe addresses with organizational measures. In these cases, measures for failsafe network isolation are required.

Suitable measures in the sense of the IEC 61784-3-3 PROFIsafe specification are (2-port) routers that represent a natural network boundary for layer 2. This applies to networks in which RT_CLASS_UDP is not permitted or not supported. The 2-port router ensures that no PROFIsafe telegrams can find their way into other networks.

The SCALANCE SC622-2C router meets these requirements of the PROFIsafe specification and can therefore be used for the cell security concept as shown in Figure 3-40. In addition, networks can be safely isolated by means of a PN/PN coupler or with separate X1/X2 interfaces of failsafe S7 CPUs. Additional information and options are described in greater detail in the FAQ article 109740240: \21\.

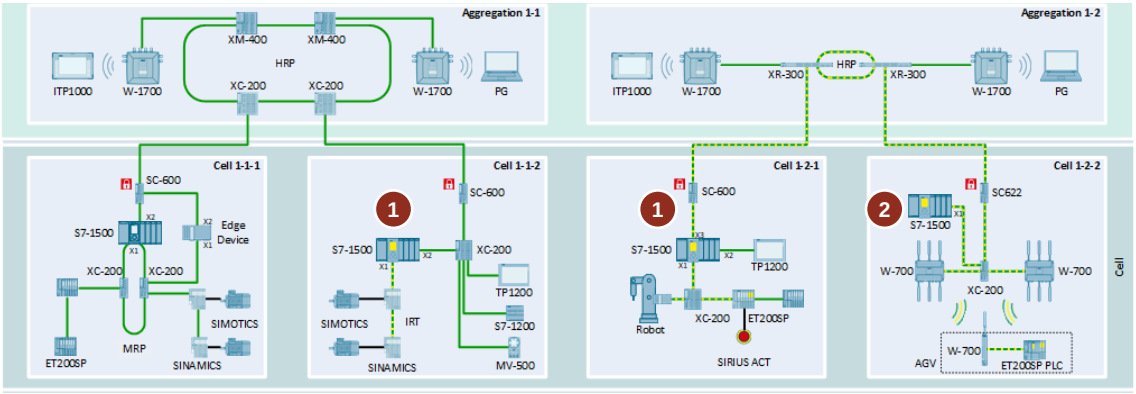
Even with multiple separate network controllers, IPCs do not represent network isolators from the perspective of the PROFIsafe specification. Therefore they cannot be used for failsafe isolation.

3.8.3 Implementation of the requirements for the network concept

In Figure 3-40 you will see various options for failsafe isolation of cells from one another.

1. While the isolation in cells "Cell 1-1-2" and "Cell 1-2-1" is provided by the separate X1/X2 or X1/X3 interfaces of the CPU,
2. in cell "1-2-2" the isolation is implemented with the help of a SCALANCE SC622-2C router. The CPU and the SCALANCE SC622-2C, respectively, ensure that no layer-2 telegrams are transmitted to other networks. Accordingly, the PROFIsafe address ranges of cells 1-1-2, 1-2-1 and 1-2-2 can overlap.

Figure 3-40



Note

Because IPCs are not suitable for (failsafe) network isolation, IPCs with multiple network interfaces may never be connected with more than one network at a time. This does not apply as long as other organizational measures can guarantee the uniqueness of PROFIsafe addresses and/or if the corresponding plant components are in a safe state.

PROFIsafe address assignment

If the PROFIsafe address will be assigned via STEP 7 Safety, an online connection from the engineering station to the F-CPU (PROFINET I/O controller) is required. To establish the online connection, the F-CPU must be reachable on layer 3. The assignment of the PROFIsafe addresses to the F-I/O devices in the subnet of the F-CPU then continues via layer-2 mechanisms.

Accordingly, a PROFIsafe address can also be assigned from across a SCALANCE SC622-2C router.

3.8.4 Safety-related CPU-CPU communication

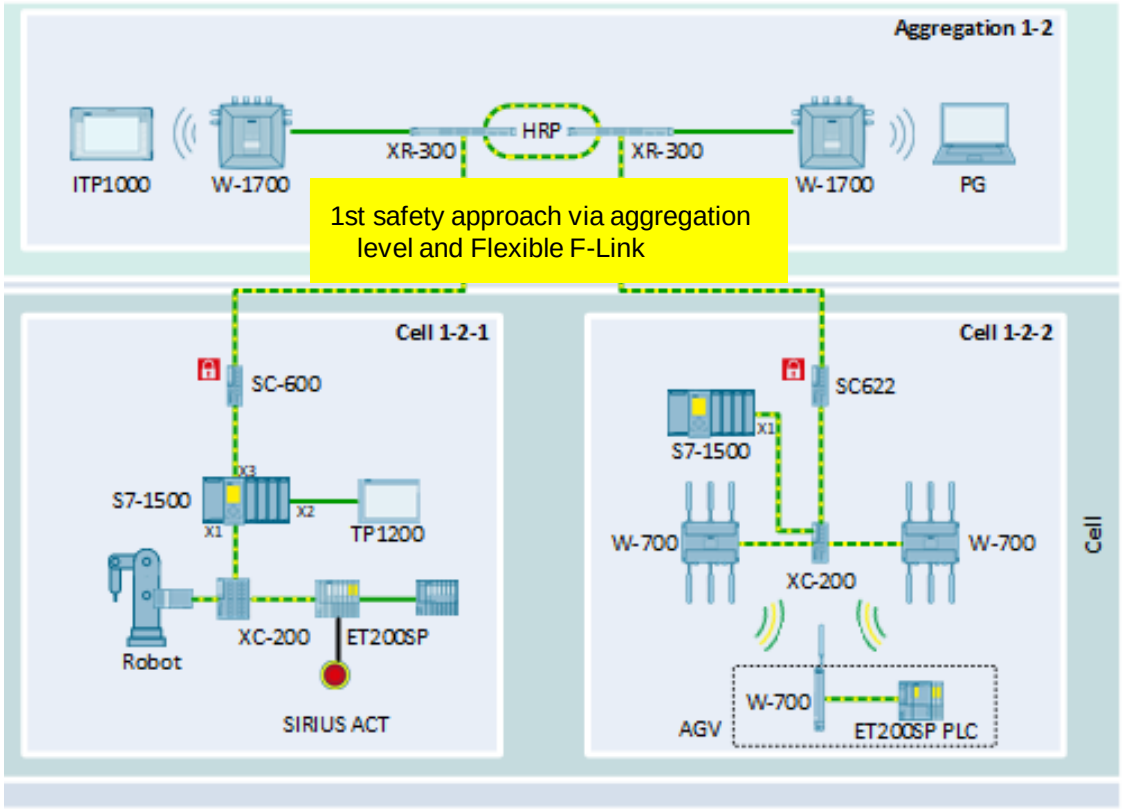
Communication within a cell

For safety-related CPU-CPU communication within a cell/subnet, you have the option of I/O controller-to-I-Device communication. In the same manner as with the default via PROFINET I/O, communication is implemented via configured transfer ranges (F-CD) and the SENDDP and RCVDP instructions. This option offers the advantage of deterministic failsafe communication without additional hardware (see manual \19\).

Communication between different cells via Flexible F-Link

The so-called "Flexible F-Link" is available for safety-related CPU-CPU communication across cell/subnet boundaries. Here, Flexible F-Link relies on standard communication mechanisms (**O**pen **U**ser **C**ommunication). These mechanisms provide the option of routing from one cell into a different cell via layer 3 and the aggregation level (e.g. via TCP/IP). This does not compromise the cell security concept. In such case, Flexible F-Link does not place any special requirements on the configuration of the router or port being used. Simply make sure that the Open User Communication (e.g. TCP or UDP) beneath Flexible F-Link is routed to the appropriate network. Flexible F-Link also does not require any additional hardware.

Figure 3-41



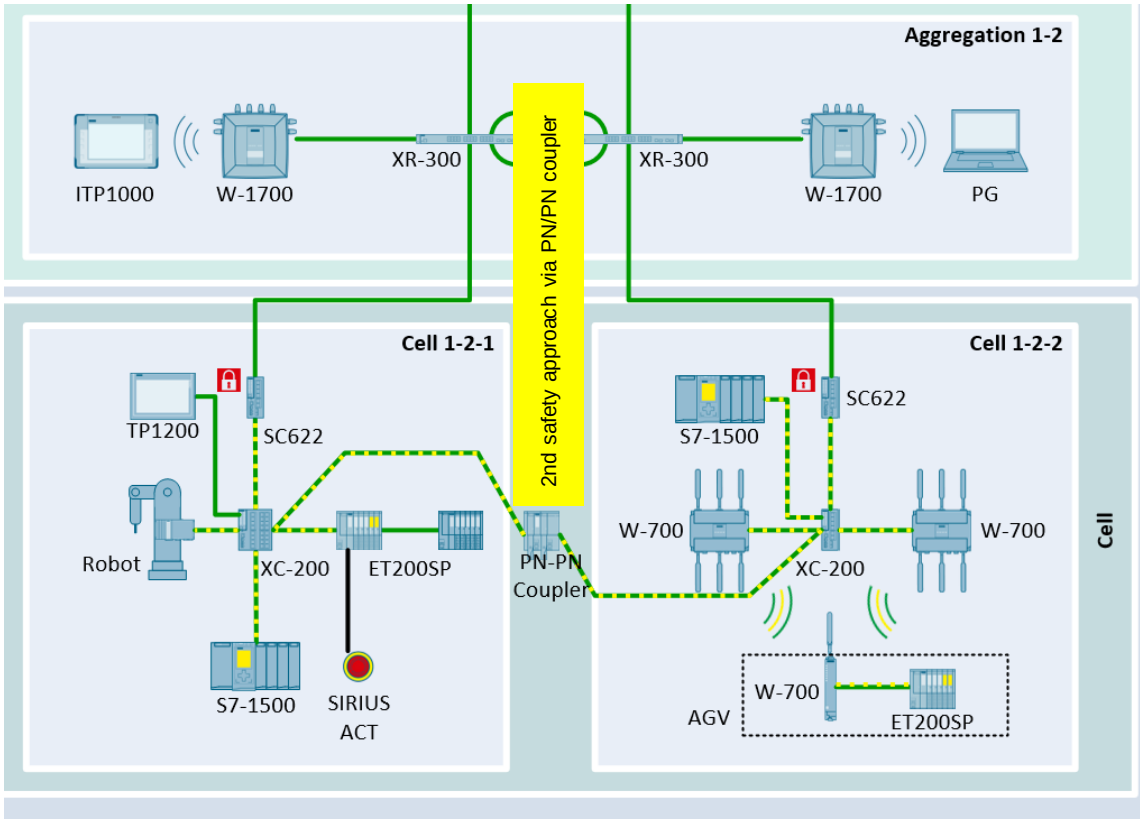
Because standard communication is used as the underlying communication method, Flexible F-Link is not a deterministic communication method. Therefore, especially for very rapid safety reaction times, it is not suitable for every application. You must verify on a case-by-case basis whether the required reaction times can be implemented with Flexible F-Link. As a decision-making aid, reaction times can be calculated using the SIMATIC STEP 7 reaction time table (S7Safety_RTTplus): \43\. An application example on the configuration of a Flexible F-Link

communication link, as well as other helpful tips and tricks, can be found in article ID 109768964: \20\.

Communication between different cells via PN/PN coupler

If safety communication cannot be implemented with Flexible F-Link due to hard realtime requirements and short safety reaction times, two F-CPUs can be connected to each other with a PN/PN coupler. In this case, while it is possible to establish deterministic communication, this solution also necessitates additional hardware for each connected cell. Especially in larger plants and where there is a rising need for networked cells, this entails higher hardware costs and additional configuration effort.

Figure 3-42



3.9 M2M communication

3.9.1 Components and application

Machine-to-machine (M2M) communication depends on which information the preceding and subsequent machine in the line need.

When it comes to communication, there are various applications for the data being exchanged. Transmission of workpiece data, for example, requires consistent transmission of relatively large volumes of data. By contrast, safety communication requires synchronous transmission of typically just a few signals as well as a guarantee of the authenticity of the data.

There are various communications protocols with different properties available to meet differing requirements. For protocols and capabilities with a focus on M2M communication, refer to the following Table:

Table 3-26

Protocol	Properties
S7 protocol	The S7 protocol is not an open standard. As such, it is only suitable for SIMATIC devices. Sending and receiving is regulated using instructions in the user program. Confirmation of receipt runs on layer 7. Additional information: FAQ on the S7 protocol: \9\
Open User Communication (OUC)	Open User Communication refers to open communication using TCP/UDP/ISO-on-TCP protocols. The TCP-based protocols are connection-oriented and contain a confirmation of receipt. UDP by contrast is connectionless and needs a manual confirmation of receipt. Secure communication with TLS is possible here. Additional information: FAQ on the OUC protocols: \11\
OPC UA client/server	OPC UA client/server is a TCP-based, connection-oriented data transmission method with emulation of services needed in industry (Browsing, Read, Write, Subscription, Method Call). OPC UA is a platform- and system-independent, object-oriented communication standard for automation. Interoperability and standardization are facilitated by information models that can be created yourself or which are based on industry standards. Additional information: S7-1500 communication function manual – Details on OPC UA client/server - \15\

Protocol	Properties
OPC UA Pub/Sub	In addition to the client/server service, OPC UA also has the capability to transmit data with Publish/Subscribe. The nodes (machines) are not directly connected with each other and a configuration to declare the nodes to each other is not necessary. Generally speaking, OPC UA Pub/Sub can run on various levels of abstraction, for example UDP or MQTT. With this data transmission method with OPC UA Pub/Sub, there is no receipt confirmation or consistent data transmission without additional manual effort. The advantage comes into play with peer-to-peer relationships that need fewer resources with Pub/Sub in comparison to client/server, thereby achieving better performance. Additional information: C2C Communication via OPC UA PubSub with SIMATIC S7-1500 on the Basis of UDP (\16\) and MQTT (\63\).
PROFINET I-Device	With I-Device, PROFINET RT on layer 2 is used to exchange data in realtime. Because of the use of the layer-2 protocol, it is not possible to use IP routing. Additional information: Application example on the use of I-Devices: \23\
PROFINET PN/PN coupler	The PN/PN coupler uses PROFINET, thereby allowing for rapid and deterministic data exchange between at most 4 PN I/O controllers for each network side via virtual I/O modules or data record communication. Data exchange between PN I/O controllers is possible across network boundaries while maintaining full network isolation, meaning that routing functions are not supported. Additional information: PN/PN coupler operator's manual - \24\
Flexible F-Link	Flexible F-Link represents one option for failsafe CPU-CPU communication. Flexible F-Link relies on a standard communication channel (e.g. TCP, UDP). It enables the transmission of failsafe data with standard communication blocks even across network boundaries (routing). Additional information: SIMATIC Safety manual: \22\

For more details on communication in the S7-1500, refer to the communication function manual: \10\

3.9.2 Requirements for the network concept

Machine-to-machine communication places the following general requirements on the network concept:

General requirements

- **Routing capability**

  When machines and cells are protected by a firewall, it is important that the M2M protocol can be routed through the firewall. This means that a protocol based on layer 3 is easier to handle.

- **Security mechanisms**

  As demonstrated already in chapter 1.5, protecting the communication between the security zones is an important aspect of security. A machine can function as its own security zone. Therefore, protocols like TLS (Transport Layer Security) that include their own encryption are suitable as M2M protocols. Alternatively, encrypted tunnel mechanisms can be used together with a VPN and TLS, for example OpenVPN.

- **Realtime capability**

  With high-performance process machines that exchange process-related information, realtime capability can be a requirement for M2M communication. This means that information must be sent to the partner and received within guaranteed time intervals. The most common methods in this case are to use an I-Device or PN/PN coupler with PROFINET RT.

Advanced requirements

Additionally, there are still other requirements that, while they don't pertain directly to the network concept, still play a role when selecting the communications protocol.

- **Openness**

  Because machines are not always supplied by the same manufacturer, the openness of the M2M protocol is an important aspect. Using an open standard such as OPC UA enables compatibility of machinery from different manufacturers.

- **Standardization**

  Standardized interfaces can be employed to increase the reusability of a machine within an industry or within a large company. With information modeling, OPC UA provides the ability to configure a uniform interface to the outside.

- **Safety**

  The transmission of safety-related signals across machine boundaries represents an essential requirement. In the process, data integrity (data are current and correct), authenticity (correct recipient) and prompt transmission (timeliness) must be guaranteed.

3.9.3 Implementation of the requirements for the network concept

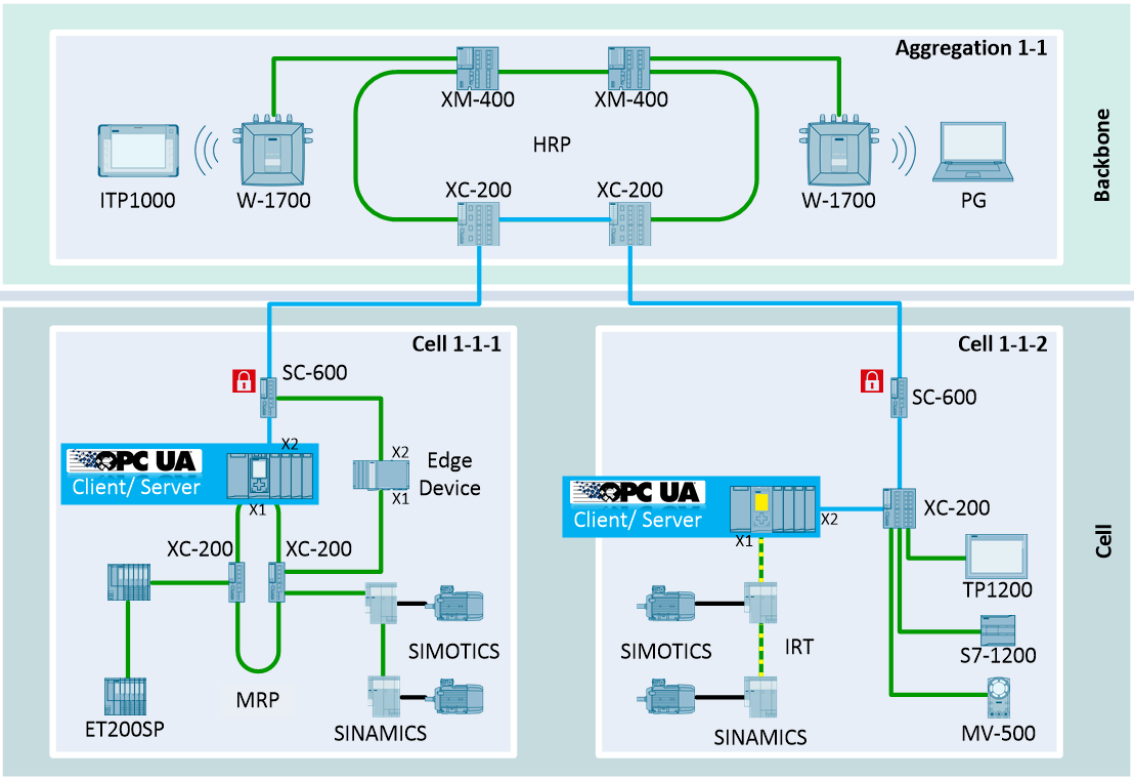
Because of the requirements that cannot be currently combined within one single protocol, three separate solutions are employed. They are described in detail in the following:

- OPC UA client/server (capable of routing, secure, open, standardized)
- Flexible F-Link (capable of routing, secure, safety-focused)
- PN/PN coupler (realtime-capable)

OPC UA client/server

The preferred solution for standardized, open M2M communication is OPC UA client/server communication. Both sides of this solution use the native OPC UA client & server functionality of the S7-1500. In addition, information modeling outputs the machine's data economy in a uniform structure on the server side. Method calls are utilized for consistent data transmission. Additional details on possible data access with OPC UA client/server are presented in the communication manual of the S7-1500 in the OPC UA chapter: \15\.

Figure 3-43



The following configurations must be made in detail in the controllers:

1. Enable the OPC UA client/server function

2. Set the server security policy
   a. It is recommended to use the policy "Basic256Sha256 – Sign & Encrypt".

3. Certificates for trusted clients
   a. From a security perspective, automatic acceptance of client certificates should not be used.
   b. Certificates can be managed locally in TIA Portal.

4. User authentication
   a. From a security perspective, guest authentication should be disabled.

   b. For access to the server and for client use, special roles can be assigned for the user in TIA Portal.

5. Modeling of server interfaces
   a. Simple modeling with TIA Portal
   (see application example \25\)
   b. Modeling of custom information models or emulation of companion specifications with "Siemens OPC UA Modeling Editor" (SiOME)
   (see application example \26\.)

6. Provision of server methods
   a. Methods for consistent data transmission must be provided.
   (see application example \27\)

7. Programming of client function
   a. The client function is programmed using system blocks in the controller.
   (see application example \28\)
   b. On the client, the same security settings are used as those described under points number 2 through 4.

8. SC-600 settings
   a. The port used (default 4840) must be allowed in the firewall for inbound and outbound traffic.
   b. Create routes from the subnet of cell 1 into the subnet of cell 2 and vice versa.
   (see routing chapter 2.2.6 and after).
   c. Advantage of the chosen solution: Easy configuration, as the communication only runs via the aggregation level and not through the DMZ firewall.

Note If you use controllers not from the S7-1500 series, you must make sure that the necessary OPC UA feature set is supported.

The solution shown uses fixed IP addresses in the cell. Addressing of client and server is also done with the IP address and the associated port. Alternatively, it is possible to reach the server with the "Fully Qualified Domain Name" (FQDN). FAQ \29\ describes the necessary considerations when configuring the client.

The advantage of the solution described lies in the communication via the aggregation level. Machines that communicate with each other in a line are usually bundled into an aggregation, making this solution possible. Alternatively, there are situations where communication must take place between machines across the boundary of the aggregation level. This case requires additional configuration in the DMZ firewall (firewall rules, routes).

Flexible F-Link

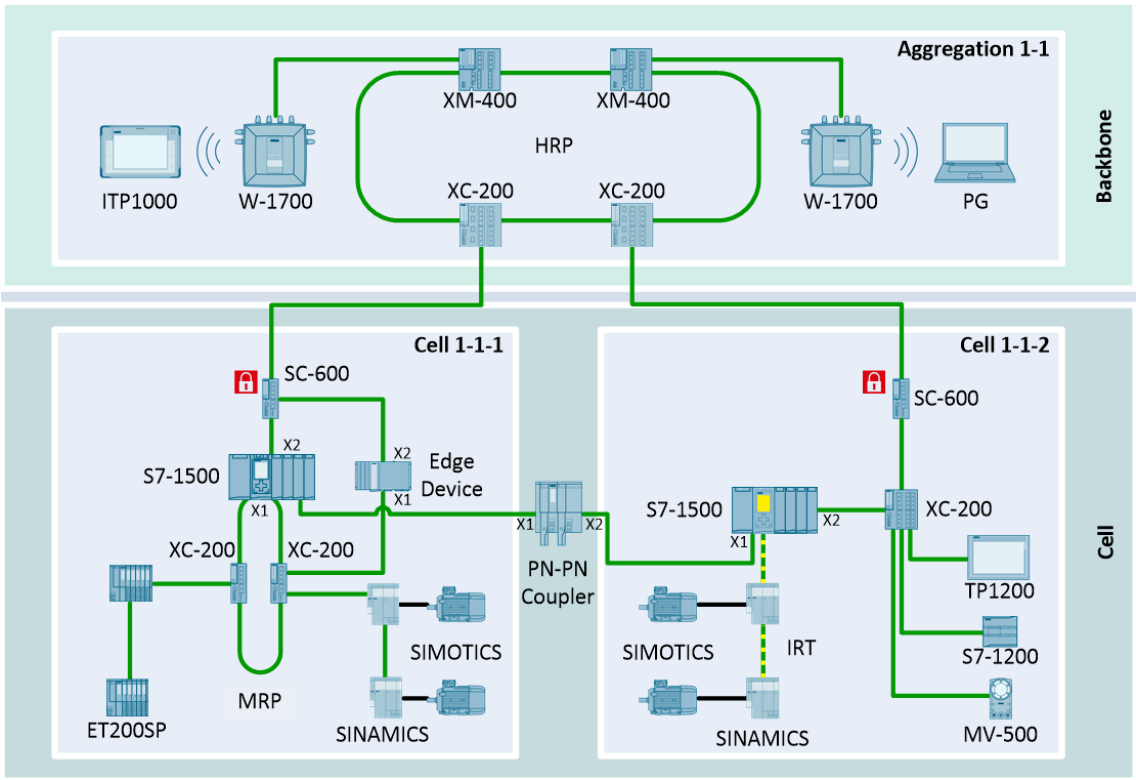
If safety-related communication is necessary, it is recommended to use the Flexible F-Link.

More details on this topic can be found in chapter 3.8.4 – Safety-related CPU-CPU communication.

PN/PN coupler

The solution with the PN/PN coupler is employed to meet hard realtime requirements. Even as a follow-up measure, it is easy to set up direct data communication between two machines in different subnets. Unlike with I-Device, it is not necessary here that both controllers be located in the same subnet. In addition to data records, input and output data can be transmitted on a send clock of down to 125 µs.

Figure 3-44



In the context of the network concept, the following points should be observed:

- Another free IP address must be available in the subnet of the respective cell.
- The additional PROFINET traffic should be taken into account in the network load. For details on the PROFINET network load, see chapter 3.7 "PROFINET communication".
- Because the PN/PN coupler isolates the networks on layer 2, uniqueness of the PROFIsafe addresses is assured. For more details on PROFIsafe communication with the PN/PN coupler, see chapter 3.8.4 – Safety-related CPU-CPU communication.

Additional information on configuring the PN/PN coupler:

PN/PN coupler operator's manual (\24\)

3.10 Communication to clouds

As a consequence of digitalization, communication into cloud systems is becoming increasingly important. Typical applications in this context are monitoring of KPI data or production parameters in online dashboards. Connectivity can be granted by the automation components themselves as well as through gateway applications with the appropriate data aggregation.

The MQTT communication standard is a widely-used and simple method for a cloud connection. Connections with an advanced feature set (e.g. data buffering) often employ proprietary solutions. The selection of cloud components therefore also affects the configuration of network components.

An MQTT-based connection of an S7-1500 CPU to MindSphere is described below as an example. It represents systems with an integrated cloud connectivity function.

3.10.1 Requirements for the network concept

A library with MQTT client communication blocks (\49\) is available in Industry Online Support for the SIMATIC S7-1500 and S7-1200.

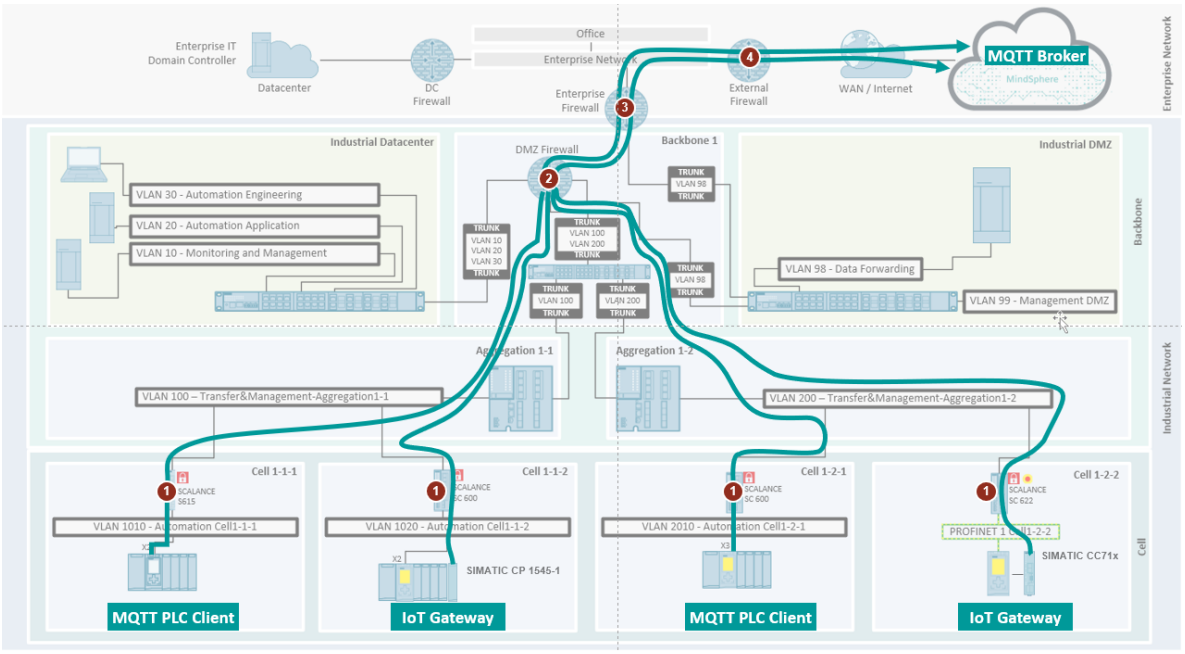
The application example "Connecting SIMATIC S7-1200 /S7 1500 CPUs to the MindConnect IoT Extension" (\50\) describes the application of these blocks for establishing an MQTT link between S7-1500/1200 controllers based on MQTT.

In this case, the CPUs establish a TLS-secured MQTT connection (TCP port 8883) to MindSphere and transmit data points to the cloud on either a cyclic or an event-driven basis.

Architecture overview

The diagram below shows the communication path into the cloud using the example of the S7-1500 stations in cells 1-1-1 and 1-2-1 (via MQTT blocks in the S7-1500 CPU) and the S7-1500 stations in cells 1-1-2 and 1-2-2 (via the IoT gateways CP 1545-1 and the CloudConnect CC71x).

Figure 3-45



MindSphere configuration

The following parameters will be defined when configuring MindSphere:

- URL of the MindConnect IoT extension
  This URL serves as the connection destination for the CPUs.

- User name and password on the MQTT broker of the MindConnect IoT extension
- Device name and type
  Name and type of the device in the MQTT broker

Configuration of CPUs and IoT gateways

In addition to the parameters that must be defined in MindSphere, the CPUs need the following base configuration:

- Configured DNS and NTP server
- Trusted root certificate from the QuoVadis Root CA

3.10.2 Implementation of the requirements in the network concept

Make the following configuration in the network components for the architecture shown in Figure 3-45. An exact list with IP addresses is located in Appendix X.

Configuration of the cell firewalls

In the cell firewalls, the TLS-secured MQTT protocol must be allowed to the outside (default port: TCP, 8883). Because of the URL-based addressing, filtering for the destination IP is not possible here.

Configuration of the DMZ firewall

Only the MQTT connections must be allowed here. Depending on the firewall design, here it is possible to filter based on the destination URL.

Configuration of the enterprise firewall:

The enterprise firewall is configured in the same manner as the DMZ firewall. Because of the source NAT configuration described in the Routing chapter, only the external IP address of this firewall is visible in the context of the MQTT connections in the office network.

Configuration of the external firewall in the office network

MQTT connections from the external IP of the enterprise firewall to the URL of the MindConnect IoT extension must be allowed in the external firewall.

Thanks to the NAT configuration this must only be done once. MQTT connections to the IoT extension that will be allowed in the enterprise firewall at a later time have already been allowed at the external firewall thanks to the aforementioned NAT configuration.

3.11 Certificate management

Communication connections with security (authentication/encryption) and HTTPS web servers generally require X.509 certificates.

In these network concepts, this applies to the following connections:

- S7 communication between CPU and HMI or TIA Portal
- OPC UA server
- TCP connections from or to the CPU (e.g. cloud connection with MQTT)
- Web servers of CPU and network components

All certificates of devices configured with TIA Portal are managed centrally in the global security settings of the projects. Application example \51\ illustrates certificate handling in TIA Portal.

For the OPC UA server of the S7-1500, there is also the option of updating the certificates during runtime by using the OPC UA interface with GDS Push. Application example \52\ demonstrates the corresponding workflows and interfaces for this.

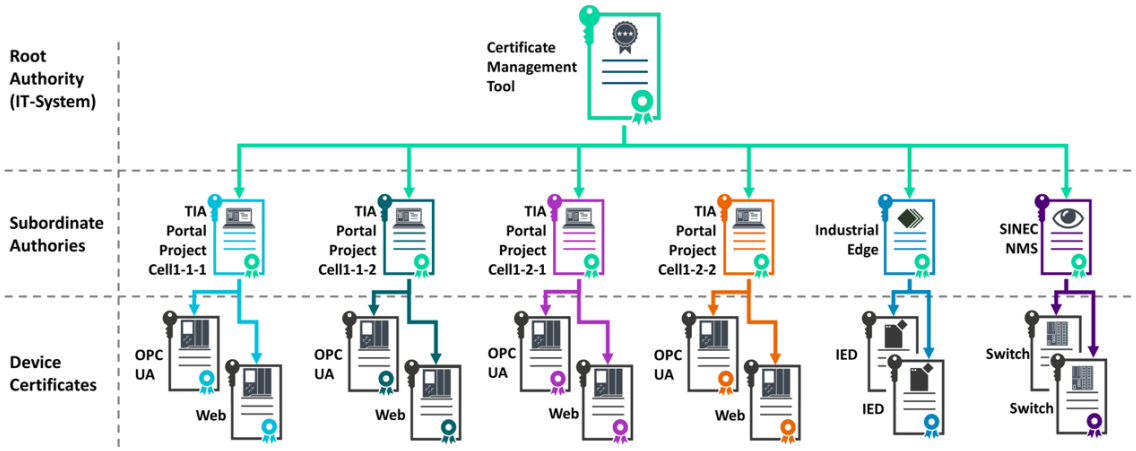
The web server certificates of the network components are managed centrally with SINEC NMS.

Industrial Edge Management likewise gives you the ability to manage the certificates for the IEM and the IED.

Because certificate handling is dependent on the individual engineering systems, it is recommended to construct a suitable public key infrastructure with the appropriate administrative tools. In this way, the certificate from the Root Authority can be trusted in every system. In addition, custom "Subordinate CAs" can be created for individual TIA Portal projects, SINEC NMS or Industrial Edge Management, for example. With these Subordinate CAs, it would then be possible to derive the device certificates from TIA Portal, Industrial Edge Management or SINEC NMS.

The following Figure shows one such PKI infrastructure.

Figure 3-46



3.12 Security

The underlying solution approach in this network concept is based on the cell security concept. Here, three essential points must be observed:

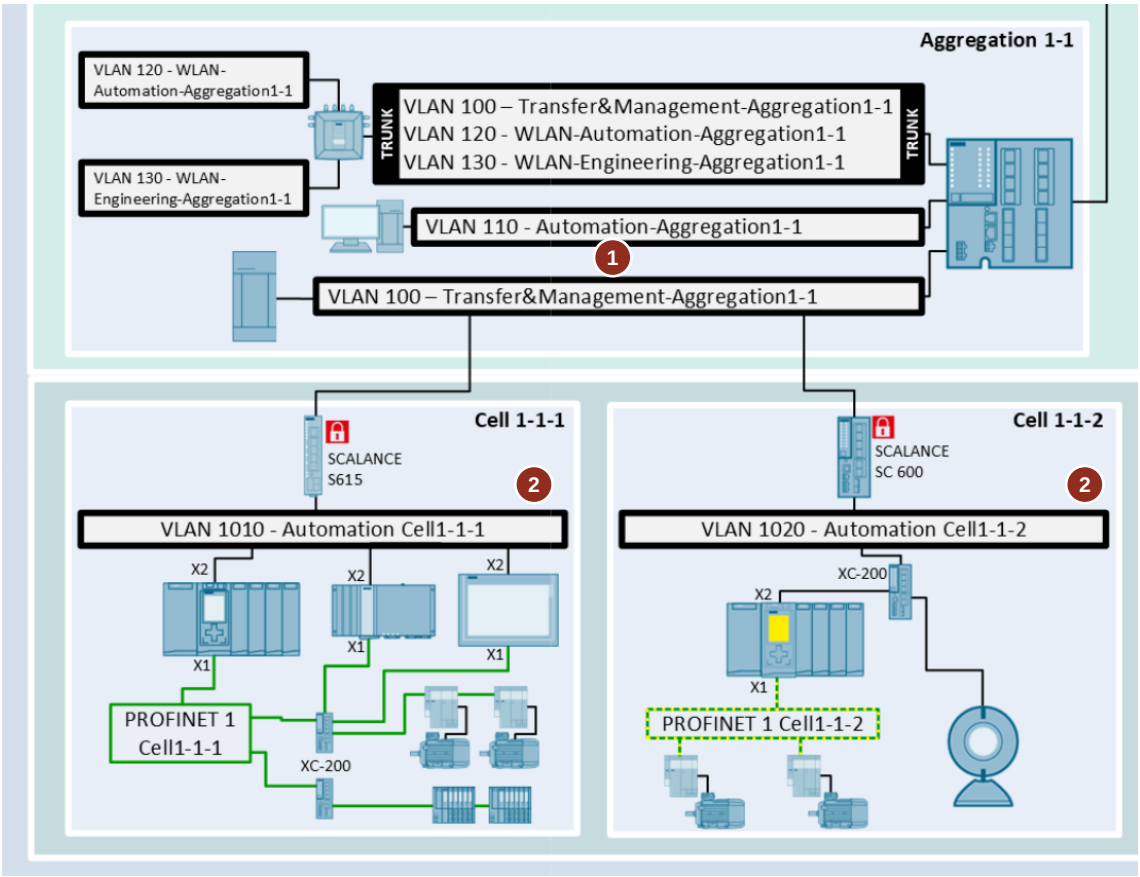
- Network segmentation
- Zone boundary protection
- Secure communication between the zones

3.12.1 Network segmentation with VLANs

Segmentation with VLANs

Segmentation of the network relies on the use of different VLANs. In this way, nodes can be grouped depending on their communication relationships. VLAN separation keeps the overall size of the layer-2 domains small. Communication between the VLANs runs on layer 3 while the SCALANCE cell firewalls / DMZ firewall handle routing.

Figure 3-47



In Figure 3-47, the isolation is used in two variants.

1. At the same port with different VLANs, i.e. at one trunk port to separate different types of traffic (VLAN 100/110).
2. On the cell level in the SCALANCE S615/SC600 at different ports to achieve isolation between cell/aggregation (VLANs 1010/1020).

Even without further security mechanisms, this division offers certain advantages compared to a large, flat layer-2 structure:

- Thanks to the smaller layer-2 domains, propagation of multicasts and broadcasts is limited. These can be targeted at the nodes in the same VLAN rather than at all nodes.
- Errors and problems with wiring or address assignment (network loop, duplicate IP addresses) usually remain limited to the segment, i.e. to the VLAN/cell. Nodes in other segments remain unaffected.
- As a consequence, troubleshooting/diagnostics is significantly easier, as it is often immediately apparent what segment/area a problem lies in and it is possible to respond accordingly.
- The layer-3 handoffs at the cell firewall / DMZ firewall provide the capability of easy, targeted monitoring of traffic in the network, as well as restriction of traffic.

Cells and VLAN assignment/division

This network concept presents a variant commonly used for subdivision. Depending on the complexity of the network, more or fewer VLANs/IP subnets may be necessary or sufficient, especially on the aggregation level or higher. Dividing parts of the plant into different cells is recommended in most cases. This also forms the basis of the cell security concept.

Which nodes will be bundled into a cell is generally decided based on communication/security needs. The most important limitation in this process is the use of deterministic, time-critical protocols like PROFINET between devices. PROFINET requires layer-2 reachability. As a consequence, controllers and devices here cannot be assigned to different cells simply by using a router.

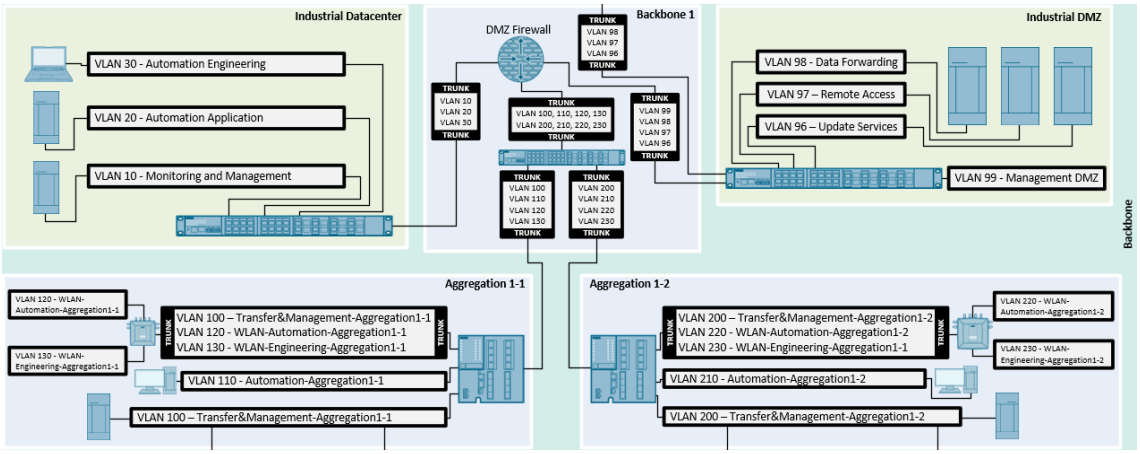
This often automatically results in a certain underlying structure that dictates how cells must be set up. For example, certain machines, production lines or plant elements may be bundled into cells based on size. A typical scale for a cell is around 250 nodes.

If the cells become too large due to the use of PROFINET, the requirements for the application should be reviewed. It is possible that plant elements may be transferred to less time-critical mechanisms such as OPC connections, S7 connections or TCP connections. Otherwise, the setup with a PN/PN coupler between cells provides an alternative (see chapter 3.9).

Segmentation in aggregation and datacenter

VLANs are also used above the cells to either separate or collate the various types of traffic as necessary. Like in the cells, the same essential advantage obtains: Interference is limited to the VLAN and not all traffic is affected.

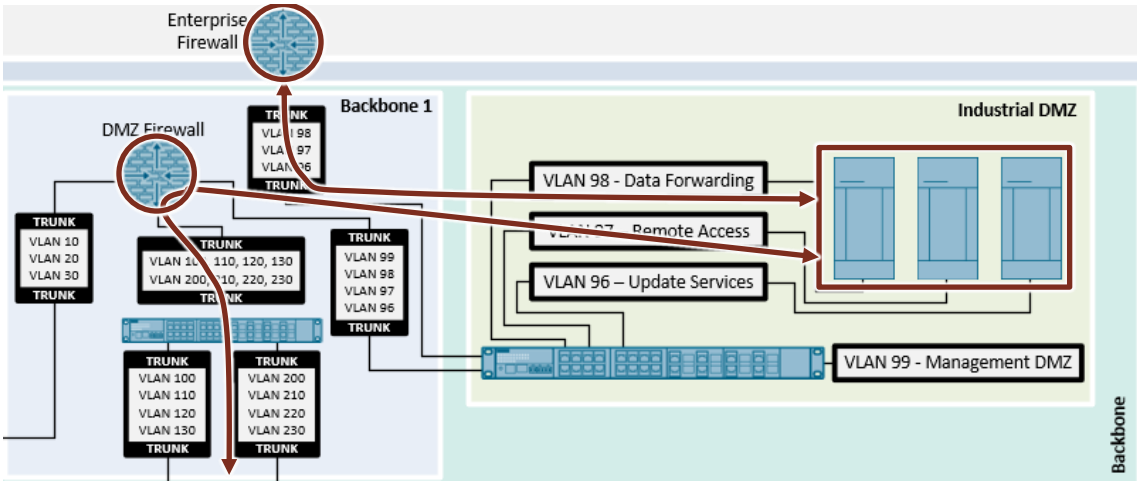
Figure 3-48



Moreover, the VLANs can be prioritized by application. For example, data for remote access can be given priority treatment over the update services.

Data are exchanged between the VLANs exclusively via the DMZ firewall. The entire configuration can thus be easily managed from a central location. It is also possible to specify general traffic restrictions from this location. For example, certain ports/protocols can be blocked entirely or DNS queries filtered in this way.

Figure 3-49



In the enterprise/office network direction, the enterprise firewall spans its own DMZ, ensuring a two-step decoupling. Direct connections to the outside should be prohibited wherever possible. Instead, both sides will connect to an application in the DMZ that provides the relevant services. For example, jump host instances are used for remote access. The user can connect to these instances and access the underlying levels from there. In this way it is possible to block and prevent direct remote access to the cell.

3.12.2 Zone boundary protection with firewalls

Overview

Inbound and outbound communication from the cells is limited as far as possible. Only the services that are explicitly allowed in the firewalls can pass through. All other requests are discarded. To configure the rules, the IP addresses of the nodes, the protocol and port as well as the direction of the connection setup must be known.

The TCP and UDP protocols are the most commonly used. A total of 2^{16} = 65,535 ports is available on each.

Each connection knows two ports:

- Origin/source port from which the connection is being established
- Destination port where the inbound connection is expected

In standard protocols, the associated port is defined and does not change (e.g. NTP on UDP 123). Otherwise, manufacturer-specific documentation will describe which ports are used (e.g. TCP 102 for an S7 connection).

Port numbers listed in this context typically also indicate the destination port. The destination port is statically configured and is the same for all connections. The source port is usually assigned by the operating system dynamically and therefore changes each time a new connection is established. As a consequence, firewall rules can be defined for a specific destination port, while the source port remains open ("any") because it is not known in advance.

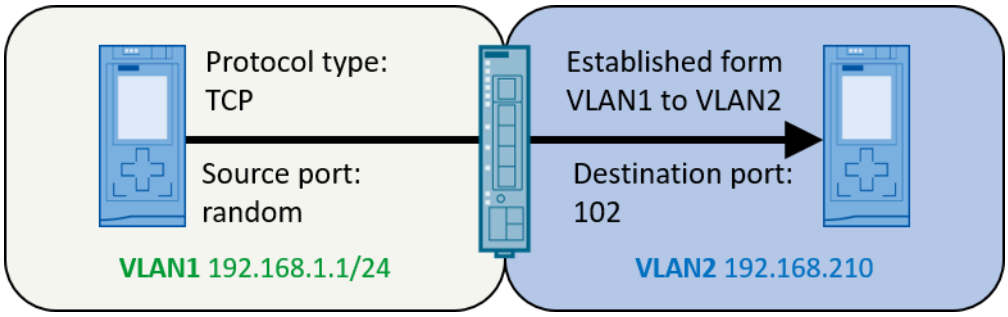
The direction of the new connection is often specified by the application, for example the NTP client actively connects to the NTP server. Connections manually configured by the user (such as the S7 protocol or TCP) have corresponding settings for which node is active or passive.

Direction in firewall rules

The direction is crucial when configuring the firewall rules. In the example in Figure 3-50, the connection from VLAN 1 to VLAN 2 must be explicitly allowed. The rule would then be:

From **VLAN1 / 192.168.1.1 / TCP Port any** to **VLAN2 / 192.168.2.1 / TCP 102**

Figure 3-50

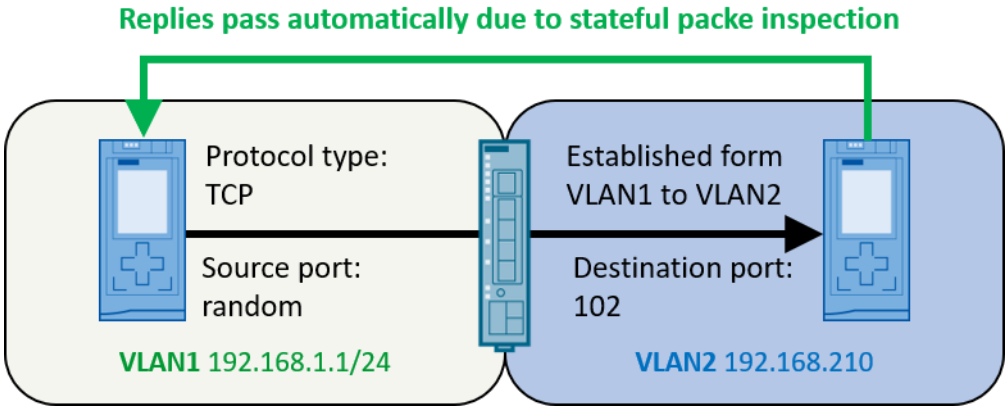


Stateful packet inspection

Because firewalls today almost always operate with stateful packet inspection, this allow rule on its own is sufficient. Here, the firewall keeps an internal record of which connections are currently active/known. The response packets in the opposite direction are automatically allowed as well, limited to the partner/IP address/port number to which the connection is active:

Consequently, no explicit rule needs to be created for the opposite direction VLAN 2 to VLAN 1. This mechanism greatly simplifies configuration and also makes it possible to reliably restrict connections with an unknown destination address (e.g. access attempts to the internet).

Figure 3-51



3.13 WLAN

3.13.1 Basics of (I)WLAN

Applications

The use of cables and lines for communication has advantages because an exclusive medium is available: The transmission properties of this medium are well defined and constant (provided that cables, routers or similar components are not replaced) and it is distinctly recognizable at any time which nodes are connected to the LAN and which ones are not.

However, the complexity of the cabling (and the possibility of cable breaks and other hardware faults) increases with the number of nodes. Ultimately, the use of wired methods for communication with freely moving nodes is only feasible in exceptional cases. Radio links also make it possible to bridge areas that would otherwise be difficult to reach with cables (streets, bodies of water).

These applications are where radio-based networks can bring to bear their advantages, foremost of which is their low dependence on a fixed location. In these cases, the potentially higher investment costs are compensated by increased customer benefits.

Electromagnetic waves

Unlike signals in a line, radio signals propagate three-dimensionally in space as electromagnetic waves.

Obstacles and objects influence the propagation of the radio waves. Effects such as reflection, scattering, absorption, interference and diffraction may occur. This produces a complex radio field that changes even further when the obstacles move around. Clearly, the area saturated by one or more transmitter(s) is not sharply defined. Thus, there is no clear delimitation of the radio field which causes a fluctuation of the transmission properties for the individual nodes of the radio network, depending on their position. In addition, it is practically impossible to discover a "silent listener" in a radio network.

These properties have considerable consequences on questions regarding connection reliability and eavesdropping security or interference immunity of a network. Assuming responsible administration, careful planning and the availability of trained employees who are aware of the specific concerns pertaining to wireless networks, they are as reliable, secure and robust as wired networks.

3.13.2 Coordination of data transfer

Radio networks are so-called "shared medium" networks, i.e. all stations share the network. To prevent simultaneous access to the network, regulations were necessary to coordinate which participant may send and when.

Distributed Coordination Function – DCF

For a WLAN in accordance with the IEEE 802.11 standard, all nodes are essentially "responsible for themselves" and exercise uncoordinated access to the wireless channel. The access of nodes carrying critical data cannot be predicted. The basis for DCF is the CSMA/CA protocol. This protocol requires a check from each station before transmission to determine whether the medium is free. Only then may data be transmitted.

If two stations are checked at the same time, it is possible for both to recognize the medium as free and transmit data simultaneously. This results in a collision, making the data unusable. A wireless transmitting station is not able to detect a signal collision itself. Its own signal covers the signals from other stations, and it is impossible to distinguish collisions from interference.

In order to avoid these non-recognizable collisions as well as possible, the CA (Collision Avoidance) system is also used. If the occupied medium is now free, a station ready to transmit will not start straight away with the data transmission but will wait for a randomly determined period of time. After the lapse of this wait time, the station will again check the status of the medium. Because of this random wait time, it is very unlikely that both will start to transmit at the same time.

Point Coordination Function – PCF

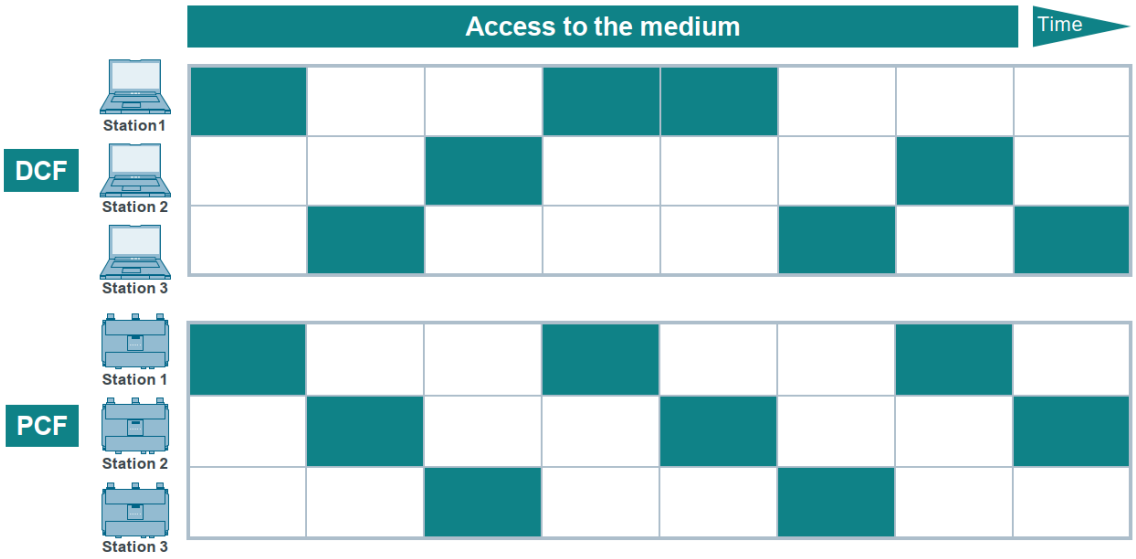
The abbreviation PCF describes a method of access defined in the IEEE 802.11 standard. However, implementation of this method is not mandatory. The method can be used to avoid some of the disadvantages of the DCF method.

In PCF, not all network nodes have equal rights. Instead, one or more access points act as central administrators in the network. One access point then assigns time slots to the other nodes, the clients: Within these slots, the frequency is reserved for these clients and they can transmit without being disturbed.

Using PCF, it is possible to assign regular network access to the clients and to ensure the transmission of data within a specific period. Therefore, PCF is preferred for applications that require continuous data streams (synchronous data transmission such as video or audio streams and, of course, process values). The transmission periods achieved, however, are in the range of several hundred milliseconds and the speed of the change from one wireless cell to the next does not meet realtime requirements. In practice, PCF is rarely supported by manufacturers.

The following diagram shows the difference between the two methods when it comes to accessing the medium.

Figure 3-52



Industrial Point Coordination Function – iPCF

With iPCF, SIEMENS presents a proprietary alternative to PCF which solves many of the problems with PCF. Furthermore, iPCF enables the clients to change wireless cell extremely fast, where the log-off and new log-in of the client ("handover") happens so quickly that the realtime requirements for communication are still met.

In iPCF, the access points poll the clients in their wireless cell in regular, very short intervals. The clients respond with the relevant data frames and can register their need to send further data telegrams. However, they only initiate another broadcast when they are polled again by the access point according to their need.

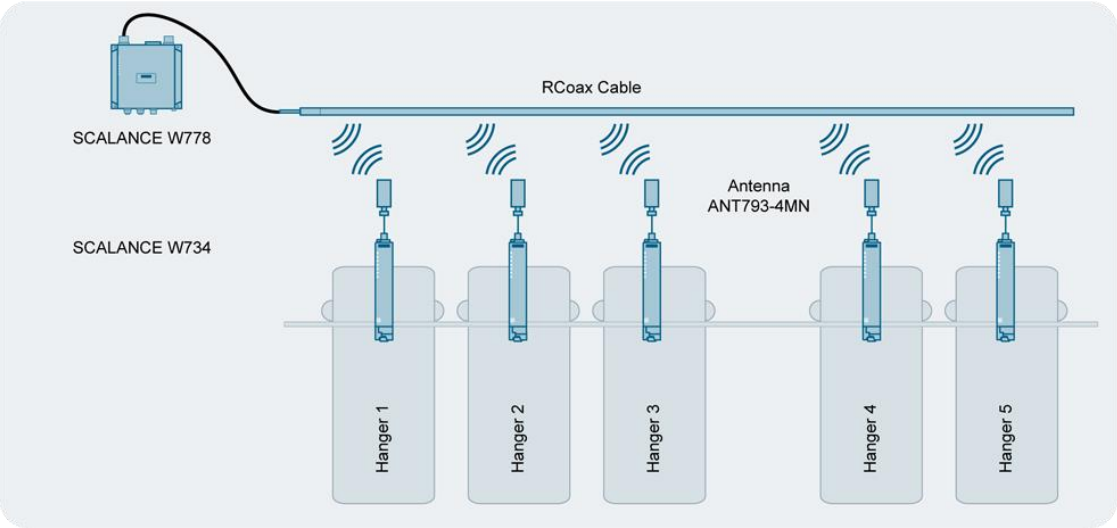
The following effects emerge from these properties:

- The access point can be parameterized to poll at a very rapid rate. This results in very low response times for each client (deterministic transmission) and very short roaming times.
- The transmission of larger, non-time-critical telegrams is delayed until free cycle time becomes available.
- The scanning of a node is seen by all other nodes in the cell. This allows a client to detect the quality of the wireless link to the access point even when it is not communicating with the access point itself.
- Thank to the short polling cycle times, a client very quickly determines whether the connection to its access point still exists or not. If the contact has been lost, the client can react within a very short time, establishing a connection to an alternative access point.
- In iPCF mode, both the search for a new access point and the login to this access point are optimized for their time performance. Handover times well below 50 ms are achieved.

That means that with iPCF, industrial applications with medium level realtime requirements are WLAN-capable in the two-digit millisecond range, for example PROFINET (see chapter 3.7) and PROFIsafe (see chapter 3.8).

iPCF can be used in a wide variety of applications, for example with overhead monorails and when using RCoax lines.

Figure 3-53



The special iPCF-MC (Management Channel) variant is available for free-roaming nodes like AGVs or high-bay warehouses (explanations for iPCF and iPCF-MC can be found in manual \64\).

Figure 3-54

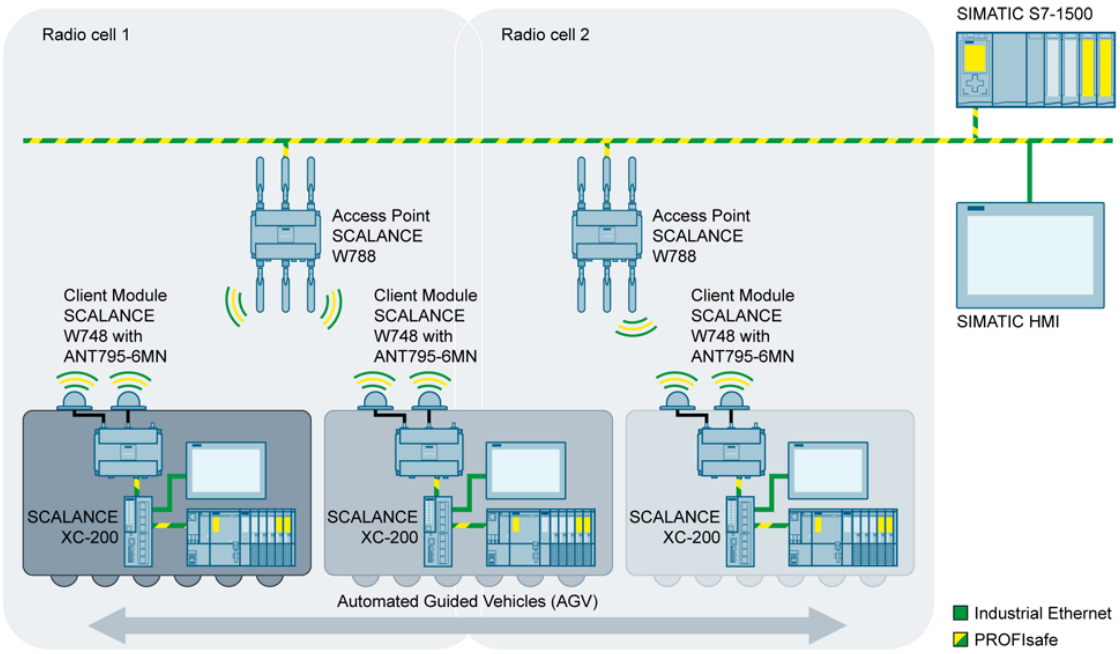
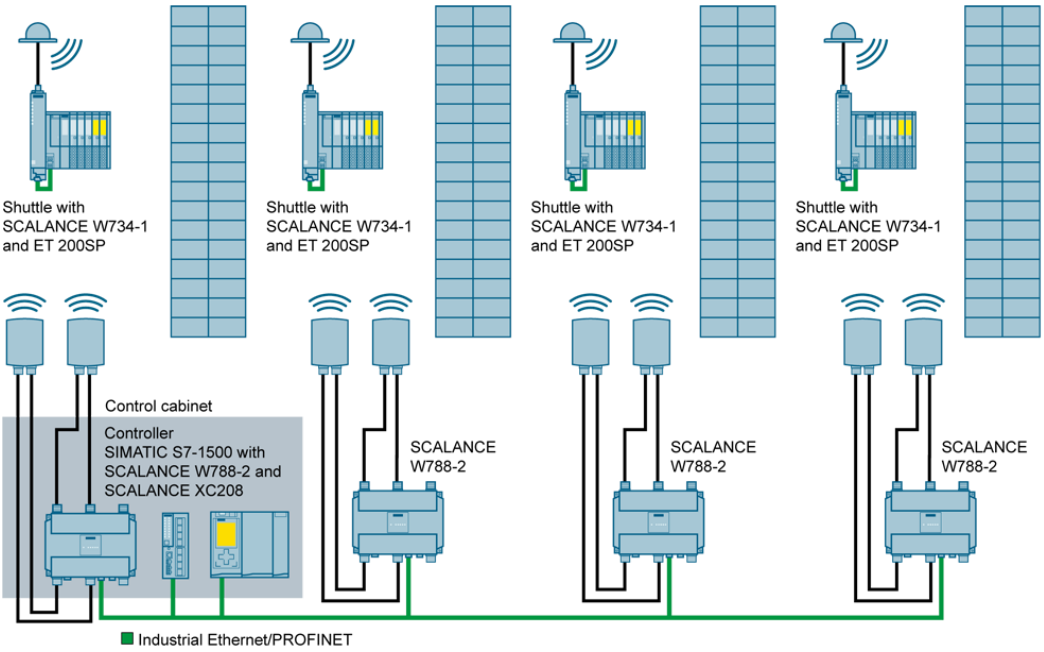


Figure 3-55



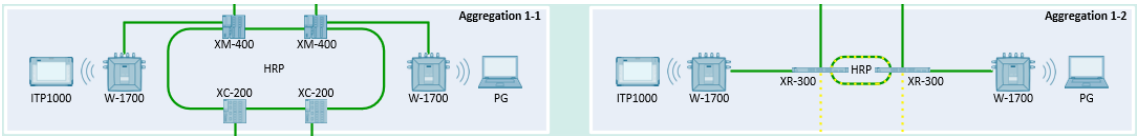
3.13.3 Implementation of (I)WLAN in the network concept

Today, WLANs and IWLANs are found in almost all areas of a modern production environment. In general, it is possible to identify two types of application:

Hall WLAN

Hall-wide WLAN saturation is used, for instance, to access enterprise data, provide a plant-wide radio network for mobile nodes, or to easily diagnose local machines on the fly. This so-called "hall WLAN" is usually implemented in the aggregation level.

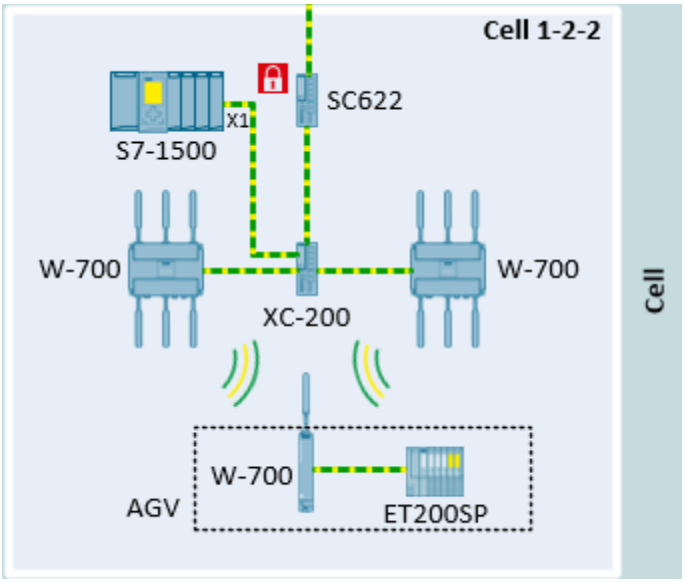
Figure 3-56



Locally installed IWLAN networks

Locally installed IWLAN networks are exceptionally well suited for addressing the special requirements of the cell in question without having to compromise. Multiple applications can nevertheless use the radio network simultaneously.

Figure 3-57



3.13.4 Radio field planning

Regardless of where the WLAN network is installed and what purpose it serves, a thorough plan should always be created. This forms the foundation for optimum functionality.

"Radio" as such is a limited resource. Due to its nature as a "shared medium" it is not possible to increase capacity by simply installing more cables, for example. With proactive coexistence management, it is possible to optimize the use of this resource, which in most cases meets the requirements of industrial applications. Always consult an expert concerning coexistence management.

The first step always involves an analysis of the environment and an inventory of the application-level boundary conditions. At minimum, this should always answer the following questions:

- On which frequency does the transmitter work?
- Is its application time critical or security critical?
- How large is the volume of data to be transmitted?
- Does transmission occur cyclically, sporadically or continuously?

- Where are the nodes stationed?

3.13.5 Coexistence management

The individual radio fields can work independently of one another if they are decoupled in at least one of the four domains, i.e. separated:

- Space
- Frequency
- Time
- Code

Spatial isolation

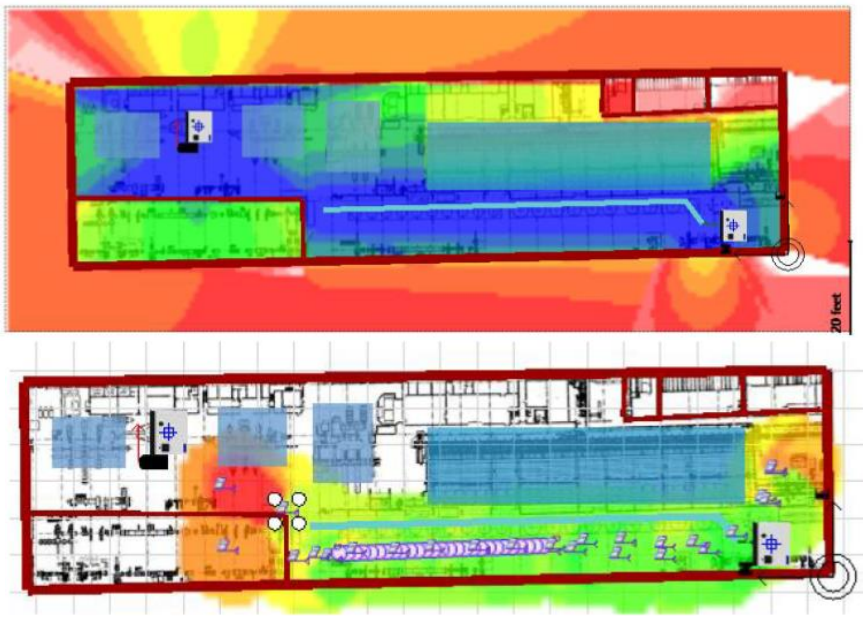
Spatial decoupling is achieved by keeping the overlap between the various radio systems as low as possible.

This is achieved by:

- Reducing the transmit power to the minimum necessary (no overshoot)
- Selecting suitable antennae
- Optimizing the installation site of access points and clients to the extent permitted by the function of the plant.

The selection of antennae and positions should always be checked with simulations and verification measurements. The Figure below shows one such result of a simulation.

Figure 3-58

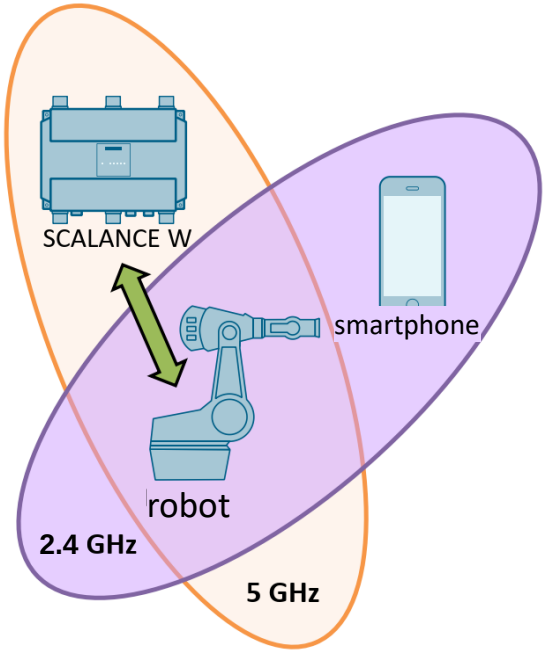


Frequency decoupling

For frequency decoupling, it is critical that the frequency ranges of the individual radio systems overlap as little as possible. In the simplest case, this is achieved by selecting the right radio channels. In a more advanced case, this is achieved by modulation and multiplex methods such as MIMO.

The following graphic shows an example of decoupling in the frequency range: The access point can communicate with the robot, even though it is in the transmission area at the same time as both are communicating at different frequencies (orange: 5 GHz, purple: 2.4 GHz). Even though the fields overlap in space and time, they are decoupled in the frequency domain.

Figure 3-59



Decoupling in time

For temporal decoupling, the configuration of the individual nodes is decisive. They must be selected in such a way that the probability of a time-critical transmission such as PROFINET I/O overlapping with another transmission is as low as possible. It is possible, for example, to reserve a channel exclusively for time-critical transmissions, as long as this is feasible in practice.

Code decoupling

For code decoupling, it is mainly the separation and distinction of different data streams transmitted in parallel via a shared frequency band that has priority. To make each distinct, the data streams of the nodes are coded with independent and individual spreading codes (orthogonal codes). In this way it is possible to detect unambiguously which signal belongs to which user.

3.13.6 Security

When using WLANs, users can easily get the feeling that the connection is not secure, as it is not necessary for an intruder to access a factory site and physically connect with the network in order to listen in on data: In principle, anyone located within range of the radio signal can listen in on a network's data traffic.

However, this assumption is misleading as hardly any cable-based, isolated LANs remain today: in reality, most LANs are connected with the internet and so they, too, are potentially vulnerable

to external attack. Security must be deliberately configured for radio networks as well as for cable-based networks.

Thanks to advances in security standards and in component performance, radio networks today can be considered as secure as cable-based networks.

One of the simplest measures for securing a radio network consists of configuring the access points and their transmission power, for example, so that they only actually cover the required space without any overshoot. In an ideal case, this restricts the radio network to the company site and prevents external eavesdropping.

Encryption and authentication methods

A reduction in the radio power can admittedly only provide limited protection and cannot be realized for every scale. More advanced, effective and secure methods include the selection of a suitable infrastructure as well as the use of powerful encryption and authentication protocols.

These have been developed in the working group of the IEEE 802.11i standard.

- TKIP ("Temporary Key Integrity Protocol") as a temporary solution for older WLAN devices.
- AES-CCMP (Advanced Encryption Standard, CTR / CBC-MAC Protocol) as a final encryption method that is recommended by the NIST (National Institute of Standards and Technology) today.
- AKM ("Authentication and Key Management") to secure a unique authentication process in a WLAN.

It was on this basis that the Wi-Fi Alliance founded WPA2 ("Wi-Fi Protected Access 2") as a new security standard. Encryption with WPA2 focuses on the full implementation of the IEEE 802.11i extension and uses AES-CCMP. Two methods of operation are possible here:

- WPA2 (RADIUS): Authentication by a server (RADIUS server) is subject to fixed specifications. The dynamic exchange of the keys in each data frame introduces further security.
- WPA2-PSK: With this method, authentication is achieved using a password rather than a server. This password is configured manually on the client and access point.

The sign-in process and assignment of access permissions for clients with WPA2 (RADIUS) is defined in the IEEE 802.1X standard. The RADIUS protocol based on "EAP" ("Extensible Authentication Protocol") is utilized in order to implement this for larger networks and 802.1X (also in office networks) as a network access protocol (NAC).

RADIUS protocol

The RADIUS protocol (Remote Authentication Dial In User Service) for authentication on the network was originally developed for cable-based systems. However, it has also proven to be successful in other areas, particularly the wireless sector. With RADIUS, there is a central server referred to as RADIUS, which contains a list including the access authorizations for all nodes. If a client wishes to connect to the network, the access point forwards the request to the RADIUS server. It reacts by generating a "challenge", i.e. a request for the client to send an appropriate "response" if it has the password saved on the RADIUS server.

This method has two advantages:

- The password is never sent via the network in plain text, meaning it cannot be intercepted by an unauthorized individual.
- Since the access authorizations are saved on a central server, the method is particularly suitable when using roaming clients. Not all access points need to store the access data from the clients, but they can request them any time from the RADIUS computer.

EAP protocol

The acronym EAP (Extensible Authentication Protocol) covers a wide framework of different authentication mechanisms for network access. In other words, EAP is not an authentication method itself, but rather describes the mechanism according to which the client and server can agree on a method.

One of the methods that can be used under EAP is "EAP-TLS" ("EAP Transport Layer Security"), in which the network nodes have to be "certified" before they are authorized for network communication. In other words, they must be authenticated at a central server. This method is comparable to SSL, familiar from the internet.

Aside from this method, a large number of different, partially manufacturer-specific protocols exist that can be used with EAP.

3.14 Edge computing

3.14.1 Components and application

Components

The Siemens Industrial Edge ecosystem delivers the capability to run automation-specific software on centrally-administered platforms in the form of apps.

Typical use cases of these apps are:

- Administration and monitoring of components (e.g. asset management)
- Data concentration and protocol conversion on the line level
- Flexible expansion of the feature set of an automation solution through in-house apps

The Industrial Edge ecosystem comprises the following components:

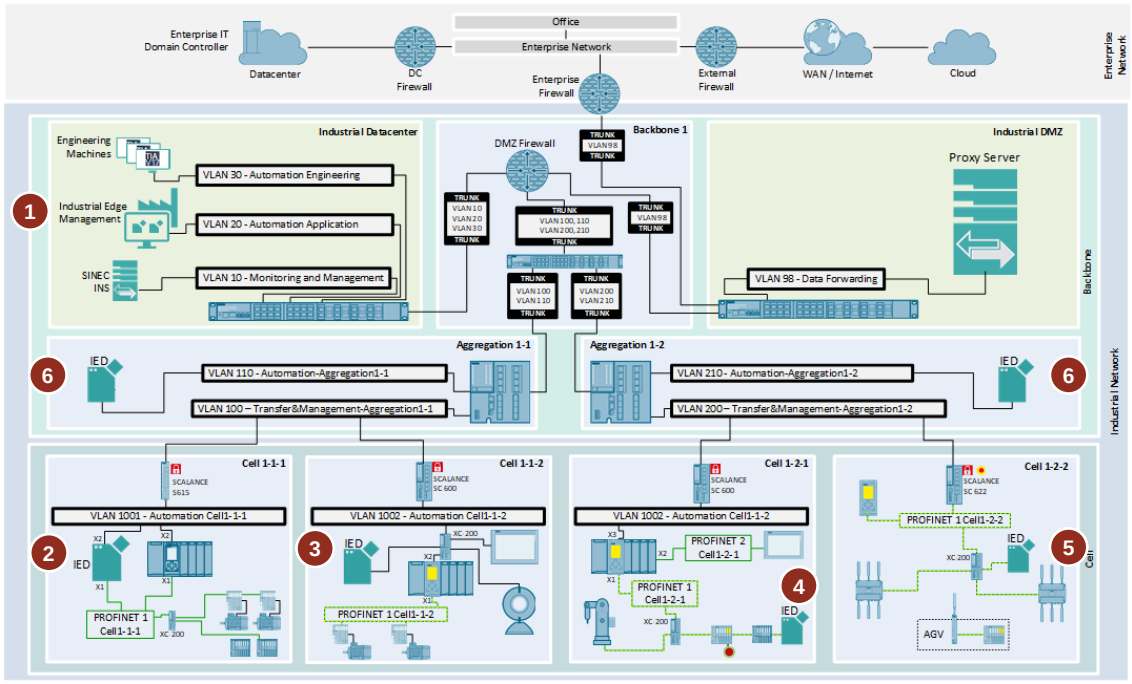
Table 3-27

Component	Description
Industrial Edge HUB (IEH)	The Industrial Edge Hub (IEH) is the central gateway for downloading and configuring Industrial Edge Management (IEM). At the IEH, you can: • Download the Industrial Edge Management OS to enable IEM on site and all the necessary software for running IEM. • Purchase available Edge apps through an app catalog • View all necessary documentation and information about Industrial Edge The IEH is available on the internet at the URL https://iehub.eu1.edge.siemens.cloud/ once access has been applied for. Then it can be ordered through the Siemens Mall or the Software Market Place.
Industrial Edge Management (IEM)	Industrial Edge Management (IEM) is the central infrastructure of Industrial Edge. Industrial Edge Management is available on-premises as a local IEM. Industrial Edge Management allows you to: • Manage connected Edge devices, including any Edge apps that you install on each Edge device. • Manage and analyze Edge devices with available tools • Manage collaboration with other developers via role-based developer functions
Industrial Edge Device (IED)	Edge apps are run on Edge devices. Edge devices can: • Store and retrieve automation data locally • Transmit/query data to/from cloud infrastructure (e.g. MindSphere)
Industrial Edge apps	Edge apps are used for intelligent processing of automation data. Edge apps are obtainable from Siemens, business partners (OEMs), third-party suppliers and your own in-house development. You can use IEM to install Edge apps, containerized with Docker, from the Industrial Edge Hub to selected Edge devices.

Placement of Edge components in the network concept

The Figure below shows a possible integration of the Industrial Edge components into the network concept.

Figure 3-60



1. Industrial Edge Management (IEM)

Industrial Edge Management (IEM) is typically run in the datacenter. Because the IEM OS is the connection destination for all IEDs, the interface configuration must be static.
To facilitate name-based addressing, for example when launching the web interface, a corresponding FQDN can be defined in SINEC INS.
In addition, the proxy server in the DMZ should be used for the connection to the IEHUB.
We suggest the following interface configuration for the IEM in the Automation-Application subnet of the datacenter:

Table 3-28

Parameter	IEM
IP address/netmask	10.0.20.10/24
Default gateway / DNS/NTP server	10.0.20.1
FQDN (stored in SINEC INS)	iem.datacenter.factory (statically defined in SINEC INS or domain controller)
Proxy server	proxyserv.dmz.factory

2. **Dual-homed Edge device** (Cell1-1-1)
A dual-homed connection for the IED is always the most versatile solution. Here, dual-homed means that an IED is used with two Ethernet interfaces. OSI layer-2 access to the fieldbus is possible via the X1 interface. The X2 interface is used both for CPU data access as well as for the upstream flow. A performance bottleneck from IP forwarding in the CPU does not occur here.

3. **Edge device in the automation cell network** (Cell 1-1-2)
   If larger volumes of data will be collected from the CPUs in a cell and (pre)processed, it is recommended to place the IED on the X2 or X3 interface of the CPU. These interfaces provide better CPU-side performance in comparison to the PN interface.
   Furthermore, the uplink traffic from the IED does not place any communication load on the CPU. When using the CPU's IP forwarding function, PROFINET field devices can be addressed on OSI layer 3 with smaller volumes of data. OSI layer-2 access to the fieldbus is not possible.
4. **Edge device in PROFINET, with CPU network isolation** (Cell 1-2-1)
   The Edge ecosystem can always be integrated into the PROFINET network. In this case, then, OSI layer-2 access is possible across the whole fieldbus. If the IED and CPU network isolation are employed at the same time, then OSI layer-3 communication to the IEM and other services (e.g. cloud) must be routed through the CPU via IP forwarding.
   With CPUs below the S7-1517, this significantly impacts communication load. Therefore this method is only recommended for smaller data volumes.
5. **Edge device in PROFINET, without CPU network isolation** (Cell 1-2-2)
   If more bandwidth is required for IEDs located in the fieldbus, it is recommended to create a gateway right in the fieldbus with SCALANCE S. In this case, the SCALANCE S shoulders the task of forwarding the OSI layer-3 data traffic. IED communication does not place a load on the CPU in this scenario. OSI layer-2 access to the field devices is also possible.
6. **Edge device in the aggregation level** (Aggregation 1-1/1-2)
   For applications that affect multiple cells, it may be prudent to place Industrial Edge devices in the aggregation level. This applies to data concentration tasks, for example. In such case, corresponding firewall rules give the IEDs OSI layer-3 access to the components in the cells.
   If devices in the PROFINET networks are accessed and the CPU-based network isolation is employed at the same time, the communication load on the CPU must be accounted for in this case as well.

Interface parameters of the Edge devices

The following interface parameters are suggested for the IEDs in the cells. If connecting to a network with DHCP services, the parameter assignment of the interfaces can be accomplished with DHCP and a static lease.

To facilitate name-based addressing, the FQDNs are defined statically in SINEC INS. If the IED is linked in the PROFINET network (Point 3 - Cell1-2-1), the corresponding cell firewall will be used as an NTP and DNS server.

Table 3-29

Parameter	IED Cell1-1-1	IED Cell1-1-2	IED Cell1-2-1	IED Cell1-2-2
IP address/netmask	X2: 10.1.10.201/24 X1: 10.1.11.201/24	10.1.20.201/24	10.2.11.201/24	10.2.20.201/24
Default gateway	X2: 10.1.10.1	10.1.20.1	10.2.11.1	10.2.20.1
DNS/NTP server	X2: 10.1.10.1	10.1.20.1	10.2.10.1	10.2.20.1
FQDN (Statically defined in SINEC INS or domain controller)	ied.cell111.factory	ied.cell112.factory	ied.cell121.factory	ied.cell122.factory

The IEDs in aggregation networks are integrated into the Automation-Aggregation subnets with the following configuration. DHCP can also be used here for configuration of the interfaces.

Table 3-30

Parameter	IED Aggregation1-1	IED Aggregation1-2
IP address/netmask	10.0.110.201/24	10.0.210.201/24
Default gateway / DNS/NTP server	10.0.110.1	10.0.210.1
FQDN (statically defined in SINEC INS or domain controller)	ied.aggregation11.factory	ied.aggregation12.factory

3.14.2 Access permission requirements in the network concept

Between an Edge device and Edge Management it is necessary to install two communication connections. The first connection is used for management and diagnosis of the Edge devices as such, while the second is used for installing the applications. There are essentially two possible configuration methods:

- **IP-based configuration:**
  Two connections are established between the Edge device and different TCP ports of the management system. Addressing is carried out using IP addresses. The Edge device does not require a DNS server configuration.
- **DNS-based configuration**
  The management system is addressed with two different URLs. For URL-based communication, the Edge device must be able to resolve DNS queries. Therefore, a corresponding DNS server must be configured in the IED.

For setup information, please refer to the document "Industrial Edge Management – Getting Started" (\3\).

Because of the network infrastructure in this concept, the rest of this document will consider exclusively the DNS-based configuration.

Here, the following communication connections are necessary for operation:

Figure 3-61

- **Industrial Edge Management**
  The IEM system requires connections to the internet to download updates and apps. The standard HTTPS on TCP port 443 is used for this purpose.
  In the event of a Siemens remote service call, an SSH tunnel is also established to a relay server on TCP port 2020.
  The DNS and NTP standards are utilized for name resolution and time synchronization.
  So that it can be reached from the IEDs by URLs, the IEM requires a static IP address that is manually entered in the DNS server with the corresponding FQDN.
- **Industrial Edge Device**
  The Industrial Edge device also uses the standard HTTPS on TCP port 443 for the connection to the IEM. This connection is outbound from the Edge device. It is used to cyclically query tasks with the IEM.
  For passthrough access on the IED web server, the device has the capability to establish an SSH tunnel (TCP port 2020) to the IEM that can be triggered by a job.
  The NTP and DNS services are also needed.
- **Industrial Edge app**
  Connectivity is always dictated by the use case. In principle, apps can provide server as well as client services.

3.14.3 Implementation of the requirements in the network concept

To run the Industrial Edge ecosystem, the following configurations must be made in the network components. Appendix I contains a precise list of the firewall rules.

This list only considers services that are required for the functioning of the ecosystem.

Industrial Edge Management

DNS and NTP servers make up the core requirement for operation of the IEM system. These services are provided centrally in the Automation-Application subnet by the DMZ firewall (see chapter 2.6).

Internet access is still required. In this concept, internet access is provided via the proxy server in the DMZ.

The following additional settings must be made in the network components:

- DNS server configuration:
  - It is necessary to create a static DNS record for the IEM. A central definition in SINEC INS or the domain controller will then make this DNS record available to all lower-level DNS servers. This is how name-based addressing of the IEM can be done with URLs.

- Proxy server configuration:
  - The IEM requires HTTPS access (and in case of a remote service, SSH access) to the internet. In this case, the following URLs are addressed:

    Table 3-31

Destination	Protocol / purpose	Port
portal.eu1.edge.siemens.cloud portal-hub.eu1.edge.siemens.cloud portalhub.eu1.edge.siemens.cloud portal-relay.eu1.edge.siemens.cloud portalauth.eu1.edge.siemens.cloud artifacts.eu1.edge.siemens.cloud oss.eu1.edge.siemens.cloud applications.eu1.edge.siemens.cloud	HTTPS access to the IEHUB	TCP, 443
portal-relay.eu1.edge.siemens.cloud	SSH/on-demand connection to Siemens remote support	TCP, 2020

    It is recommended to create a dedicated account in the proxy server for the IEM with corresponding URL whitelisting.

- **Configuration of the DMZ firewall**
  The following rule sets must be defined in the DMZ firewall:
  - HTTPS connection from the IEM to the proxy server (port: TCP, 443)
  - SSH connection from the IEM to the proxy server (port: TCP, 2020)

- **Configuration of the enterprise firewall**
  Thanks to the proxy server, it is not necessary to configure the enterprise firewall (see chapter 2.6).

Industrial Edge Device

To operate the IEDs, NTP and DNS are likewise necessary as basic services. On the cell level, these services are provided by the cell firewalls. On the aggregation level, the services are provided by the DMZ firewall.

The following configuration of the network components is necessary for IEDs in the aggregation networks:

- **Configuration of the DMZ firewall**
  - HTTPS access from the IED to the IEM (port: TCP, 443)
    If an application-layer firewall is available in the DMZ, you can filter for the management

and registry URLs that you defined when setting up the IEM, provided your configuration is DNS-based.

- SSH access from the IED to the IEM (TCP port: 32500)
  This SSH access facilitates engineering access to the IED directly through the web interface of the IEM.
- Access from the IED to the proxy server
  The proxy server in the DMZ should be used for app access to the internet. The precise ports depend on the Edge apps you have installed. But common protocols are MQTT (ports: TCP, 1883 and 8883) and HTTPS (port: TCP, 443).
  Therefore it may be prudent to allow these connections to the proxy server in advance.

The IEDs in the cell level also necessitate the following configuration of the cell firewall:

- **Configuration of the cell firewalls**
  - HTTPS access from the IED to the IEM (port: TCP, 443)
  - SSH access from the IED to the IEM (TCP port: 32500)
  - Access from the IED to the proxy server (ports: TCP, 443, 1883, 8883)
    in preparation for app connections to the cloud

Industrial Edge apps

The necessary connections depend on the apps you have installed. For example, inbound connections to the IED for accessing web interfaces are common.

In case an app establishes connections to the internet, the proxy server in the DMZ should be used with a dedicated system account for the app in question along with corresponding URL whitelisting, provided the app supports this.

As described above, the MQTT and HTTPS protocols to the proxy server can be allowed as a future-proofing measure.

4 Use cases

4.1 Backup and restore

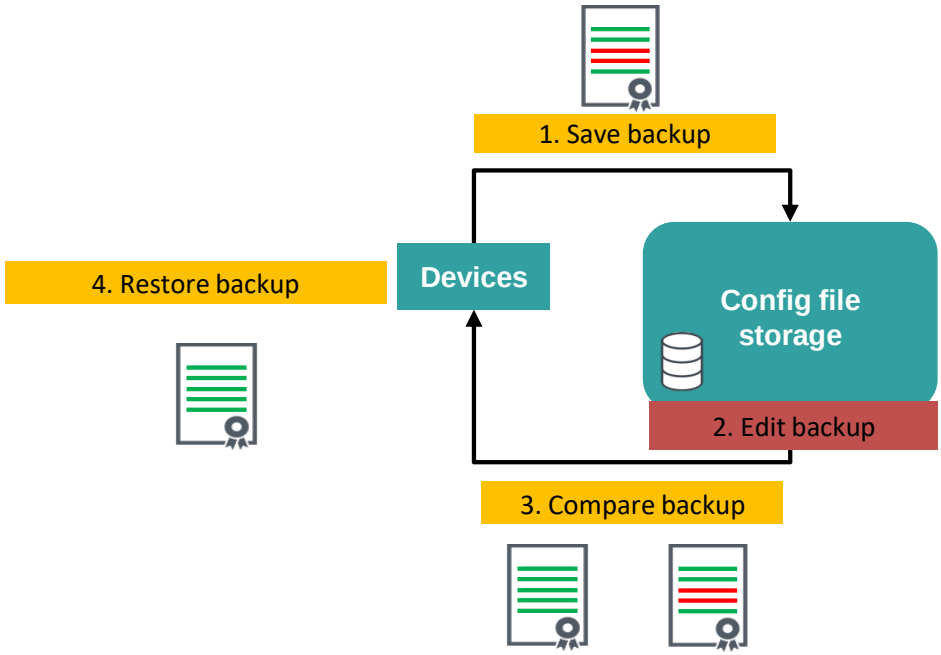
SINEC NMS

Networks are complex, and frequent changes to the configurations are the norm. To accomplish this, different configuration tools are employed.

SINEC NMS uses rule-based configuration to provide regular backup of the device configuration (configuration backup) of SCALANCE and RUGGEDCOM devices. Settings in the backup can be changed and mirrored back to the device. The current backup can be compared with an existing backup using a comparison function. The comparison results show the differences between the individual network parameters.

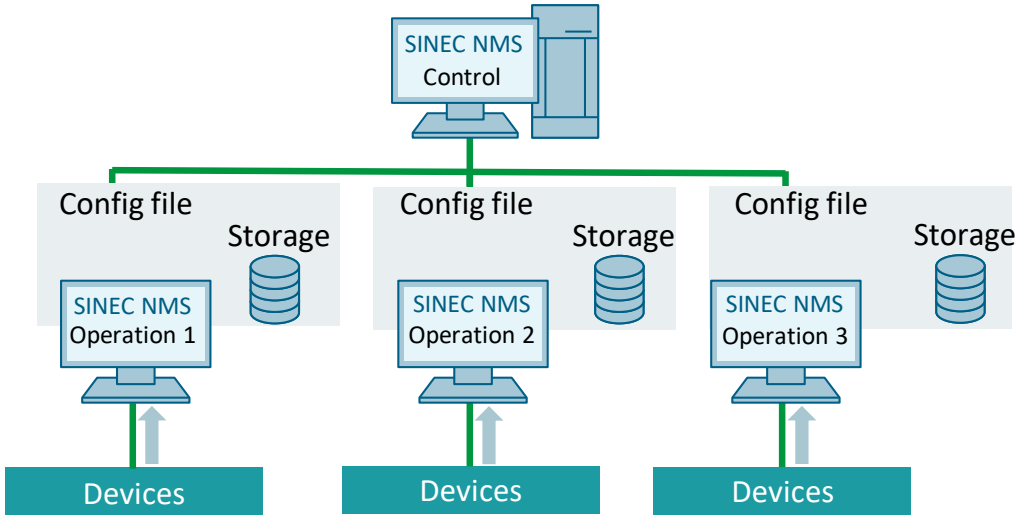
The backup can be transferred back to the device using the "Restore" function.

Figure 4-1



The device backups are stored and managed as part of their respective assigned Operations.

Figure 4-2



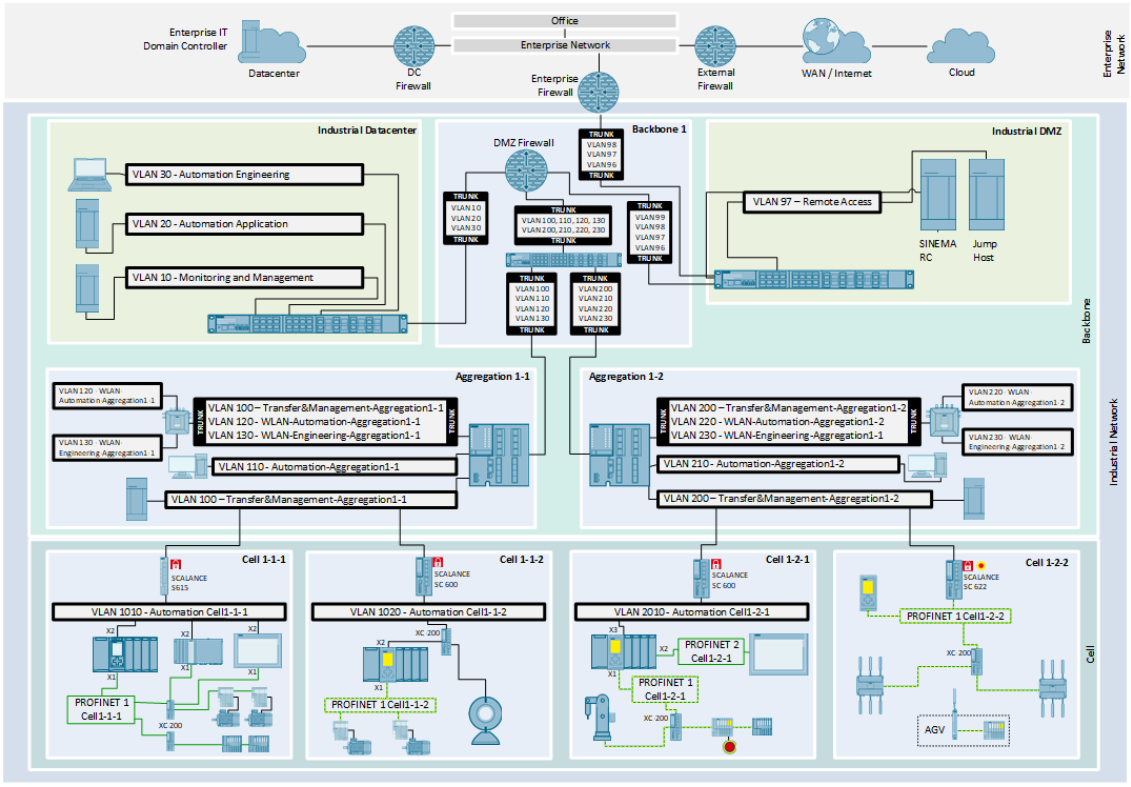
Additional information on backup with SINEC NMS can be found in the Article ID: 109762792.

4.2 Remote access

4.2.1 SINEMA RC – Easy remote access for teleservice and remote maintenance

Industrial facilities are often spread over a large area. SINEMA Remote Connect (SINEMA RC) is a management platform for remote networks that manages secure tunnel connections from a central location. In this way, widely spread-out systems or machines can be conveniently and securely maintained, controlled, and diagnosed via remote access – even if they are part of third-party networks.

Figure 4-3



The central element of SINEMA RC is a scalable server application that provides end-to-end connection management of distributed networks via the internet. It coordinates the secure connection setup between:

- Control center
- Service technicians/machine manufacturers
- Machines (cell networks) or their VPN tunnel endpoints (e.g. SCALANCE S615, SCALANCE SC-600 or SCALANCE M).

Communication between the SINEMA RC server and the remote participants is established via layer-3 VPN tunnels, taking into account the stored access rights.

The VPN tunnel endpoints are used for both network isolation via firewall and for secure remote access via VPN.

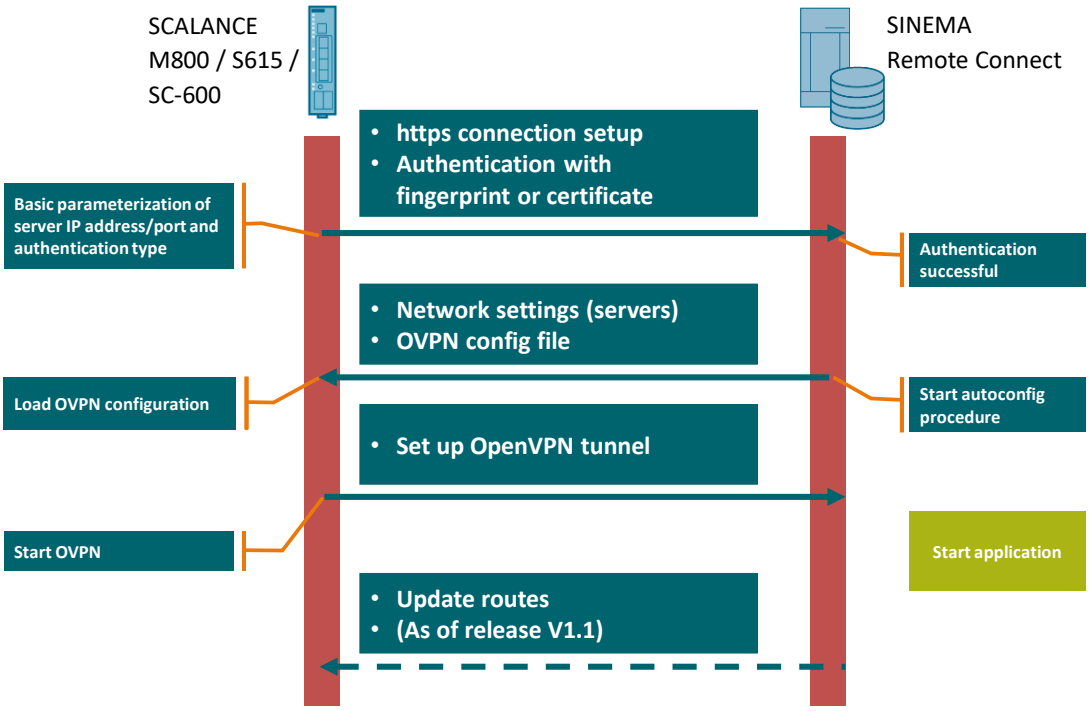
Connection setup sequence

The connection setup for secure remote access is very simple. The service technician and the machine to be serviced each establish a connection to a SINEMA RC server separately.

There, the identity of the participants is determined by certificate exchange. Only then is the remote access to the machine available.

The administration of all licenses and the software for the connected clients is done centrally. Recurring tasks can be automated thanks to a REST API, making it easy to manage even very large installations.

Figure 4-4

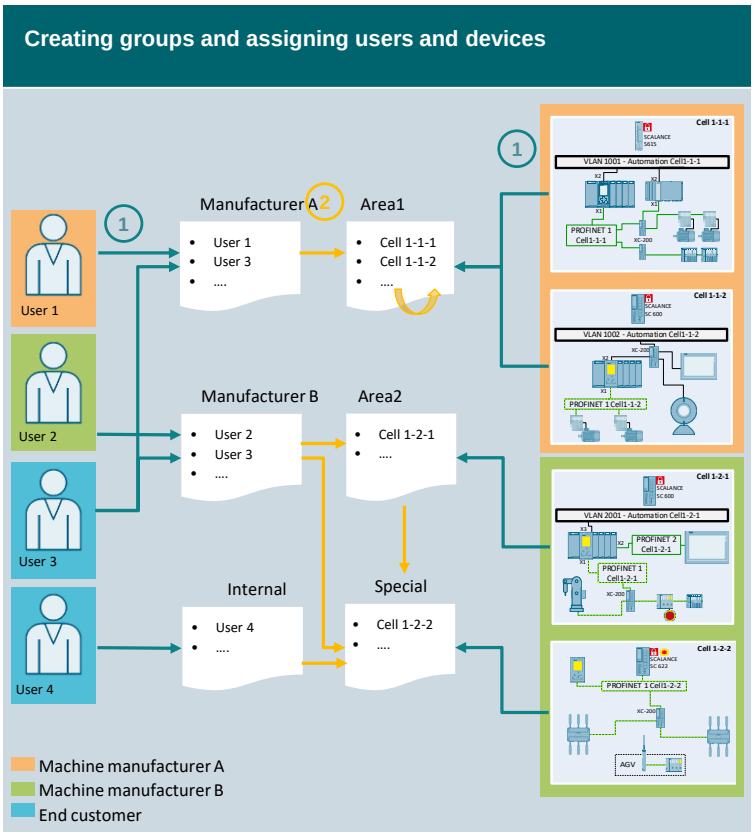


Communication relations

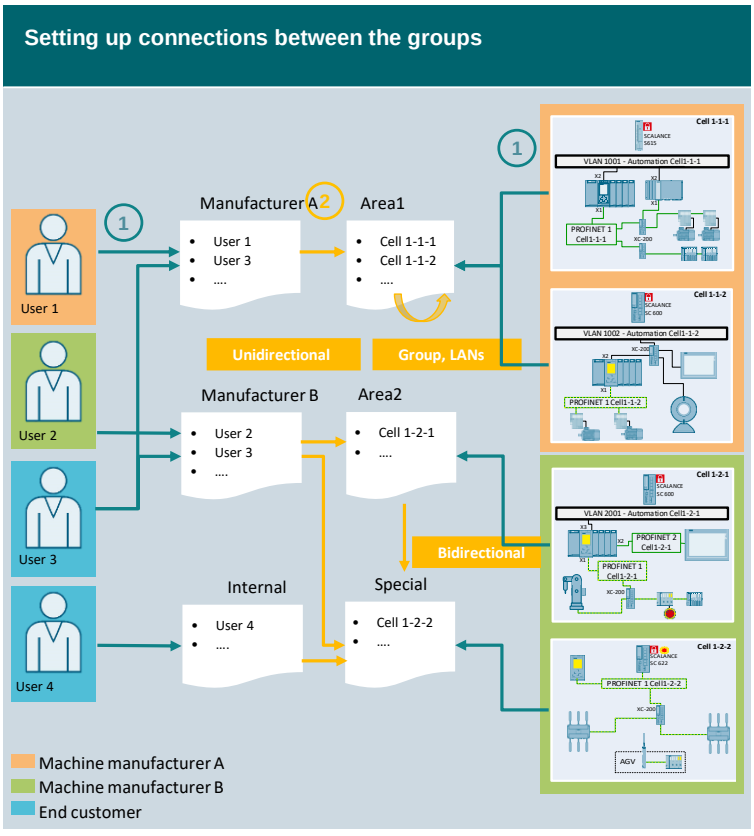
As a central management platform, the server application supports configuration of the VPN connections and endpoints as well as central user management for plant access with the help of an intuitive user interface.

SINEMA RC also makes it possible to define communication relationships in the form of groups, allowing for customized definition of permissions for users and cell networks. This way it is quick and easy to:

- Create groups and assign users or devices.



- Allow or block connections.



IP communication with NAT mechanisms

NAT (Network Address Translation) is a method of re-writing IP addresses in data packets. In this way, two different networks (internal and external) can be connected with each other. For example, serial machines with the same subnets can exist in parallel within a single network using this method.

You can select from the following NAT mechanisms:

- Without NAT

  For transparent IP communication through the OpenVPN tunnel without NAT. The devices communicating with each other always use the explicit IP address of the communication partner.

- 1:1 NAT

  The network IP address of the remote subnet is overlaid with a virtual network IP address. The network IP addresses are translated in the remote device. The host IP address remains unchanged. To address an end device in the remote subnet, the virtual IP address must be used.

- NAT for local hosts

  The IP address of the device in the remote subnet is hidden behind a dedicated IP address. The device IP addresses are translated in the remote device. To address an end device in the remote subnet, you can specify the dedicated virtual IP address.

- Source NAT in the remote subnet:

  The device to be reached in the remote subnet does not know any default gateway or has not entered the SCALANCE M/S/SC as a default gateway. The remote device can communicate through the source NAT and into the OpenVPN tunnel without a default gateway.

Note Use the NAT function of the SINEMA RC server if you want to access machines that have identical IP addresses and subnets, e.g. serial machines.

4.2.2 Implementation of SINEMA RC in the network concept

Overview

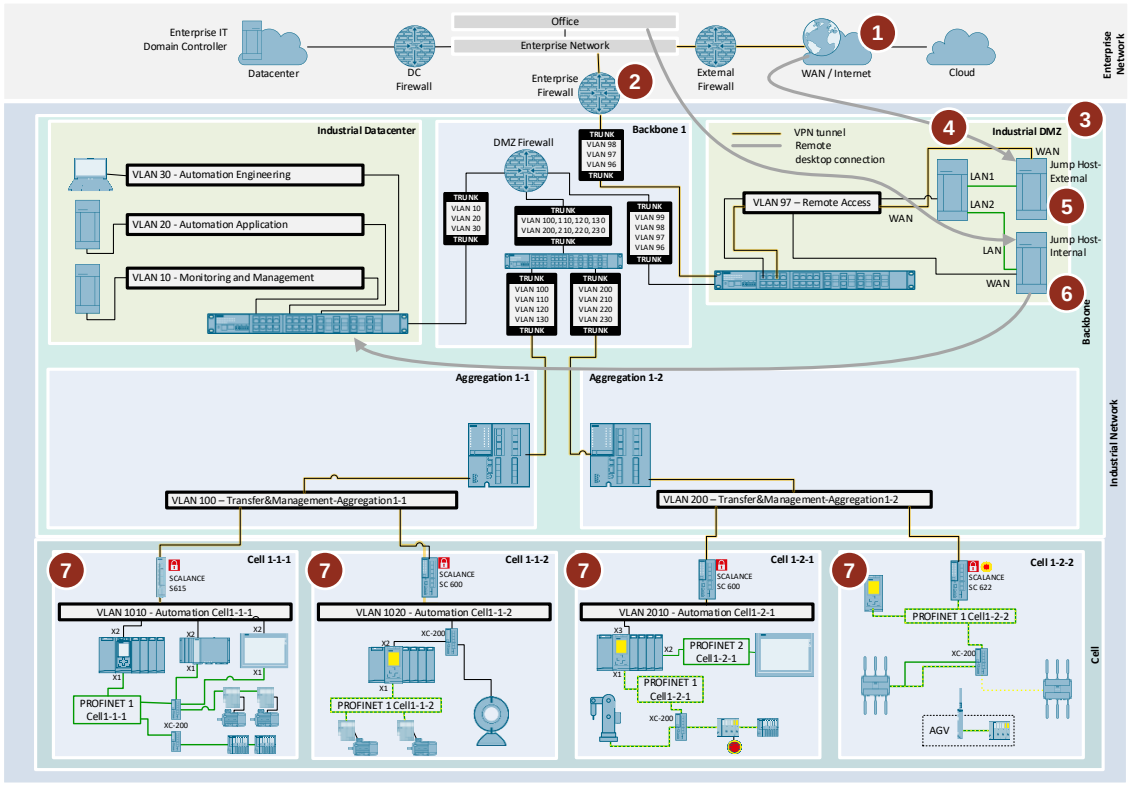
SINEMA RC and SCALANCE S615 / SC-600 in the cells are support secure remote access to the components of the cell network for maintenance, control and diagnostic purposes. The communication is protocol-independent, non-proprietary and IP-based.

Users are only permitted access to the demilitarized zone (DMZ), which implemented in the enterprise network. The VPN tunnels guard the communication links while the SINEMA RC server manages the VPN tunnels.

This prevents an external user from directly accessing the cell network without interfering with the network settings of existing nodes.

Communication between the SINEMA RC server and the remote participants is established via layer-3 VPN tunnels, taking into account the stored access rights.

Figure 4-5



The following chapters describe the functional processes and essential settings in the various SINEMA RC components in the network concept.

Table 4-1

No. in the Figure	Topic	Detail chapter
1	Access scenario from user's perspective	4.2.3
2	Configuration of external/enterprise firewall	4.2.4
3	Components in the industrial DMZ	4.2.5
4	Configuration via SINEMA RC server	4.2.6
5	Access scenario via jump host external (machine manufacturers)	4.2.7
6	Access scenario via jump host internal (service technicians)	4.2.8
7	Principle of cell protection firewall – SCALANCE S615/SC-600	4.2.9

Table 4-2 IP addresses

Component	Port	IP address
SINEMA RC server	WAN (VLAN 97)	10.0.97.10
	LAN1	10.0.91.1
	LAN2	10.0.92.1
Jump host, external	LAN	10.0.91.2
	WAN (VLAN 97)	10.0.97.20
Jump host, internal	LAN	10.0.92.2
	WAN (VLAN 97)	10.0.97.21

Component	Port	IP address
Transfer&Management-Aggregation1-1 (VLAN 100)	Physical 1	10.0.100.2
	Physical 2	10.0.100.3
	Virtual	10.0.100.1
Transfer&Management-Aggregation1-2 (VLAN 200)	Physical 1	10.0.200.2
	Physical 2	10.0.200.3
	Virtual	10.0.200.1
SCALANCE S615 (Cell 1-1-1)	WAN (VLAN 100)	10.0.100.110
SCALANCE SC600 (Cell 1-1-2)	WAN (VLAN 100)	10.0.100.120
SCALANCE SC600 (Cell 1-2-1)	WAN (VLAN 200)	10.0.200.110
SCALANCE SC622 (Cell 1-2-2)	WAN (VLAN 200)	10.0.200.120

Note

Additional detailed information on the IP addresses can be found in chapters 2.2.6 and the ones following it, as well as in Appendix V – Static routes.

4.2.3 Access scenario from user's perspective 1

The sections below describe the functional steps in the SINEMA RC system. The scenarios refer to the numbering in Figure 4-5.

Note

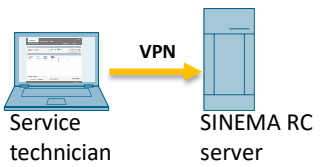
To check the time validity of certificates, it is important that the PC always has the current date and time.

Check the time on your PC and adjust it if necessary. Alternatively, you can have the system time automatically synchronized with an NTP time server. This ensures that the current time is obtained precisely.

Internal users – service technicians and automation engineers

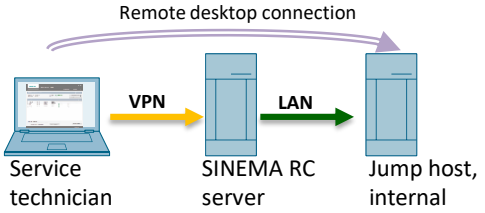
The service technician or automation engineer connects his/her PC with the internet or enterprise network.

The service technician or automation engineer launches the SINEMA Remote Connect client on his PC and uses it to establish a VPN tunnel to the SINEMA Remote Connect server (DMZ).



Thanks to its configuration setting, the SINEMA Remote Connect server gives the service technician or engineer access to its LAN interface.

The service technician or automation engineer connects with the jump host (internal) in the DMZ via a remote desktop connection on his PC.



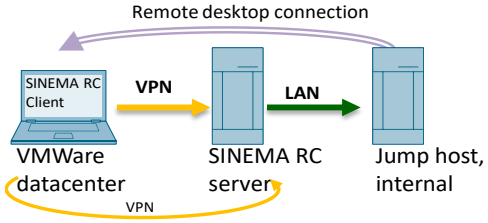
With the jump host (internal), the service technician or automation engineer connects via a remote desktop connection to a corresponding VM in the datacenter for:

- Simple tasks (e.g. downloads)

  The service technician or automation engineer can use the normal infrastructure (firewall rules without VPN) to access the cell networks.

- Critical protocols (e.g. unauthenticated access with SNMP V1, for example):

  Via the remote desktop connection, the service technician or automation engineer starts the SINEMA RC client on the VM in the datacenter (engineering station). The SINEMA RC client establishes a VPN tunnel to the SINEMA RC server .



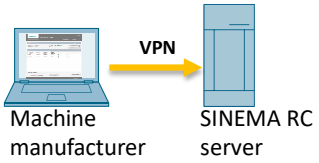
A SINEMA RC client is installed on the VMs in the datacenter for this access.

Access to the cell networks is allowed with a key-operated switch on the SCALANCE.

External users – machine manufacturers

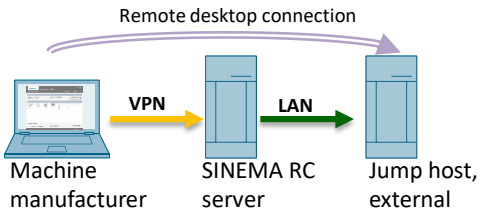
The machine manufacturer connects their PC with the internet.

The machine manufacturer launches the SINEMA Remote Connect client on their PC and uses it to establish a VPN tunnel to the SINEMA Remote Connect server (DMZ).

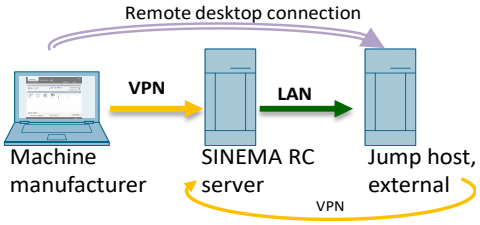


Thanks to its configuration setting, the SINEMA Remote Connect server gives the machine manufacturer access to its LAN interface.

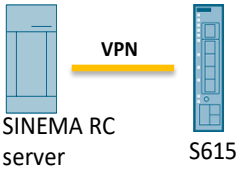
The machine manufacturer connects with the jump host (external) in the DMZ via a remote desktop connection on their PC.



Via the remote desktop connection, the machine manufacturer starts the SINEMA RC client on the jump host (external) and establishes a VPN tunnel to the SINEMA RC server.



The SINEMA RC server controls the machine manufacturer's access to the cell networks.



A SINEMA RC client is installed on the jump host (external) for this access.

Access to the cell networks is allowed with a key-operated switch on the SCALANCE.

4.2.4 Configuration of external/enterprise firewall 2

Dynamic IP address

The user connects his PC with the internet. He uses the SINEMA Remote Connect client (VPN client) for VPN access. The VPN client has WAN access to the SINEMA Remote Connect server (VPN server) via a fixed, assigned public IP address.

Request one from the provider and then store it in the DSL router.

Port forwarding

To ensure that tunnel packets can be exchanged unhindered, make sure that port forwarding for OpenVPN and HTTPS with TCP and UDP (TCP/443, UDP/1194, TCP/5443 and fallback port/6220) is allowed and that the tunnel packets are forwarded to the SINEMA Remote Connect server.

Note

These ports can be changed in the SINEMA RC server.

The port numbers are therefore only correct if you leave the settings at the default values.

For OpenVPN only UDP or TCP is used. If possible, UDP is always preferable, since UDP is faster / has better performance than TCP.

4.2.5 Components in the industrial DMZ 3

The DMZ is a neutral zone between the private network of a company and the external public network. The following servers and computer hosts are located in this DMZ:

- SINEMA RC server
- Jump host, internal for internal users (service technicians / automation engineers)
- Jump host, external for external users (machine manufacturers) with the necessary software packages and files.

Shifting the devices to the DMZ prevents external users from directly accessing a server with enterprise data.

4.2.6 Configuration via SINEMA RC server 4

Installation

Install SINEMA RC server on a PC or VM without an operating system. Note the installation requirements. You must enter the IP address of the server during the installation. Use the IP address according to Table 4-2 for this.

CAUTION	The SINEMA Remote Connect server installation includes its own operating system. If a PC is used on which an operating system is already installed, the hard disk will be formatted and all stored data will be lost.

Configuration

Configure the SINEMA RC server via the web interface (WBM):

- Define participant groups

  All members of a group belong to a single shared VPN tunnel.

  Create a device group for each cell network:
  - Cell 1-1-1 (SCALANCE S615)
  - Cell 1-1-2 (SCALANCE SC-600)
  - Cell 1-2-1 (SCALANCE SC-600)
  - Cell 1-2-2 (SCALANCE SC-600)

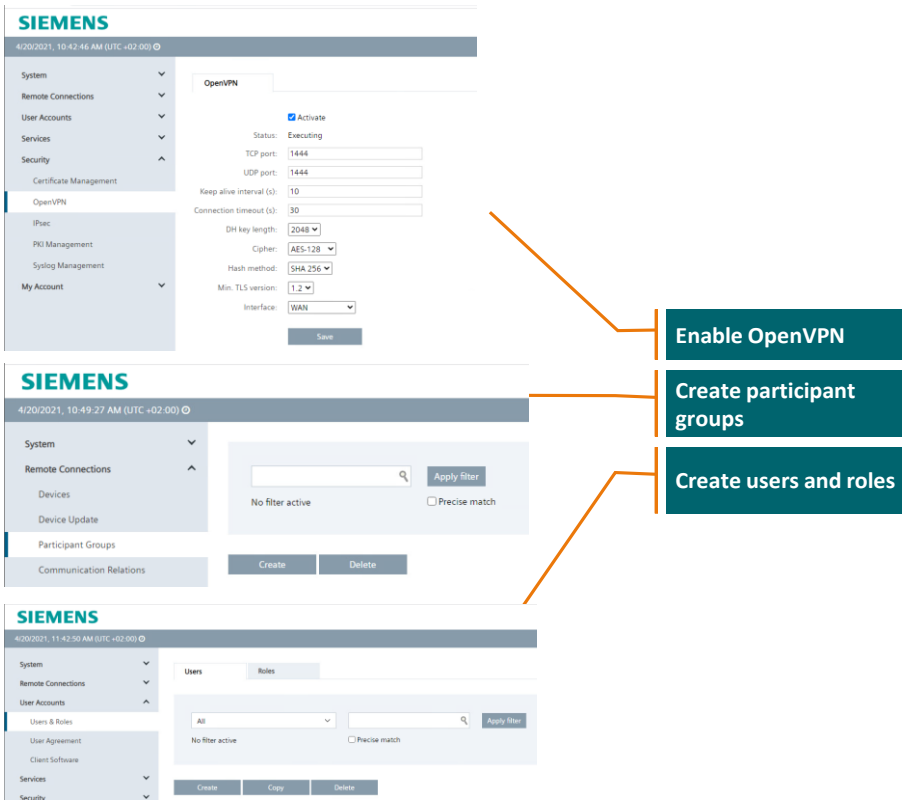
  Create the user groups for the service technician / automation engineer, the machine manufacturer and for the jump hosts (with access to LAN1 and LAN2):
  - ServicePC: User account for the service technician
  - ServiceExternal: User account for the machine manufacturer
  - Jump host, internal: User account for the jump host, internal
  - Jump host, external: User account for the jump host, external
- Implement the SCALANCE S615 or SC-600 as a device.
- Create user account for the service technician or automation engineer, machine manufacturer, jump host (internal) and jump host (external).
- Define communication relationships.
- Loading certificates and user configuration.

Note

To establish secure communication, it is essential that the current time and date are set on the SINEMA Remote Connect server. Otherwise the certificates used will be interpreted as invalid and secure VPN communication is not possible.

Depending on the configured communication relationships and the security settings, the SINEMA Remote Connect server will route between the separate VPN tunnels. Depending on the configured communication groups, the SINEMA Remote Connect server will allow its LAN interface for access to the internal network.

Figure 4-6



Interfaces

The SINEMA Remote Connect server has two physically separated interfaces on the hardware side:

- WAN interface for connecting to the external network. This interface is used for the VPN tunnels.
- LAN interface for connecting to the internal network in the DMZ (jump hosts).

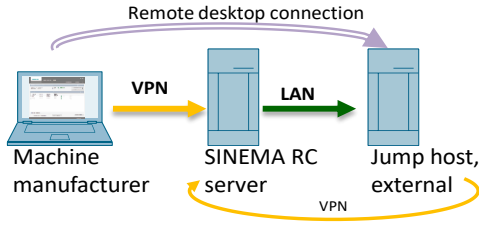
A jump host is a special-purpose computer in a network. A jump host is typically used to control or configure devices that are in a different security zone.

4.2.7 Access scenario via jump host external (machine manufacturers) 5

Various software packages can be installed on the jump host, for example:

- SINEMA Remote Connect client
- Remote desktop
- TIA Portal

Via the remote desktop connection, the machine manufacturer starts the SINEMA RC client on the jump host (external) and establishes another VPN tunnel to the SINEMA RC server and the cell. This second tunnel grants the external user secure access to the cell to perform engineering actions, for example.



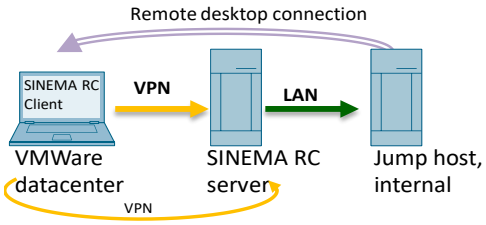
You will need a user account on the jump host for the remote desktop connection.

Create a new user account and give the user the permission for a remote desktop connection.

4.2.8 Access scenario via jump host internal (service technicians) 6

Only the remote desktop service is installed on the internal jump host.

The service technician/automation engineer connects with the jump host (internal) via a remote desktop connection, and thus to a VM (TIA Portal) in the datacenter.



You will need a user account on the jump host for the remote desktop connection.

Create a new user account and give the user the permission for a remote desktop connection.

Interfaces

The jump host has two physically separated interfaces on the hardware side:

- WAN interface for connecting to the external network. This interface is used for the VPN tunnel.
- LAN interface for connecting to the internal network in the DMZ (SINEMA RC server).

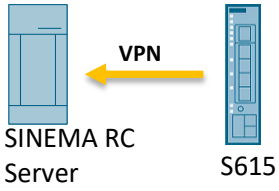
Note

You can find more information at the following link:
https://support.industry.siemens.com/cs/ww/en/view/109746841

4.2.9 Principle of cell protection firewall – SCALANCE S615/SC-600 7

The SCALANCE S615/SC-600 devices protect the cell networks thanks to their segmentation and by establishing secure communication channels. They help in setting up a flexible security concept.

The SCALANCE S615 or SC-600 devices establish a persistent or key-switch-actuated VPN tunnel to the SINEMA RC server.



The SCALANCE S615/SC-600 devices are upstream of the cell networks and protect them from unauthorized access.

Users only have access to the SCALANCE devices that have been allowed rather than to the whole subnet.

Access to the cell networks is allowed with a key-operated switch on the SCALANCE (digital input on the device).

KEY-PLUG

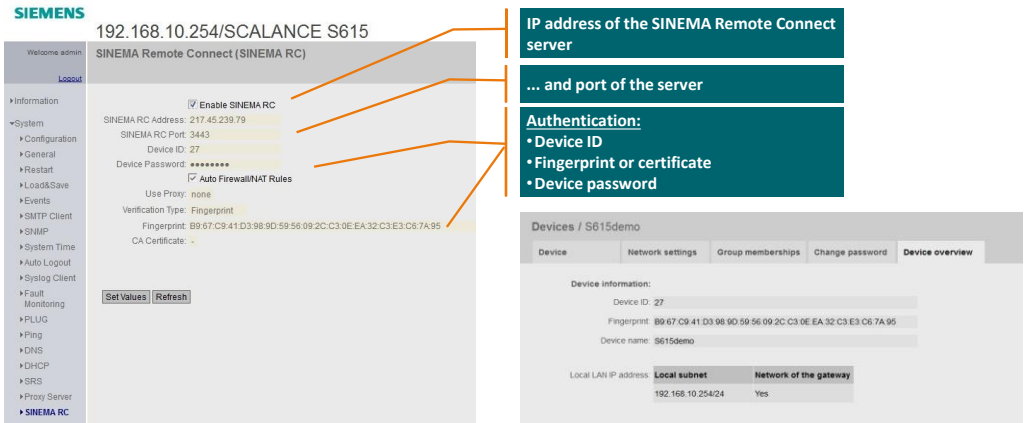
The "KEY-PLUG SINEMA REMOTE CONNECT" is required for the SCALANCE S615. The KEY-PLUG enables the SCALANCE S615 to connect to SINEMA Remote Connect. Ensure that a valid KEY-PLUG is inserted in the SCALANCE S615.

Configuration

The SCALANCE modules are configured using a web interface. The following settings are required in order to set up a VPN tunnel between the SCALANCE S615/SC600 and the SINEMA Remote Connect server:

- Initial commissioning of the SCALANCE to set basic parameters, e.g. IP address (according to Table 4-1) and clock time.
- Configure parameters for the VPN connection:
  - IP address and port of the SINEMA RC server
  - Fingerprint
  - Device ID and device password
  - Activate warning light for the VPN connection from the digital output. The warning light will illuminate as soon as the VPN tunnel to the SINEMA RC server is online.

Figure 4-7



4.3 Connecting serial machines

The use of serial machines often presents a challenge from a network standpoint. It is desirable to reuse the configuration of automation components in order to save time and effort.

For this reason, the machines are often made and delivered with identical configurations. Use of engineering software for commissioning is often undesired for labor-saving reasons.

To ensure unique addressing, the following principal approaches are possible:

1. Encapsulation of machines with NAT routers (e.g. SCALANCE S)
2. Unique addressing of components through configuration on the display or HMI
3. Automatic, unique addressing of components with DHCP and DNS standards

These variants are described in more detail below along with their advantages and disadvantages.

Note

When using X.509 certificates, changing the interface properties outside of the engineering software (especially with server services on the devices) will prevent the IP address and/or FQDN from being entered into the certificate. This should be borne in mind during certificate verification in the systems that access the corresponding communication services. If the IP address in the certificate is checked, oftentimes no connection will be possible.

The OPC UA server of the S7-1500 offers additional functionality in this regard. In this case, with TIA Portal V17 or later, a certificate with the appropriately specified IP addresses and/or FQDN can be downloaded to the CPU after commissioning with OPC UA-GDS mechanisms during runtime (\52\).

4.3.1 Encapsulation of machines with NAT routers

To guarantee reusability of a machine configuration, a router with NAT configuration can be used between the machine network and the aggregation network.

Because port forwarding must be configured for inbound connections, more configuration is required in the network components in order to ensure accessibility from machine components in higher-level networks. In addition, when device density is high, this solution entails significantly higher IP address demand in the aggregation networks. For this reason, this architecture is recommended primarily for machines with few inbound connections.

Note

If using port forwarding for inbound connections, check the compatibility of the protocols you are using.

For example, OPC UA connections require this fact to be accounted for on the client side. The following FAQ contains information on using OPC UA with NAT:
\53\ – What are the causes when connection to an OPC UA server fails?

Advantages of this solution

- The machine components retain the IP addresses configured in the TIA Portal project. (access in the cell network or via SINEMA RC requires no additional knowledge about the addressing scheme).
- Commissioning can be performed entirely by a network technician (no knowledge about the automation components necessary).

Disadvantages of this solution

- Access from higher-level networks occurs via a different IP address than in the local cell network (this can be confusing for maintenance personnel).
- Some protocols do not work with NAT, or only to a limited extent.
- Depending on the extent of the network, the need for addresses in the aggregation networks can rise significantly.

Additional information

Additional information on the concepts touched on here can be found in the following application example:

\55\ – Which NAT scenarios can you realize with SCALANCE SC-600/M-800/S615?

4.3.2 Unique addressing of components through configuration on the display or HMI

With CPU/HMI systems, there is the option of changing the IP address after the project download. Thus, if the cell protection firewall is provided by the end customer or system integrator, it is possible to modify the interface configuration of the automation components during commissioning and without any engineering software.

It is possible to carry out the interface configuration for the CPU and HMI after enabling the configuration parameter "Allow modification of IP address directly at device", for example by using system blocks, scripting, the web server, PRONETA (see \65\) or the SIMATIC Automation Tool.

With regard to the lower-level PROFINET devices, a multi-purpose I/O system can be configured. If the IP address of the PROFINET interface on the CPU should change, then the CPU will automatically re-initialize the subordinate devices to the corresponding subnet.

Note In the event of re-initialization of the PROFINET networks, address conflicts in the affected subnet must be prevented manually.

In combination with this, an HMI device can call the "T_Config" block by creating a screen for interface parameter assignment in the CPU. After the CPU interfaces are configured, suitable scripts can be used to adjust the HMI interface to fit the new subnet.

This assumes that the machine is configured with factory settings and a default subnet and that, before connecting it to higher-level networks, it has been reconfigured to use IP subnets that were agreed on with the end customer.

The configuration screens in the HMI have a certain risk of user error and should be protected with appropriate user rights.

Advantages of this solution

- All components of the machine receive their own interface configuration and are reachable from higher-level networks by means of routing.
- The configuration can be accomplished in the machine's HMI in a user-friendly manner.

Disadvantages of this solution

- Field devices that are not linked to the PROFINET I/O controller must be re-initialized in other ways.
- All stakeholders must coordinate and plan the IP subnets together.
- IP addresses of the machine do not match the IP addresses configured in TIA Portal. Therefore, they must be documented for engineering access.

Additional information

Additional information on the concepts touched on here can be found in the following application example:

\54\ – Configuring standard machines in TIA Portal (configuration control)

4.3.3 Automatic, unique addressing of components with DHCP and DNS standards

The S7-1500, WinCC Unified Panels and managed switches support automatic address assignment via DHCP.

A DHCP server in the network automatically configures the interfaces of the components connected to the network.

The following parameters are usually provided for this:

- IP address
- Subnet mask
- Default gateway
- DNS server
- NTP server

If the end customer or system integrator provides a cell firewall with DHCP and DNS server, the IP addresses can be assigned in this way even without configuration on the components.

Because in this case the IP address would not be known from the project engineering, the addressing of the components would proceed on the basis of "Fully Qualified Domain Names" (FQDN) in place of IP addresses.

The FQDNs are set in the DNS server. This can be done either automatically or manually, depending on the feature set of the cell firewall.

To automatically create a record in the DNS server, the DHCP server generally performs a "DNS update" according to RFC 2136.

The "DNS notify" mechanism per RFC 1996 or conditional DNS forwarding in the DMZ firewall can be utilized to synchronize the DNS records with a higher-level DNS server. Combining these mechanisms allows for automatic assignment as well as automatic distribution of DNS records in the network.

Advantages of this solution

- The machine's CPU and HMI receive their own interface configuration and are reachable from higher-level networks by means of routing.
- The configuration is fully automatic. Address conflicts are thereby prevented.

- Addresses are managed with common IT mechanisms (and can be centralized, depending on the extent of the network).
- The component are addressable based on their names.

Disadvantages of this solution

- The field devices in the PN network cannot be re-initialized.

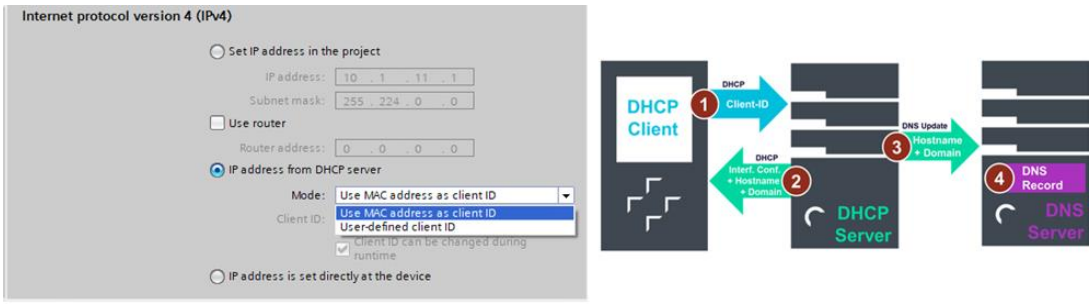
Configuration of CPUs

The CPU configuration can affect the FQDN used for the DNS records in the following way:

- **No information about hostname and FQDN in the CPU configuration**

  With the default setting, the MAC address of the CPU is applied as the DHCP client ID. To prevent issues when replacing parts, there is the alternate option of defining a custom client ID.

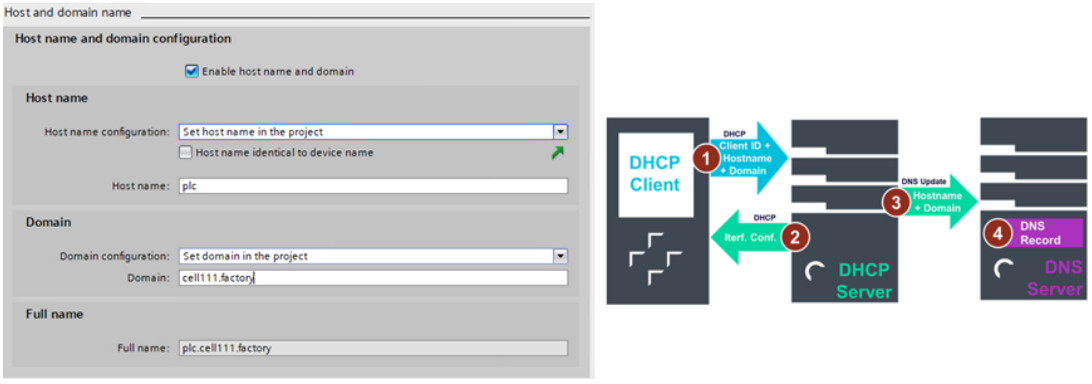
Figure 4-8



- **Complete FQDN given in the CPU configuration**

  If the complete FQDN is saved in the CPU configuration, it will be carried over in the DNS server unchanged.

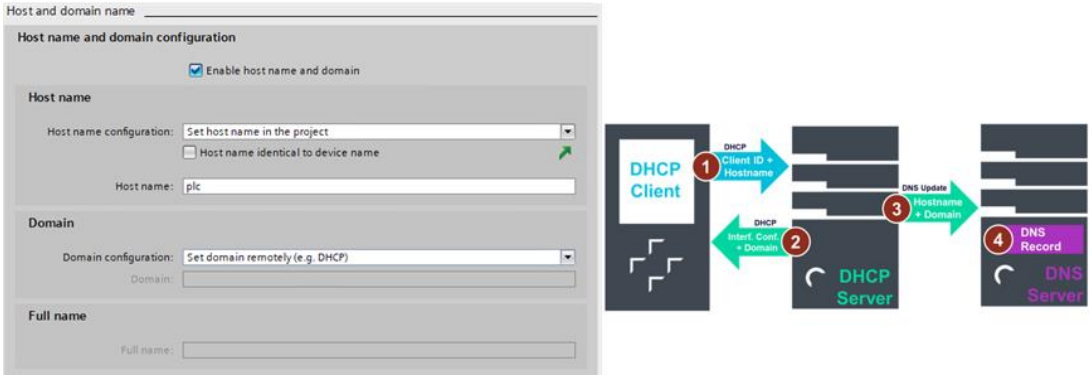
Figure 4-9



- **Hostname given in the CPU configuration**

  If just the hostname is stored in the CPU configuration, the corresponding domain in the DNS server will be expanded. With the right configuration of the domains in the DNS server, it will still be possible to distinguish serial machines by using the unique FQDNs even through the hostname is reused. This option is therefore the best option for a setup with serial machines.

Figure 4-10



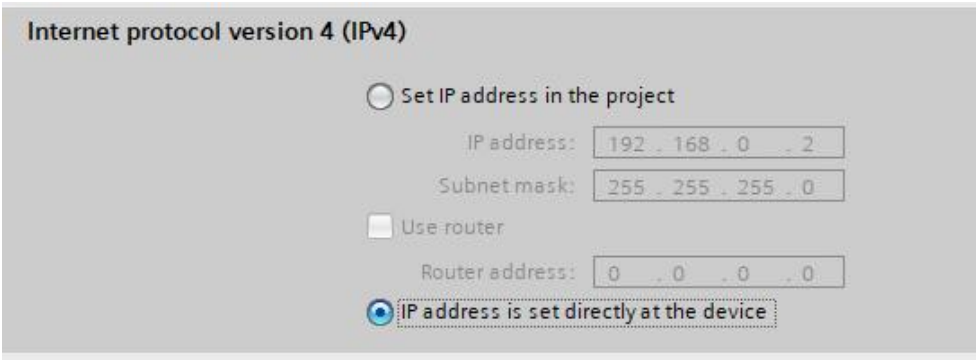
Configuration of WinCC Unified Panels

The HMI Panel is identified on the DHCP server with a non-configurable hostname that is derived from the MAC address.

In case the panel needs to be addressable with a custom FQDN, it should be manually defined in the DNS server.

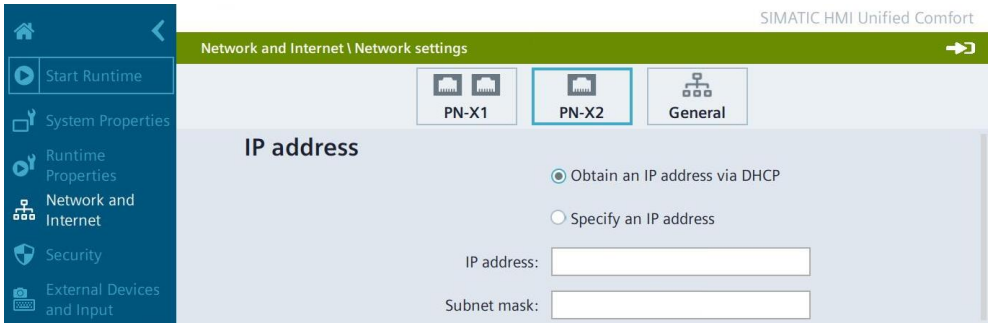
To enable DHCP on the WinCC Unified Panel, you must choose the option "Allow modification of IP address directly at device" in the configuration.

Figure 4-11



Then it will be possible to enable obtaining of addresses via DHCP in the Panel system settings.

Figure 4-12



Note

NTP server configuration is not possible via DHCP with a WinCC Unified Panel. In this case it is recommended to read the default gateway with scripts and also set it as the NTP server.

Alternatively, a higher-level NTP server that is reachable from all cells (e.g. SINEC INS) can be entered in the configuration. However, this would require additional rules in the firewall components.

Communication between HMI and CPU

Communication between HMI and CPU can only be configured on the basis of IP addresses.

If the IP address is assigned via DHCP, it is necessary to modify the connection configuration accordingly in the HMI during runtime.

This can be accomplished in the WinCC Unified Panel by using a script with the following contents:

1. A failed connection setup attempt to the CPU is used as a trigger.
2. The DNS lookup command line text
   "getent hosts *[hostname of the CPU]*" is used to find the IP address of CPU.

Note

Because the CPU is located in a local domain with the HMI, here it is sufficient to use the hostname. To ensure copyability of the configuration, in this case it will be necessary to omit the FQDN.

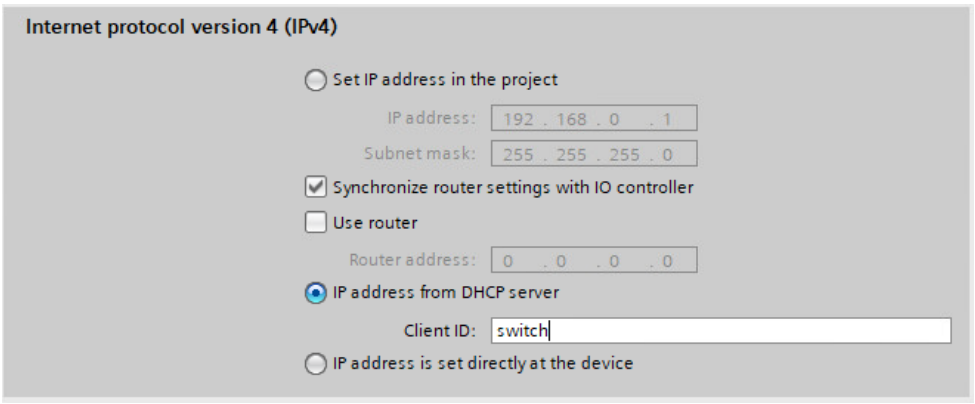
The domain configuration of the DHCP and DNS server ensures hostname-based addressability within the cell (e.g. "CPU").
The FQDN (e.g. "CPU.cell111.factory") is only used for access outside of the cell.

3. The IP address gained from the DNS lookup command is entered in the HMI-to-CPU connection using the system function "ChangeConnection()".
4. The HMI establishes the connection to the CPU.

Configuration of switches in the Automation-Cell subnets

The interface configuration of the switches in the Automation-Cell subnets can likewise be made using DHCP. Here, a corresponding client ID can be entered in the configuration. In this case, the DHCP server must be configured such that the client ID is used as the hostname for updating the DNS server. We recommend configuring switches that are located in the PROFINET networks below the CPUs as PROFINET devices. In this way, the interface configuration is managed by the CPU just like it is with the I/O devices.

Figure 4-13



Configuration of PROFINET networks

The PROFINET subnet is made flexible through the use of a multiple-use I/O system.

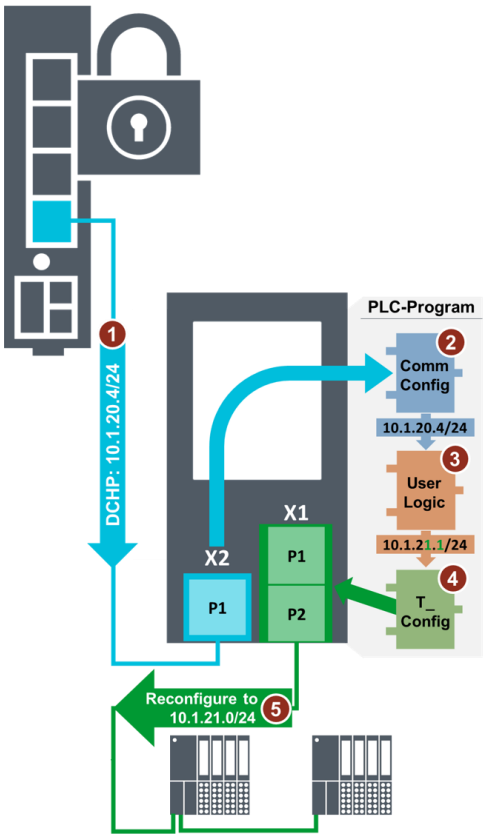
More information on this topic can be found in the following application example:
\54\ – Configuring standard machines in TIA Portal (configuration control)

In this network concept, 10 subnets are reserved for each of the cells. Thus, there is usually sufficient address space available for the configuration of multiple PROFINET subnets.

By using the "CommConfig" system function of the S7-1500, it is possible to read the IP address (obtained via DHCP) of the interface in the Automation-Cell subnet. Then, the next subnet can be calculated from the IP address and subnet mask. The first IP address of this subnet is then assigned to the PROFINET interface with the help of the "T_Config" system function. The multiple-use I/O system gives all lower-level devices IP addresses from the corresponding subnet.

The procedure is explained using the example of cell 1-2-1 as follows:

Figure 4-14



1. The X2 interface of the CPU is assigned an IP address from subnet 10.1.20.0/24 via DHCP.
2. The CPU program reads the configuration of the X2 interface.
3. The associated program logic calculates the configuration of the X1 interface.
4. The calculated configuration is now assigned to the X2 interface.
5. By reconfiguring the multiple-use I/O system, all devices on the CPU have now been re-initialized accordingly.

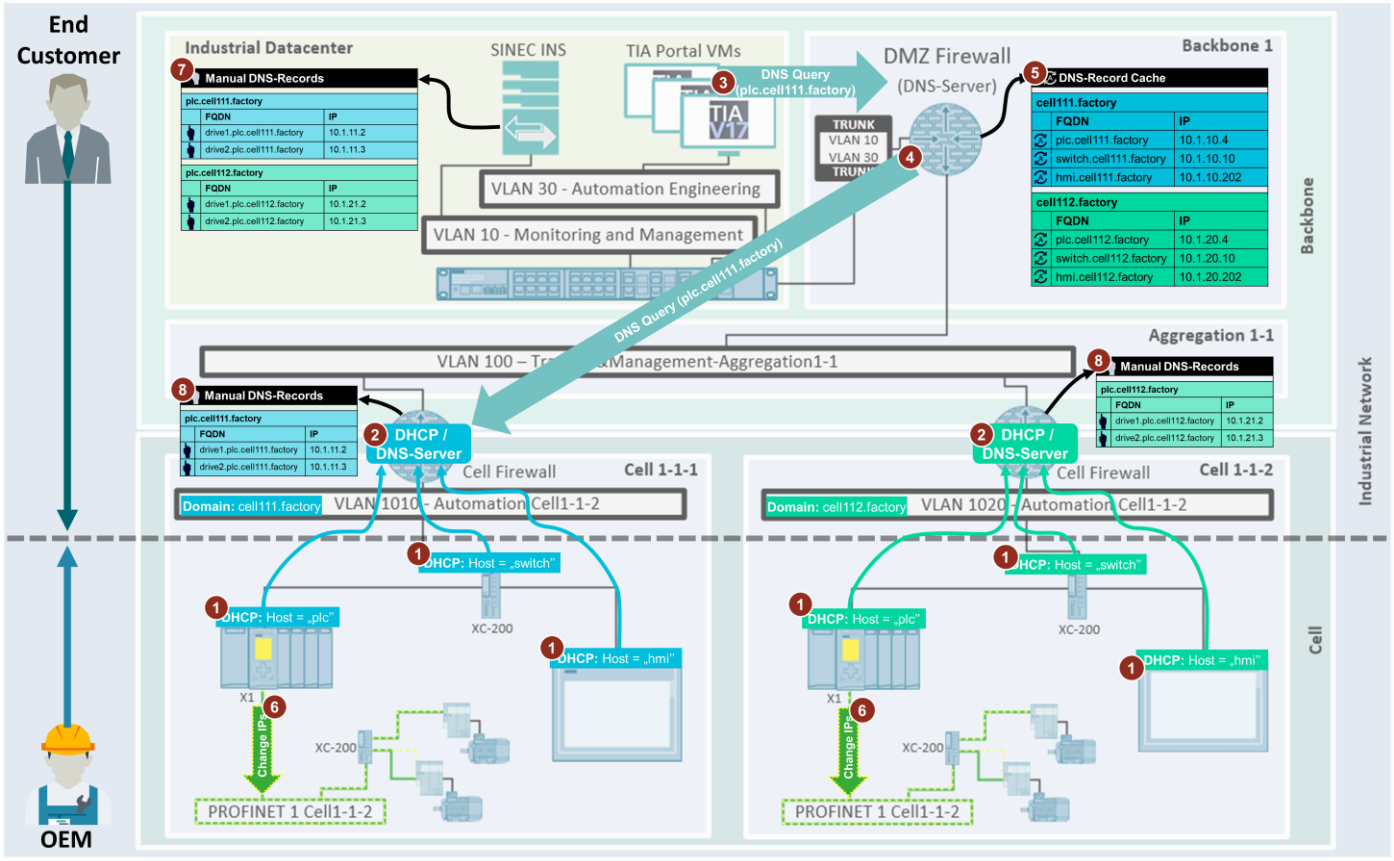
Note

The S7-1500 does not support routing protocols, so it cannot inform the router of the lower-level subnets. In case the PROFINET devices of higher-level subnets (e.g. aggregation or datacenter) need to be reachable, the appropriate routes must be created in the cell protection firewall and the "IP forwarding" function must be enabled in the PLC (see chapter 2.2.6 and following).

Architecture in the network concept

The use cases described above are summarized in an architecture diagram as follows.

Figure 4-15



The Figure shows two cells (Cell1-1-2 and Cell1-1-2) which are completely identical with respect to their components and configuration.

1. The automation components supplied by the OEM obtain their interface configuration from the cell protection firewalls, which are managed by the end customer.
2. The firewalls are located in different DNS zones. After the DHCP leases are created, they send the corresponding FQDNs to their integrated DNS server.
3. When the DMZ firewall receives a query for a record in the corresponding cell domain,
4. it queries the associated cell protection firewall based on forwarding rules.
5. Caching is employed in the DMZ firewall to reduce query volume.
6. The PROFINET subnets are configured by the CPU based on the subnet that is assigned to the X2 interface. Follow an appropriate scheme here to prevent conflicts in address assignment (see chapter 2.2.5). To guarantee FQDN-based reachability, DNS records can be created for PROFINET devices manually.
7. This can be done, for example, either centrally in the DNS configuration of SINEC INS, or
8. in a distributed manner in the DNS configuration of the cell protection firewalls.
   Distributed configuration has the advantage that only the hostname is necessary for addressing within the cell.
   If the records are created centrally, addressing must always be done with the FQDN (hostname + domain).

Based on the name-based addressing architecture demonstrated here, manual handling of IP addresses for the machine suppliers becomes completely superfluous. The ability of the components to reach each other is guaranteed by the routes defined in chapter 2.2.5. This is ultimately how coordination effort between supplier and end customer can be reduced to a minimum.

Configuration of the network components

The DHCP and DNS servers mapped on the cell level are usually integrated in the cell firewalls. To guarantee seamless operation of the DNS infrastructure, all DNS servers should have the ability to communicated with one another on TCP and UDP port 53. Refer to chapter 2.6.5 for the corresponding firewall configuration.

The following DNS forwarding rules are necessary to direct the DNS queries going from the DMZ firewall to the cell protection firewalls:

Table 4-3

Domain	DNS server
cell111.factory	Firewall-Cell1-1-1 *10.0.100.110*
cell112.factory	Firewall-Cell1-1-2 *10.0.100.120*
cell121.factory	Firewall-Cell1-2-1 *10.0.200.110*
cell122.factory	Firewall-Cell1-2-2 *10.0.200.120*

Note

At present, only manually defined DNS records are supported in the SCALANCE and SINEC portfolio. When using static leases, DHCP is however better suited for rapid commissioning of serial machines while avoiding address conflicts. After the IP addresses have been assigned with DHCP, associated DNS records can be created by hand in the DNS settings of the SCALANCE S components.

In case the DNS records need to be created in the cell protection firewalls automatically, the use of Palo Alto firewalls is recommended at the cell transition as well.

5 Technical appendix

5.1 Appendix I – Firewall rules for Industrial Edge

For the functioning of the Industrial Edge ecosystem, it is recommended to allow the connections described below, using the architecture with DNS-based configuration (as described in chapter 3.14) as a guide.

5.1.1 DMZ firewall

Table 5-1

Source	Destination	Destination port	Use
Industrial Edge Management *10.0.20.10*	Proxy server *10.0.98.20*	TCP 443	HTTPS connections to Industrial Edge Hub ***URLs:*** \66\
		TCP 2020	SSH service tunnel to Industrial Edge Hub ***URL:*** \67\
Industrial Edge-Device Cell1-1-1 *10.1.10.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server
Industrial Edge-Device Cell1-1-2 *10.1.20.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server
Industrial Edge-Device Cell1-2-1 *10.2.11.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server
Industrial Edge-Device Cell1-2-2 *10.2.20.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server

5.1.2 Cell1-1-1 firewall

Table 5-2

Source	Destination	Destination port	Use
Industrial Edge-Device Cell1-1-1 *10.1.10.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server

5.1.3 Cell1-1-2 firewall

Table 5-3

Source	Destination	Destination port	Use
Industrial Edge-Device Cell1-1-2 *10.1.20.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server

5.1.4 Cell1-2-1 firewall

Table 5-4

Source	Destination	Destination port	Use
Industrial Edge-Device Cell1-2-1 *10.2.11.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server

5.1.5 Cell1-2-2 firewall

Table 5-5

Source	Destination	Destination port	Use
Industrial Edge-Device Cell1-2-2 *10.2.20.201*	Industrial Edge Management *10.0.20.10*	TCP 443	HTTPS access from the IED to the IEM
		TCP 32500	SSH tunnel from the IED to the IEM

Source	Destination	Destination port	Use
	Proxy server *10.0.98.20*	TCP 443	HTTPS access from the IED to the proxy server
		TCP 1883, 8883	MQTT access from the IED to the proxy server

5.2 Appendix II – SINEC NMS connections

The following firewall rules must be put in place for network monitoring between SINEC NMS Control and Operation.

Table 5-6

From	To	Port	Protocol	Service
Control	Operation	8443	TCP	HTTPS (web server)
Control	Operation	5671	TCP	Data exchange (RabbitMQ)
Control	Operation	49131	TCP	Firmware update file synchronization (SFTP)
Operation	Control	443	TCP	HTTPS (web server)
Operation	Control	5671	TCP	Data exchange (RabbitMQ)
Operation	Control	49113	TCP	Heartbeat (reachability test)
Operation	Control	49114	TCP	Version check

The following firewall rules must be put in place for network monitoring between Operation and device.

Table 5-7

From	To	Port	Protocol	Service
Operation	Device	161	UDP	SNMP polling
Operation	Device	102	TCP	SIMATIC diagnostics
Operation	Device	ICMP Echo request.	IP service	Network scan
Operation	Device	22	TCP	SSH connection
Operation	Device	34,964 & 49,152 to 65,535	UDP	PROFINET diagnostics
Operation	Device	443	TCP	Backup/restore config
Device	Operation	162	UDP	SNMP Traps
Device	Operation	69	UDP	Firmware update (TFTP)

5.3 Appendix III – UMC firewall rules

The following firewall configuration is recommended for the operation of central user management with UMC:

5.3.1 DMZ firewall

General requirement

In principle, all PC stations with UMC ring server, UMC server or UMC runtime server should be integrated into the Microsoft Active Directory of the domain controller. The rules required for the VMs, PC stations and Field PGs are already listed in the associated chapters. The following rules apply for the connection of the dedicated UMC stations:

Table 5-8

Source	Destination	Destination port	Use
UMC primary/secondary ring server *10.0.10.121* *10.0.10.122* UMC server in the Automation-Engineering subnet *10.0.30.20* Application server in the Transfer&Management-Aggregation subnets *10.0.100.100* *10.0.200.100*	Domain controller *10.0.98.10*	TCP/UDP 389	LDAP
		TCP 636	LDAP SSL
		TCP 3268	LDAP GC
		TCP 3269	LDAP GC SSL
Note: This Table only considers the Active Directory services necessary for UMC. Additional communication connections are required for the operation of PCs in the Active Directory group. For more details, please refer to the following Microsoft article: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts			

Rules for systems in the backbone level

Table 5-9

Source	Destination	Destination port	Use
UMC server in the Automation-Engineering subnet *10.0.30.20*	UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	TCP 4002	Synchronization and authentication

Source	Destination	Destination port	Use
UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	UMC server in the Automation-Engineering subnet *10.0.30.20*	TCP 4002	Synchronization and authentication
WinCC server *10.0.20.20*	UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	TCP 4002	Synchronization and authentication
UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	WinCC server *10.0.20.20*	TCP 4002	Synchronization and authentication
SINEC NMS Control *10.0.10.111*	UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	TCP 443	Synchronization and authentication
UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	SINEC NMS Control *10.0.10.111*	TCP 4002	Synchronization and authentication
SINEC INS *10.0.10.110*	UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	TCP 443	Synchronization and authentication
SINEMA RC server *10.0.97.10*	UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	TCP 443	Synchronization and authentication
Network components in the DMZ *10.0.99.10 to 10.0.99.99*	SINEC INS *10.0.10.110*	UDP 1812	Access from the network components in the DMZ to the SINEC INS RADIUS server

Rules for systems in the aggregation level

Table 5-10

Source	Destination	Destination port	Use
UMC server in the Transfer&Management-Aggregation subnets *10.0.100.100* *10.0.200.100*	UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	TCP 4002	Synchronization and authentication
UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	UMC server in the Transfer&Management-Aggregation subnets *10.0.100.100* *10.0.200.100*	TCP 4002	Synchronization and authentication
Field PGs in the WLAN-Engineering-Automation subnets *10.0.130.0/24* *10.0.230.0/24*	UMC server in the Automation-Engineering subnet *10.0.30.20*	TCP 4002	Synchronization and authentication
UMC server in the Automation-Engineering subnet *10.0.30.20*	Field PGs in the WLAN-Engineering-Automation subnets *10.0.130.0/24* *10.0.230.0/24*	TCP 4002	Synchronization and authentication
Network components in the aggregation level *10.0.100.10 to 10.0.100.99* *10.0.200.10 to 10.0.200.99*	SINEC INS *10.0.10.110*	UDP 1812	Access from the network components in the aggregation level to the SINEC INS RADIUS server
WLAN-Engineering-Aggregation subnets *10.0.130.0/24* *10.0.230.0/24*	UMC ring server (Primary, Secondary, Cluster) *10.0.10.120* *10.0.10.121* *10.0.10.122*	TCP 443	Configuration access from Field PGs in the aggregation level to the web interface of the UMC ring servers

Rules for systems in the cell level:

Table 5-11

Source	Destination	Destination port	Use
Field PGs in Automation-Cell subnets (DHCP range) *10.1.10.201 to 10.1.10.254* *10.1.20.201 to 10.1.20.254* *10.2.10.201 to 10.2.10.254* *10.2.20.201 to 10.2.20.254*	UMC server in the Automation-Engineering subnet *10.0.30.20*	TCP 4002	Synchronization and authentication
UMC server in the Automation-Engineering subnet *10.0.30.20*	Field PGs in Automation-Cell subnets (DHCP range) *10.1.10.201 to 10.1.10.254* *10.1.20.201 to 10.1.20.254* *10.2.10.201 to 10.2.10.254* *10.2.20.201 to 10.2.20.254*	TCP 4002	Synchronization and authentication
Network components in the cell level *10.1.10.10 to 10.1.10.99* *10.1.20.10 to 10.1.20.99* *10.2.10.10 to 10.2.10.99*	SINEC INS *10.0.10.110*	UDP 1812	Access from the network components in the cell level to the SINEC INS RADIUS server

5.3.2 Cell1-1-1 firewall

Table 5-12

Source	Destination	Destination port	Use
Field PGs in Automation Cell1-1-1 subnet (DHCP range) *10.1.10.201 to 10.1.10.254*	UMC server in the Automation-Engineering subnet *10.0.30.20*	TCP 4002	Synchronization and authentication
UMC server in the Automation-Engineering subnet *10.0.30.20*	Field PGs in Automation Cell1-1-1 subnet (DHCP range) *10.1.10.201 to 10.1.10.254*	TCP 4002	Synchronization and authentication
WinCC Unified Panel *10.1.10.201*	UMC server in the Transfer&Management-Aggregation1-1 subnet *10.0.100.100*	TCP 443	HTTPS communication to the UMC server on the aggregation level
Network components in the cell *10.1.10.10 to 10.1.10.99*	SINEC INS *10.0.10.110*	UDP 1812	Access from the network components in the cell to the SINEC INS RADIUS server

5.3.3 Cell1-1-2 firewall

Table 5-13

Source	Destination	Destination port	Use
Field PGs in Automation Cell1-1-2 subnet (DHCP range) *10.1.20.201 to 10.1.20.254*	UMC server in the Automation-Engineering subnet *10.0.30.20*	TCP 4002	Synchronization and authentication
UMC server in the Automation-Engineering subnet *10.0.30.20*	Field PGs in Automation Cell1-1-2 subnet (DHCP range) *10.1.20.201 to 10.1.20.254*	TCP 4002	Synchronization and authentication
Network components in the cell *10.1.20.10 to 10.1.20.99*	SINEC INS *10.0.10.110*	UDP 1812	Access from the network components in the cell to the SINEC INS RADIUS server

5.3.4 Cell1-2-1 firewall

Table 5-14

Source	Destination	Destination port	Use
Field PGs in Automation Cell1-2-1 subnet (DHCP range) *10.2.10.201 to 10.2.10.254*	UMC server in the Automation-Engineering subnet *10.0.30.20*	TCP 4002	Synchronization and authentication
UMC server in the Automation-Engineering subnet *10.0.30.20*	Field PGs in Automation Cell1-2-1 subnet (DHCP range) *10.2.10.201 to 10.2.10.254*	TCP 4002	Synchronization and authentication
WinCC Comfort Panel *10.2.11.202*	UMC server in the Transfer&Management-Aggregation1-2 subnet *10.0.200.100*	TCP 16389	SIMATIC Logon communication to the UMC server in the aggregation level
Network components in the cell *10.2.10.10 to 10.2.10.99*	SINEC INS *10.0.10.110*	UDP 1812	Access from the network components in the cell to the SINEC INS RADIUS server

5.4 Appendix IV – Subnets

The following Table shows a possible subnet configuration for this concept, including example IP addresses.

As a rule and regardless of whether redundancy is employed, three IP addresses are reserved for routing.

In case of redundant routing, all gateway addresses are needed. The first address in this case receives the frames to be routed. If the routing does not need to be redundant, the first address is used and address assignment is standardized with the empty addresses with the aim of making it possible for any gateway to be laid out redundantly later on.

With an enterprise firewall and DMZ firewall in the DMZ, this concept provides for two routers. Thus, six IP addresses are needed for routing for this zone.

Table 5-15

Designation		VLAN	IP subnet	Example systems
Datacenter	Monitoring & Management	10	Subnet address: 10.0.10.0/24 Gateway addresses: 10.0.10.1 – 10.0.10.3 Broadcast address: 10.0.10.255 DHCP range: 10.0.10.201 – 10.0.10.254	• SINEC INS • SINEC NMS Control • UMC ring server • Switches and routers in the datacenter • Management interfaces of server systems
	Automation application	20	Subnet address: 10.0.20.0/24 Gateway addresses: 10.0.20.1 – 10.0.20.3 Broadcast address: 10.0.20.255 DHCP range: 10.0.20.201 – 10.0.20.254	• WinCC server • MES server • MOM server
	Automation Engineering	30	Subnet address: 10.0.30.0/24 Gateway addresses: 10.0.30.1 – 10.0.30.3 Broadcast address: 10.0.30.255 DHCP range: 10.0.30.201 – 10.0.30.254	• TIA Portal • Web browser Engineering tools

Designation		VLAN	IP subnet	Example systems
DMZ	Management DMZ	99	Subnet address: 10.0.99.0/24 Gateway addresses: 10.0.99.1 – 10.0.99.6 Broadcast address: 10.0.99.255 DHCP range: 10.0.99.201 – 10.0.99.254	• Switches in the DMZ • Management interfaces of server systems
	Data Forwarding	98	Subnet address: 10.0.98.0/24 Gateway addresses: 10.0.98.1 – 10.0.98.6 Broadcast address: 10.0.98.255 DHCP range: 10.0.98.201 – 10.0.98.254	• Proxy server • Domain controller
	Remote access	97	Subnet address: 10.0.97.0/24 Gateway addresses: 10.0.97.1 – 10.0.97.6 Broadcast address: 10.0.97.255 DHCP range: 10.0.97.201 – 10.0.97.254	• SINEMA Remote Connect • Jump hosts for remote access
	Update services	96	Subnet address: 10.0.96.0/24 Gateway addresses: 10.0.96.1 – 10.0.96.6 Broadcast address: 10.0.96.255 DHCP range: 10.0.96.201 – 10.0.96.254	• WSUS server Virus pattern server
	SINEMA RC LAN1 – jump host - internal	91	Subnet address: 10.0.91.0/24 Gateway address: 10.0.91.1 Broadcast address: 10.0.91.255	Subnet for coupling between SINEMA RC and jump host
	SINEMA RC LAN2 – jump host - external	92	Subnet address: 10.0.92.0/24 Gateway address: 10.0.92.1 Broadcast address: 10.0.92.255	Subnet for coupling between SINEMA RC and jump host

Designation		VLAN	IP subnet	Example systems
Aggregation1-1	Transfer&Management-Aggregation1-1	100	Subnet address: 10.0.100.0/24 Gateway addresses: 10.0.100.1 – 10.0.100.3 Broadcast address: 10.0.100.255 DHCP range: 10.0.100.201 – 10.0.100.254	• Uplink, interface of the cell firewalls • SINEC NMS Operation • UMC server
	Automation-Aggregation1-1	110	Subnet address: 10.0.110.0/24 Gateway addresses: 10.0.110.1 – 10.0.110.3 Broadcast address: 10.0.110.255 DHCP range: 10.0.110.201 – 10.0.110.254	• Thin clients (HMI)
	WLAN-Automation-Aggregation1-1	120	Subnet address: 10.0.120.0/24 Gateway addresses: 10.0.120.1 – 10.0.120.3 Broadcast address: 10.0.120.255 DHCP range: 10.0.120.201 – 10.0.120.254	• AGVs (non realtime) • Tablets • Smart watches • Laptops

Designation		VLAN	IP subnet	Example systems
	WLAN-Engineering-Aggregation1-1	130	Subnet address: 10.0.130.0/24 Gateway addresses: 10.0.130.1 – 10.0.130.3 Broadcast address: 10.0.130.255 DHCP range: 10.0.130.201 – 10.0.130.254	Field PGs
Aggregation1-2	Transfer&Management-Aggregation1-2	200	Subnet address: 10.0.200.0/24 Gateway addresses: 10.0.200.1 – 10.0.200.3 Broadcast address: 10.0.200.255 DHCP range: 10.0.200.201 – 10.0.200.254	• Uplink, interface of the cell firewalls • SINEC NMS Operation • UMC server
	Automation-Aggregation1-2	210	Subnet address: 10.0.210.0/24 Gateway addresses: 10.0.210.1 – 10.0.210.3 Broadcast address: 10.0.210.255 DHCP range: 10.0.210.201 – 10.0.210.254	• Thin clients (HMI)

Designation		VLAN	IP subnet	Example systems
	WLAN-Automation-Aggregation1-2	220	Subnet address: 10.0.220.0/24 Gateway addresses: 10.0.220.1 – 10.0.220.3 Broadcast address: 10.0.220.255 DHCP range: 10.0.220.201 – 10.0.220.254	• AGVs (non realtime) • Tablets • Smart watches • Laptops
	WLAN-Engineering-Aggregation1-2	230	Subnet address: 10.0.230.0/24 Gateway addresses: 10.0.230.1 – 10.0.230.3 Broadcast address: 10.0.230.255 DHCP range: 10.0.230.201 – 10.0.230.254	• Field PGs
Cell1-1-1	Automation Cell1-1-1	1010	Subnet address: 10.1.10.0/24 Gateway addresses: 10.1.10.1 – 10.1.10.3 Broadcast address: 10.1.10.255 DHCP range: 10.1.10.201 – 10.1.10.254	• CPUs • Edge devices • HMI Panels
	PROFINET 1 Cell1-1-1	none	Subnet address: 10.1.11.0/24 Gateway addresses: 10.1.11.1 – 10.1.11.3 Broadcast address: 10.1.11.255	• CPUs • PROFINET devices

Designation		VLAN	IP subnet	Example systems
Cell1-1-2	Automation Cell1-1-2	1020	Subnet address: 10.1.20.0/24 Gateway addresses: 10.1.20.1 – 10.1.20.3 Broadcast address: 10.1.20.255 DHCP range: 10.1.20.201 – 10.1.20.254	• CPUs • Edge devices • HMI Panels
	PROFINET 1 Cell1-1-2	none	Subnet address: 10.1.21.0/24 Gateway addresses: 10.1.21.1 – 10.1.21.3 Broadcast address: 10.1.21.255	• CPUs • PROFINET devices

Designation		VLAN	IP subnet	Example systems
Cell1-2-1	Automation Cell1-2-1	2010	Subnet address: 10.2.10.0/24 Gateway addresses: 10.2.10.1 – 10.2.10.3 Broadcast address: 10.2.10.255 DHCP range: 10.2.10.201 – 10.2.10.254	• CPUs • Edge devices
	PROFINET 1 Cell1-2-1	none	Subnet address: 10.2.11.0/24 Gateway addresses: 10.2.11.1 – 10.2.11.3 Broadcast address: 10.2.11.255	• CPUs • HMI Panels
	PROFINET 2 Cell1-2-1	none	Subnet address: 10.2.12.0/24 Gateway addresses: 10.2.12.1 – 10.2.12.3 Broadcast address: 10.2.12.255	• CPUs • PROFINET devices
Cell1-2-2	Automation Cell1-2-2	none	Subnet address: 10.2.20.0/24 Gateway addresses: 10.2.20.1 – 10.2.20.1 Broadcast address: 10.2.20.255	• CPUs • HMI Panels • PROFINET devices • Edge devices

5.5 Appendix V – Static IP addresses

The Tables below provide an overview of the components mentioned throughout this document that have statically assigned IP addresses.

5.5.1 Monitoring and Management subnet (10.0.10.0/24)

Table 5-16

IP address	Component
10.0.10.1 to 10.0.10.3	Router (redundancy)
10.0.10.10 to 10.0.10.99	Network components (switches)
10.0.10.110	SINEC INS (DNS, NTP, RADIUS server)
10.0.10.111	SINEC NMS Control
10.0.10.120	Cluster IP of the UMC ring server
10.0.10.121	UMC priority ring server
10.0.10.122	UMC secondary ring server

5.5.2 Subnet Automation-Application (10.0.20.0/24)

Table 5-17

IP address	Component
10.0.20.1 to 10.0.20.3	Router (redundancy)
10.0.20.10	Industrial Edge Management
10.0.20.20	WinCC server system (WinCC V7.x, WinCC RT Prof., WinCC Unified PC RT)
10.0.20.2122	WinCC terminal server OPC UA client

5.5.3 Automation-Engineering subnet (10.0.30.0/24)

Table 5-18

IP address	Component
10.0.30.1 to 10.0.30.3	Router (redundancy)
10.0.30.10	TIA project/license server
10.0.30.20	UMC server for engineering
10.0.30.100 to 10.0.30.200	Engineering VMs in the datacenter with static IP addresses

5.5.4 Management-DMZ subnet (10.0.99.0/24)

Table 5-19

IP address	Component
10.0.99.1 to 10.0.99.6	Routers (redundancy, DMZ firewall and enterprise firewall)
10.0.99.10 to 10.0.99.99	Network components (switches)

5.5.5 Data-Forwarding subnet (10.0.98.0/24)

Table 5-20

IP address	Component
10.0.98.1 to 10.0.98.6	Routers (redundancy, DMZ firewall and enterprise firewall)
10.0.98.10	Microsoft Active Directory domain controller
10.0.98.20	Proxy server

5.5.6 Remote-Access subnet (10.0.97.0/24)

Table 5-21

IP address	Component
10.0.97.1 to 10.0.97.6	Routers (redundancy, DMZ firewall and enterprise firewall)
10.0.97.10	SINEMA Remote Connect server
10.0.97.20	Jump server for remote access

5.5.7 Update-Services subnet (10.0.96.0/24)

Table 5-22

IP address	Component
10.0.96.1 to 10.0.96.6	Routers (redundancy, DMZ firewall and enterprise firewall)

5.5.8 Transfer&Management-Aggregation1-1 subnet (10.0.100.0/24)

Table 5-23

IP address	Component
10.0.100.1 to 10.0.100.3	Router (redundancy)
10.0.100.10 to 10.0.100.99	Network components (switches, WLAN APs/clients)
10.0.100.100	Transfer&Management-Aggregation1-1 application server (SINEC NMS Operation + UMC server)

5.5.9 Automation-Aggregation1-1 subnet (10.0.110.0/24)

Table 5-24

IP address	Component
10.0.110.1 to 10 to 10.0.110.3	Router (redundancy)
10.0.110.10	WinCC client stations (WebNavigator, WebUx, Unified Client, thin clients)
10.0.110.201	Industrial Edge device Aggregation1-1

5.5.10 WLAN-Automation-Aggregation1-1 subnet (10.0.120.0/24)

Table 5-25

IP address	Component
10.0.120.1 to 10.0.120.3	Router (redundancy)

5.5.11 WLAN-Engineering-Aggregation1-1 subnet (10.0.130.0/24)

Table 5-26

IP address	Component
10.0.130.1 to 10.0.130.3	Router (redundancy)
10.0.130.0/24	Field PGs

5.5.12 Transfer&Management-Aggregation1-2 subnet (10.0.200.0/24)

Table 5-27

IP address	Component
10.0.200.1 to 10.0.200.3	Router (redundancy)
10.0.200.10 to 10.0.200.99	Network components (switches, WLAN APs/clients)

IP address	Component
10.0.200.100	Transfer&Management-Aggregation1-2 application server (SINEC NMS Operation + UMC server)

5.5.13 Automation-Aggregation1-2 subnet (10.0.210.0/24)

Table 5-28

IP address	Component
10.0.210.1 to 10.0.210.3	Router (redundancy)
10.0.210.10	WinCC Unified runtime station
10.0.210.201	Industrial Edge device Aggregation 1-2

5.5.14 WLAN-Automation-Aggregation1-2 subnet (10.0.220.0/24)

Table 5-29

IP address	Component
10.0.210.1 to 10.0.210.3	Router (redundancy)

5.5.15 WLAN-Engineering-Aggregation1-2 subnet (10.0.230.0/24)

Table 5-30

IP address	Component
10.0.230.1 to 10.0.230.3	Router (redundancy)
10.0.230.0/24	Field PGs

5.5.16 Automation Cell1-1-1 subnet (10.1.10.0/24)

Table 5-31

IP address	Component
10.1.10.1 to 10.1.10.3	Routers (reserved for redundancy)
10.1.10.10 to 10.1.10.99	Network components (switches, WLAN APs/clients)
10.1.10.201	Industrial Edge device Cell1-1-1 (static DHCP lease)
10.1.10.202	SIMATIC HMI Unified Comfort Panel (X2) (static DHCP lease)

5.5.17 PROFINET1-Cell1-1-1 subnet (10.1.11.0/24)

Table 5-32

IP address	Component
10.1.11.1	CPU
10.1.11.2 to 10.1.11.200	Reserved for PROFINET devices
10.1.11.201	Industrial Edge-Device Cell1-1-1
10.1.11.202	SIMATIC HMI Unified Comfort Panel (X1)

5.5.18 Automation Cell1-1-2 subnet (10.1.20.0/24)

Table 5-33

IP address	Component
10.1.20.1 to 10.1.20.3	Routers (reserved for redundancy)
10.1.20.10 to 10.1.20.99	Network components (switches, WLAN APs/clients)
10.1.20.201	Industrial Edge device Cell1-1-2 (static DHCP lease)

5.5.19 Automation Cell1-2-1 subnet (10.2.10.0/24)

Table 5-34

IP address	Component
10.2.10.1 to 10.2.10.3	Routers (reserved for redundancy)
10.2.10.10 to 10.2.10.99	Network components (switches, WLAN APs/clients)

5.5.20 PROFINET2-Cell1-2-1 subnet (10.2.11.0/24)

Table 5-35

IP address	Component
10.2.11.201	Industrial Edge-Device Cell1-2-1
10.2.11.202	SIMATIC HMI Comfort Panel (X1)

5.5.21 PROFINET-Cell1-2-2 subnet (10.2.20.0/24)

Table 5-36

IP address	Component
10.2.20.1 to 10.2.20.3	Routers (reserved for redundancy)
10.2.20.201	Industrial Edge device Cell1-2-2 (static DHCP lease)

5.6 Appendix VI – Static routes

The routing configuration in this section is based on the following router address configuration:

Table 5-37

Router	Subnet	IP address(es)	
Enterprise firewall	Uplink network	DHCP/independent of overlying infrastructure	
	Data Forwarding (VLAN 98)	Physical 1: Physical 2: **Virtual:**	10.0.98.2/24 10.0.98.3/24 **10.0.98.1/24**
	Remote Access (VLAN 97)	Physical 1: Physical 2: **Virtual:**	10.0.97.2/24 10.0.97.3/24 **10.0.97.1/24**
	Update Services (VLAN 96)	Physical 1: Physical 2: **Virtual:**	10.0.96.2/24 10.0.96.3/24 **10.0.96.1/24**
DMZ firewall	Monitoring and Management (VLAN 10)	Physical 1: Physical 2: **Virtual:**	10.0.10.2/24 10.0.10.3/24 **10.0.10.1/24**
	Automation Application (VLAN 20)	Physical 1: Physical 2: **Virtual:**	10.0.20.2/24 10.0.20.3/24 **10.0.20.1/24**
	Automation Engineering (VLAN 30)	Physical 1: Physical 2: **Virtual:**	10.0.30.2/24 10.0.30.3/24 **10.0.30.1/24**
	Management DMZ (VLAN99)	Physical 1: Physical 2: **Virtual:**	10.0.99.2/24 10.0.99.3/24 **10.0.99.1/24**
	Data Forwarding (VLAN 98)	Physical 1: Physical 2: **Virtual:**	10.0.98.5/24 10.0.98.6/24 **10.0.98.4/24**
	Remote Access (VLAN 97)	Physical 1: Physical 2: **Virtual:**	10.0.97.5/24 10.0.97.6/24 **10.0.97.4/24**
	Update Services (VLAN 96)	Physical 1: Physical 2: **Virtual:**	10.0.96.5/24 10.0.96.6/24 **10.0.96.4/24**

Router	Subnet	IP address(es)	
	Transfer&Management-Aggregation1-1 (VLAN 100)	Physical 1: Physical 2: **Virtual:**	10.0.100.2/24 10.0.100.3/24 **10.0.100.1/24**
	Automation-Aggregation1-1 (VLAN 110)	Physical 1: Physical 2: **Virtual:**	10.0.110.2/24 10.0.110.3/24 **10.0.110.1/24**
	WLAN-Automation-Aggregation1-1 (VLAN 120)	Physical 1: Physical 2: **Virtual:**	10.0.120.2/24 10.0.120.3/24 **10.0.120.1/24**
	WLAN-Engineering-Aggregation1-1 (VLAN 130)	Physical 1: Physical 2: **Virtual:**	10.0.130.2/24 10.0.130.3/24 **10.0.130.1/24**
	Transfer&Management-Aggregation1-2 (VLAN 200)	Physical 1: Physical 2: **Virtual:**	10.0.200.2/24 10.0.200.3/24 **10.0.200.1/24**
	Automation-Aggregation1-2 (VLAN 210)	Physical 1: Physical 2: **Virtual:**	10.0.210.2/24 10.0.210.3/24 **10.0.210.1/24**
	WLAN-Automation-Aggregation1-2 (VLAN 220)	Physical 1: Physical 2: **Virtual:**	10.0.220.2/24 10.0.220.3/24 **10.0.220.1/24**
	WLAN-Engineering-Aggregation1-2 (VLAN 230)	Physical 1: Physical 2: **Virtual:**	10.0.230.2/24 10.0.230.3/24 **10.0.230.1/24**
Cell 1-1-1 firewall	Transfer&Management-Aggregation1-1 (VLAN 100)	External:	10.0.100.110/24
	Automation Cell1-1-1 (VLAN 1010)	Internal:	10.1.10.1/24
Cell 1-1-1 CPU	Automation Cell1-1-1	X2:	10.1.10.4/24
	PROFINET 1 Cell1-1-1	X1:	10.1.11.1/24
Cell 1-1-2 firewall	Transfer&Management-Aggregation1-1 (VLAN 100)	External:	10.0.100.120/24
	Automation Cell1-1-2 (VLAN 1020)	Internal:	10.1.20.1/24

Router	Subnet	IP address(es)	
Cell 1-1-2 CPU	Automation Cell1-1-2	X2:	10.1.20.4/24
	PROFINET 1 Cell1-1-2	X1:	10.1.21.1/24
Cell 1-2-1 firewall	Transfer&Management-Aggregation1-2 (VLAN 200)	External:	10.0.200.110/24
	Automation Cell1-2-1 (VLAN 2010)	Internal:	10.2.10.1/24
Cell 1-2-1 CPU	Automation Cell1-2-1	X3:	10.2.10.4/24
	PROFINET 2 Cell1-2-1	X2:	10.2.11.4/24
	PROFINET 1 Cell1-2-1	X1:	10.2.12.1/24
Cell 1-2-2 firewall	Transfer&Management-Aggregation1-2 (VLAN 200)	External:	10.0.200.120/24
	Automation Cell1-2-2	Internal:	10.2.20.1/24

Enterprise firewall routing table

The address scheme presented above results in the following routing table for the enterprise firewall:

Table 5-38

Destination	Next hop	Purpose
10.0.10.0/24	10.0.98.4	Route to Monitoring and Management
10.0.20.0/24	10.0.98.4	Route to Automation Application
10.0.30.0/24	10.0.98.4	Route to Automation Engineering
10.0.100.0/24	10.0.98.4	Route to Transfer&Management-Aggregation1-1
10.0.110.0/24	10.0.98.4	Route to Automation-Aggregation1-1
10.0.120.0/24	10.0.98.4	Route to WLAN-Automation-Aggregation1-1
10.0.130.0/24	10.0.98.4	Route to WLAN-Engineering-Aggregation1-1
10.0.200.0/24	10.0.98.4	Route to Transfer&Management-Aggregation1-2
10.0.210.0/24	10.0.98.4	Route to Automation-Aggregation1-2
10.0.220.0/24	10.0.98.4	Route to WLAN-Automation-Aggregation1-2
10.0.230.0/24	10.0.98.4	Route to WLAN-Engineering-Aggregation1-2
10.1.10.0/24	10.0.98.4	Route to Automation Cell1-1-1
10.1.11.0/24	10.0.98.4	Route to PROFINET 1 Cell1-1-1
10.1.20.0/24	10.0.98.4	Route to Automation Cell1-1-2
10.1.21.0/24	10.0.98.4	Route to PROFINET 1 Cell1-1-2
10.2.10.0/24	10.0.98.4	Route to Automation Cell1-2-1
10.2.11.0/24	10.0.98.4	Route to PROFINET 2 Cell1-2-1
10.2.12.0/24	10.0.98.4	Route to PROFINET 1 Cell1-2-1
10.2.20.0/24	10.0.98.4	Route to Automation Cell1-2-2

Destination	Next hop	Purpose
any	DHCP/depends on overlying infrastructure	Default gateway to enterprise networks

DMZ firewall routing table

The address scheme presented above results in the following routing table for the DMZ firewall:

Table 5-39

Destination	Next hop	Purpose	
10.1.10.0/24	10.0.100.110	Route to Automation Cell 1-1-1	
10.1.11.0/24	10.0.100.110	10.0.100.110	Route to PROFINET 1 Cell 1-1-1
10.1.20.0/24	10.0.100.110	10.0.100.120	Route to Automation Cell 1-1-2
10.1.21.0/24	10.0.100.110	10.0.100.120	Route to PROFINET 1 Cell 1-1-1
10.2.10.0/24	10.0.100.110	10.0.200.110	Route to Automation Cell 1-2-1
10.2.11.0/24	10.0.100.110	10.0.200.110	Route to PROFINET 2 Cell 1-2-1
10.2.12.0/24	10.0.100.110	10.0.200.110	Route to PROFINET 1 Cell 1-2-1
10.2.20.0/24	10.0.100.110	10.0.200.120	Route to Automation Cell 1-2-2
any		10.0.98.1	Default gateway (Data Forwarding interface of the enterprise firewall)

Routing tables for the DMZ servers

The following configurations apply for the servers in the DMZ as a function of the subnet:

Servers in the Data Forwarding subnet:

Table 5-40

Destination	Next hop	Purpose
10.0.10.0/24	10.0.98.4	Route to Monitoring and Management
10.0.20.0/24	10.0.98.4	Route to Automation Application
10.0.30.0/24	10.0.98.4	Route to Automation Engineering
10.0.100.0/24	10.0.98.4	Route to Transfer&Management-Aggregation1-1
10.0.110.0/24	10.0.98.4	Route to Automation-Aggregation1-1
10.0.120.0/24	10.0.98.4	Route to WLAN-Automation-Aggregation1-1
10.0.130.0/24	10.0.98.4	Route to WLAN-Engineering-Aggregation1-1
10.0.200.0/24	10.0.98.4	Route to Transfer&Management-Aggregation1-2
10.0.210.0/24	10.0.98.4	Route to Automation-Aggregation1-2
10.0.220.0/24	10.0.98.4	Route to WLAN-Automation-Aggregation1-2
10.0.230.0/24	10.0.98.4	Route to WLAN-Engineering-Aggregation1-2
10.1.10.0/24	10.0.98.4	Route to Automation Cell1-1-1
10.1.11.0/24	10.0.98.4	Route to PROFINET 1 Cell1-1-1
10.1.20.0/24	10.0.98.4	Route to Automation Cell1-1-2
10.1.21.0/24	10.0.98.4	Route to PROFINET 1 Cell1-1-2
10.2.10.0/24	10.0.98.4	Route to Automation Cell1-2-1
10.2.11.0/24	10.0.98.4	Route to PROFINET 2 Cell1-2-1
10.2.12.0/24	10.0.98.4	Route to PROFINET 1 Cell1-2-1
10.2.20.0/24	10.0.98.4	Route to Automation Cell1-2-2
any	10.0.98.1	Default gateway (Data Forwarding interface of the enterprise firewall)

Servers in the Remote Access subnet:

Table 5-41

Destination	Next hop	Purpose
10.0.10.0/24	10.0.97.4	Route to Monitoring and Management
10.0.20.0/24	10.0.97.4	Route to Automation Application
10.0.30.0/24	10.0.97.4	Route to Automation Engineering
10.0.100.0/24	10.0.97.4	Route to Transfer&Management-Aggregation1-1
10.0.110.0/24	10.0.97.4	Route to Automation-Aggregation1-1
10.0.120.0/24	10.0.97.4	Route to WLAN-Automation-Aggregation1-1
10.0.130.0/24	10.0.97.4	Route to WLAN-Engineering-Aggregation1-1
10.0.200.0/24	10.0.97.4	Route to Transfer&Management-Aggregation1-2
10.0.210.0/24	10.0.97.4	Route to Automation-Aggregation1-2
10.0.220.0/24	10.0.97.4	Route to WLAN-Automation-Aggregation1-2
10.0.230.0/24	10.0.97.4	Route to WLAN-Engineering-Aggregation1-2
10.1.10.0/24	10.0.97.4	Route to Automation Cell1-1-1
10.1.11.0/24	10.0.97.4	Route to PROFINET 1 Cell1-1-1
10.1.20.0/24	10.0.97.4	Route to Automation Cell1-1-2
10.1.21.0/24	10.0.97.4	Route to PROFINET 1 Cell1-1-2
10.2.10.0/24	10.0.97.4	Route to Automation Cell1-2-1
10.2.11.0/24	10.0.97.4	Route to PROFINET 2 Cell1-2-1
10.2.12.0/24	10.0.97.4	Route to PROFINET 1 Cell1-2-1
10.2.20.0/24	10.0.97.4	Route to Automation Cell1-2-2
any	10.0.97.1	Default gateway (Remote Access interface of the enterprise firewall)

Servers in the Update Services subnet:

Table 5-42

Destination	Next hop	Purpose
10.0.10.0/24	10.0.96.4	Route to Monitoring and Management
10.0.20.0/24	10.0.96.4	Route to Automation Application
10.0.30.0/24	10.0.96.4	Route to Automation Engineering
10.0.100.0/24	10.0.96.4	Route to Transfer&Management-Aggregation1-1
10.0.110.0/24	10.0.96.4	Route to Automation-Aggregation1-1
10.0.120.0/24	10.0.96.4	Route to WLAN-Automation-Aggregation1-1
10.0.130.0/24	10.0.96.4	Route to WLAN-Engineering-Aggregation1-1
10.0.200.0/24	10.0.96.4	Route to Transfer&Management-Aggregation1-2
10.0.210.0/24	10.0.96.4	Route to Automation-Aggregation1-2
10.0.220.0/24	10.0.96.4	Route to WLAN-Automation-Aggregation1-2
10.0.230.0/24	10.0.96.4	Route to WLAN-Engineering-Aggregation1-2
10.1.10.0/24	10.0.96.4	Route to Automation Cell1-1-1
10.1.11.0/24	10.0.96.4	Route to PROFINET 1 Cell1-1-1
10.1.20.0/24	10.0.96.4	Route to Automation Cell1-1-2
10.1.21.0/24	10.0.96.4	Route to PROFINET 1 Cell1-1-2
10.2.10.0/24	10.0.96.4	Route to Automation Cell1-2-1
10.2.11.0/24	10.0.96.4	Route to PROFINET 2 Cell1-2-1
10.2.12.0/24	10.0.96.4	Route to PROFINET 1 Cell1-2-1
10.2.20.0/24	10.0.96.4	Route to Automation Cell1-2-2
any	10.0.96.1	Default gateway (Update Services interface of the enterprise firewall)

Routing tables of the cell firewalls

The following configuration results for the cell firewalls:

Cell 1-1-1:

Table 5-43

Destination		Next hop	Purpose
10.1.11.0/24		10.1.10.4	Route to PROFINET 1 Cell 1-1-1
10.1.20.0/24		10.0.100.120	Route to Automation Cell 1-1-2
10.1.21.0/24		10.0.100.120	Route to PROFINET 1 Cell 1-1-2
any		10.0.100.1	Default gateway (Transfer&Management1-1 interface of the DMZ firewall)

Cell 1-1-2:

Table 5-44

Destination	Next hop	Purpose
10.1.21.0/24	10.1.20.4	Route to PROFINET 1 Cell 1-2-1
10.1.10.0/24	10.0.100.110	Route to Automation Cell 1-1-1
10.1.11.0/24	10.0.100.110	Routes to PROFINET 1 Cell 1-1-1
any	10.0.100.1	Default gateway (Transfer&Management1-1 interface of the DMZ firewall)

Cell 1-2-1:

Table 5-45

Destination	Next hop	Purpose
10.2.11.0/24	10.2.10.4	Route to PROFINET 2 Cell 1-2-1
10.2.12.0/24	10.2.10.4	Route to PROFINET 1 Cell 1-2-1
10.2.20.0/24	10.0.200.120	Route to Automation Cell 1-2-2
any	10.0.200.1	Default gateway (Transfer&Management1-2 interface of the DMZ firewall)

Cell 1-2-2:

Table 5-46

Destination	Next hop	Purpose
10.2.10.0/24	10.0.200.110	Route to Automation Cell 1-2-1
10.2.11.0/24	10.0.200.110	Route to PROFINET 2 Cell 1-2-1
10.2.12.0/24	10.0.200.110	Route to PROFINET 1 Cell 1-2-1
any	10.0.200.1	Default gateway (Transfer&Management1-2 interface of the DMZ firewall)

Routing tables for the servers in the Transfer&Management-Aggregation subnets

The systems installed in the Transfer&Management-Aggregation subnets need the following routing configuration in order to communicate to the cells without a detour through the DMZ firewall.

Systems in the Transfer&Management-Aggregation1-1 subnet:

Table 5-47

Destination	Next hop	Purpose
10.1.10.0/24	10.0.100.110	Route to Automation Cell 1-1-1
10.1.11.0/24	10.0.100.110	Route to PROFINET 1 Cell 1-1-1
10.1.20.0/24	10.0.100.120	Route to Automation Cell 1-1-2
10.1.21.0/24	10.0.100.120	Route to PROFINET 1 Cell 1-1-1
any	10.0.100.1	Default gateway (Transfer&Management1-1 interface of the DMZ firewall)

Systems in the Transfer&Management-Aggregation1-2 subnet:

Table 5-48

Destination	Next hop	Purpose
10.2.10.0/24	10.0.200.110	Route to Automation Cell 1-2-1
10.2.11.0/24	10.0.200.110	Route to PROFINET 2 Cell 1-2-1
10.2.12.0/24	10.0.200.110	Route to PROFINET 1 Cell 1-2-1
10.2.20.0/24	10.0.200.120	Route to Automation Cell 1-2-2
any	10.0.200.1	Default gateway (Transfer&Management1-2 interface of the DMZ firewall)

Other devices:

All devices not explicitly listed in this Appendix do not receive further routing configuration beyond the default gateway (first address of the connected subnet). In case of devices with multiple interfaces (e.g. CPUs), the default gateway should always be defined on the interface on the highest network level (typically in the Automation-Cell subnet).

The "Enable IP forwarding" feature must also be enabled in the CPUs.

5.7 Appendix VII – Firewall rule visualization

Allowing the following connections is recommended for operation of the visualization components.

Note

Other ports for additional SIMATIC Panel products that you would need for configuring external firewalls can be found here:

https://support.industry.siemens.com/cs/ww/en/view/109773506/120442899979

5.7.1 DMZ firewall

Table 5-49

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	HMI Panel *10.1.11.202* *10.2.11.202*	TCP 5001	This service is used to transmit images and runtime to Panels.
		TCP 161	The SNMP client functionality is used by STEP 7 to read status information from PROFINET devices.
Engineering VMs *10.0.30.100 to 10.0.30.254*	WinCC Unified PC RT *10.0.20.10*	TCP 20008	This service is used to load the runtime.
Engineering VMs *10.0.30.100 to 10.0.30.254*	WinCC V7.x RT *10.0.20.10*	TCP 2308 Alternative: 50523	Transfer (via Ethernet; CE stub; PC loader; PC)
Web-based WinCC client *10.0.110.100 to 10.0.110.200*	HMI Panel *10.1.11.202* *10.2.11.202*	TCP 443	The HTTPS protocol is used for communication with the HMI web server via Secure Socket Layer (SSL).
	WinCC Unified PC RT or WinCC V7.x RT *10.0.20.10*		HTTPS protocol for communication between web-based clients and WinCC Unified PC RT
VNC client	HMI Panel *10.1.11.202* *10.2.11.202*	TCP 5900	Sm@rtServer
HMI Panel *10.1.11.202* *10.2.11.202*	OPC UA client *10.0.20.22*	TCP 4890	OPC UA server/client communication
WinCC Unified PC RT as OPC UA client *10.0.20.20*	Third-party controller		
WinCC server system *10.0.20.20*	CPUs *10.1.10.4*	TCP 102	Communication with the S7 controller via Ethernet/PROFINET
Industrial thin client *10.0.110.10 to 100.110.20*	WinCC terminal server *10.0.20.21*	TCP 3389	RDP connection between thin client and WinCC terminal server

5.7.2 Cell 1-1-1 firewall

Table 5-50

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	SIMATIC Unified Comfort Panel Cell1-1-1 *10.1.10.202*	TCP 5001	This service is used to transmit images and runtime to Panels.
		TCP 443	Web server access from the engineering VMs to the SIMATIC Unified Comfort Panel
		TCP 4840	OPC UA server access from the engineering VMs to the SIMATIC Unified Comfort Panel
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	SIMATIC Unified Comfort Panel Cell1-1-1 *10.1.10.202*	TCP 5001	Diagnostic and download access from the Field PGs in the aggregation level to the SIMATIC Unified Comfort Panel
		TCP 443	Web server access from the Field PGs in the aggregation level to the SIMATIC Unified Comfort Panel
		TCP 4840	OPC UA server access from the Field PGs in the aggregation level to the SIMATIC Unified Comfort Panel
OPC UA client station *10.0.20.22*	SIMATIC Unified Comfort Panel Cell1-1-1 *10.1.10.202*	TCP 4840	OPC UA server access from the OPC UA clients to the SIMATIC Unified Comfort Panel
thin client *10.0.110.10*	SIMATIC Unified Comfort Panel Cell1-1-1 *10.1.10.202*	TCP 443	Client (web) access to the SIMATIC Unified Comfort Panel
VNC client	SIMATIC Unified Comfort Panel Cell1-1-1 *10.1.11.202*	TCP 5900	Sm@rtServer

5.7.3 Cell 1-2-1 firewall

Table 5-51

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	SIMATIC Comfort Panel Cell1-2-1 *10.2.11.202*	TCP 5001	This service is used to transmit images and runtime to Panels.
		TCP 443	Web server access from the engineering VMs to the SIMATIC Comfort Panel
		TCP 4840	OPC UA server access from the engineering VMs to the SIMATIC Unified Comfort Panel

Source	Destination	Destination port	Use
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	SIMATIC Comfort Panel Cell1-2-1 *10.2.11.202*	TCP 5001	Diagnostic and download access from the Field PGs in the aggregation level to the SIMATIC Comfort Panel
		TCP 443	Web server access from the Field PGs in the aggregation level to the SIMATIC Comfort Panel

5.8 Appendix VIII – Basic configuration of the firewalls

To provide the basic DHCP, DNS, Syslog and proxy server services, the following connections must be allowed in the firewalls:

5.8.1 Enterprise firewall

Table 5-52

Source	Destination	Destination port	Use
DMZ domain controller *10.0.98.10*	Enterprise domain controller	see \4\	Import of user accounts and groups from enterprise IT
Proxy server *10.0.98.20*	---	---	Unrestricted proxy server access to higher-level networks
SINEC INS *10.0.10.110*	Enterprise firewall *10.0.98.1*	TCP/UDP 123	NTP access from SINEC INS
Domain controller *10.0.98.10*	Enterprise firewall *10.0.98.1*	TCP/UDP 53	DNS access from domain controller
SINEC INS *10.0.10.110*	Enterprise firewall *10.0.98.1*	TCP/UDP 53	DNS access from SINEC INS
DMZ firewall *10.0.98.4*	Enterprise firewall *10.0.98.1*	TCP/UDP 53	DNS access from the DMZ firewall

5.8.2 DMZ firewall

Table 5-53

Source	Destination	Destination port	Use
SINEC INS *10.0.10.110*	Domain controller *10.0.98.10*	TCP/UDP 53	DNS access from SINEC INS to the domain controller
SINEC INS *10.0.10.110*	Enterprise firewall *10.0.98.1*	TCP/UDP 123	NTP access from SINEC INS to the enterprise firewall
Monitoring&Management *10.0.10.0/24*	DMZ firewall *10.0.10.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Monitoring&Management subnet
Automation-Application *10.0.20.0/24*	DMZ firewall *10.0.20.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Automation-Application subnet
Automation-Engineering	DMZ firewall	TCP/UDP 53	DNS and NTP access from all hosts in the Automation-Engineering subnet

Source	Destination	Destination port	Use
10.0.30.0/24	*10.0.30.1*	TCP/UDP 123	
Management DMZ *10.0.99.0/24*	DMZ firewall *10.0.99.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Management-DMZ subnet
Data-Forwarding *10.0.98.0/24*	DMZ firewall *10.0.98.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Data-Forwarding subnet
Remote-Access *10.0.97.0/24*	DMZ firewall *10.0.97.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Remote-Access subnet
Update-Services *10.0.96.0/24*	DMZ firewall *10.0.96.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Update-Services subnet
Transfer&Managemnt-Aggregation1-1 *10.0.100.0/24*	DMZ firewall *10.0.100.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Transfer&Managemnt-Aggregation1-1 subnet
Automation-Aggregation1-1 *10.0.110.0/24*	DMZ firewall *10.0.110.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Automation-Aggregation1-1 subnet
WLAN-Automation-Aggregation1-1 *10.0.120.0/24*	DMZ firewall *10.0.120.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the WLAN-Automation-Aggregation1-1 subnet
WLAN-Engineering-Aggregation1-1 *10.0.130.0/24*	DMZ firewall *10.0.130.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the WLAN-Engineering-Aggregation1-1 subnet
Transfer&Managemnt-Aggregation1-2 *10.0.200.0/24*	DMZ firewall *10.0.200.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Transfer&Managemnt-Aggregation1-2 subnet
Automation-Aggregation1-2 *10.0.210.0/24*	DMZ firewall *10.0.210.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the Automation-Aggregation1-2 subnet
WLAN-Automation-Aggregation1-2 *10.0.220.0/24*	DMZ firewall *10.0.220.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the WLAN-Automation-Aggregation1-2 subnet
WLAN-Engineering-Aggregation1-2 *10.0.230.0/24*	DMZ firewall *10.0.230.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the WLAN-Engineering-Aggregation1-2 subnet

5.8.3 Cell1-1-1 firewall

Table 5-54

Source	Destination	Destination port	Use
Automation Cell1-1-1 *10.1.10.0/24*	Firewall-Cell1-1-1 *10.1.10.1*	TCP/UDP 53 TCP/UPD 123	DNS and NTP access from all hosts in the Automation Cell1-1-1 subnet
PROFINET1-Cell1-1-1 *10.1.11.0/24*	Firewall-Cell1-1-1 *10.1.10.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the PROFINET1-Cell1-1-1 subnet
DMZ firewall *10.0.100.1* *10.0.100.2* *10.0.100.3*	Firewall-Cell1-1-1 *10.0.100.110*	TCP/UDP 53	DNS access from the DMZ firewall

5.8.4 Cell1-1-2 firewall

Table 5-55

Source	Destination	Destination port	Use
Automation Cell1-1-2 *10.1.20.0/24*	Firewall-Cell1-1-2 *10.1.20.1*	TCP/UDP 53 TCP/UPD 123	DNS and NTP access from all hosts in the Automation Cell1-1-2 subnet
PROFINET1-Cell1-1-1 *10.1.21.0/24*	Firewall-Cell1-1-2 *10.1.20.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the PROFINET1-Cell1-1-2 subnet
DMZ firewall *10.0.100.1* *10.0.100.2* *10.0.100.3*	Firewall-Cell1-1-2 *10.0.100.120*	TCP/UDP 53	DNS access from the DMZ firewall

5.8.5 Cell1-2-1 firewall

Table 5-56

Source	Destination	Destination port	Use
Automation Cell1-2-1 *10.2.10.0/24*	Firewall-Cell1-2-1 *10.2.10.1*	TCP/UDP 53 TCP/UPD 123	DNS and NTP access from all hosts in the Automation Cell1-2-1 subnet
PROFINET2-Cell1-2-1 *10.2.11.0/24*	Firewall-Cell1-2-1 *10.2.10.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the PROFINET2-Cell1-2-1 subnet

Source	Destination	Destination port	Use
PROFINET1-Cell1-2-1 *10.2.12.0/24*	Firewall-Cell1-2-1 *10.2.10.1*	TCP/UDP 53 TCP/UDP 123	DNS and NTP access from all hosts in the PROFINET1-Cell1-2-1 subnet
DMZ firewall *10.0.200.1* *10.0.200.2* *10.0.200.3*	Firewall-Cell1-2-1 *10.0.200.210*	TCP/UDP 53	DNS access from the DMZ firewall

5.8.6 Cell1-2-2 firewall

Table 5-57

Source	Destination	Destination port	Use
Automation Cell1-2-2 *10.2.20.0/24*	Firewall-Cell1-2-2 *10.2.20.1*	TCP/UDP 53 TCP/UPD 123	DNS and NTP access from all hosts in the PROFINET-Cell1-2-2 subnet
DMZ firewall *10.0.200.1* *10.0.200.2* *10.0.200.3*	Firewall-Cell1-2-2 *10.0.200.220*	TCP/UDP 53	DNS access from the DMZ firewall

5.9 Appendix IX – Firewall rule engineering

Allowing the following connections is recommended for engineering work on the automation components:

5.9.1 Rules for operation of the engineering infrastructure

The following general rules should be defined for the engineering systems:

DMZ firewall

Table 5-58

Source	Destination	Destination port	Use
Project/license server *10.0.30.10*	Domain controller *10.0.98.10*	see \4\	Active Directory link for the project/license server
	Proxy server *10.0.98.20*	TCP 443	Web license key download URL: https://www.automation.siemens.com/swdl/"
Engineering VMs *10.0.30.100 to 10.0.30.254*	Domain controller *10.0.98.10*	see \4\	Active Directory link for the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	Domain controller *10.0.98.10*	see \4\	Active Directory link for the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.1.10.201 to 10.1.10.254* *10.1.20.201 to 10.1.20.254* *10.2.10.201 to 10.2.10.254* *10.2.20.201 to 10.2.20.254*	Domain controller *10.0.98.10*	see \4\	Active Directory link for the Field PGs in the cell level
Engineering VMs	Project/license server	TCP 8735	Access from the engineering VMs in the local Automation-Engineering subnet to the project/license server

Source	Destination	Destination port	Use
10.0.30.100 to 10.0.30.254	*10.0.30.10*	TCP 4410	(local access, no firewall configuration necessary)
Project/license server *10.0.30.10*	Engineering VMs *10.0.30.100 to 10.0.30.254*	TCP 4410	Distribution of licenses from the project/license server to engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	Project/license server *10.0.30.10*	TCP 8735 TCP 4410	Access from the Field PGs in the WLAN-Engineering-Aggregation subnets to the project/license server
Project/license server *10.0.30.10*	Field PGs (DHCP, aggregation level) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs
Field PGs (DHCP range, cell level) *10.1.10.201 to 10.1.10.254*	Project/license server *10.0.30.10*	TCP 8735	Access from the Field PGs in the Automation-Cell subnets to the project/license server

Source	Destination	Destination port	Use
10.1.20.201 to 10.1.20.254 *10.2.10.201 to 10.2.10.254* *10.2.20.201 to 10.2.20.254*		TCP 4410	
Project/license server *10.0.30.10*	Field PGs (DHCP, cell level) *10.1.10.201 to 10.1.10.254* *10.1.20.201 to 10.1.20.254* *10.2.10.201 to 10.2.10.254* *10.2.20.201 to 10.2.20.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs
Jump server *10.0.97.20*	Engineering VMs *10.0.30.100 to 10.0.30.254*	TCP/UDP 3389	Remote desktop connection from the Remote Connect jump server to engineering VMs
Field PGs (DHCP range, cell level) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254* *10.1.10.201 to 10.1.10.254* *10.1.20.201 to 10.1.20.254* *10.2.10.201 to 10.2.10.254* *10.2.20.201 to 10.2.20.254*	Engineering VMs *10.0.30.100 to 10.0.30.254*	TCP/UDP 3389	Remote desktop connection to engineering VMs

Cell1-1-1 firewall

Table 5-59

Source	Destination	Destination port	Use
Field PGs (DHCP range, Cell1-1-1) *10.1.10.201 to 10.1.10.254*	Domain controller *10.0.98.10*	see \4\	Active Directory link, Field PGs in the cell
Field PGs (DHCP range, Cell1-1-1) *10.1.10.201 to 10.1.10.254*	Project/license server *10.0.30.10*	TCP 8735	Access from the Field PGs in the Automation Cell1-1-1 subnet to the project/license server
		TCP 4410	
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-1-1) *10.1.10.201 to 10.1.10.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the Automation Cell1-1-1 subnet
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-1-1) *10.1.10.201 to 10.1.10.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the Automation Cell1-1-1 subnet
Field PGs (DHCP range, Cell1-1-1) *10.1.10.201 to 10.1.10.254*	Engineering VMs *10.0.30.100 to 10.0.30.254*	TCP/UDP 3389	Remote desktop connection to engineering VMs

Cell1-1-2 firewall

Table 5-60

Source	Destination	Destination port	Use
Field PGs (DHCP range, Cell1-1-2) *10.1.20.201 to 10.1.20.254*	Domain controller *10.0.98.10*	see \4\	Active Directory link, Field PGs in the cell
Field PGs (DHCP range, Cell1-1-2) *10.1.20.201 to 10.1.20.254*	Project/license server *10.0.30.10*	TCP 8735	Access from the Field PGs in the Automation Cell1-1-2 subnet to the project/license server
		TCP 4410	
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-1-2) *10.1.20.201 to 10.1.20.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the Automation Cell1-1-2 subnet
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-1-2) *10.1.20.201 to 10.1.20.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the Automation Cell1-1-2 subnet
Field PGs (DHCP range, Cell1-1-2) *10.1.20.201 to 10.1.20.254*	Engineering VMs *10.0.30.100 to 10.0.30.254*	TCP/UDP 3389	Remote desktop connection to engineering VMs

Cell1-2-1 firewall

Table 5-61

Source	Destination	Destination port	Use
Field PGs (DHCP range, Cell1-2-1) *10.2.10.201 to 10.2.10.254*	Domain controller *10.0.98.10*	see \4\	Active Directory link, Field PGs in the cell
Field PGs (DHCP range, Cell1-2-1) *10.2.10.201 to 10.2.10.254*	Project/license server *10.0.30.10*	TCP 8735	Access from the Field PGs in the Automation Cell1-2-1 subnet to the project/license server
		TCP 4410	
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-2-1) *10.2.10.201 to 10.2.10.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the Automation Cell1-2-1 subnet
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-2-1) *10.2.10.201 to 10.2.10.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the Automation Cell1-2-1 subnet
Field PGs (DHCP range, Cell1-2-1) *10.2.10.201 to 10.2.10.254*	Engineering VMs *10.0.30.100 to 10.0.30.254*	TCP/UDP 3389	Remote desktop connection to engineering VMs

Cell1-2-2 firewall

Table 5-62

Source	Destination	Destination port	Use
Field PGs (DHCP range, Cell1-2-2) *10.2.20.201 to 10.2.20.254*	Domain controller *10.0.98.10*	see \4\	Active Directory link, Field PGs in the cell
Field PGs (DHCP range, Cell1-2-2) *10.2.20.201 to 10.2.20.254*	Project/license server *10.0.30.10*	TCP 8735	Access from the Field PGs in the PROFINET-Cell1-2-2 subnet to the project/license server
		TCP 4410	
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-2-2) *10.2.20.201 to 10.2.20.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the PROFINET-Cell1-2-2 subnet
Project/license server *10.0.30.10*	Field PGs (DHCP, Cell1-2-2) *10.2.20.201 to 10.2.20.254*	TCP 4410	Distribution of licenses from the project/license server to Field PGs in the PROFINET-Cell1-2-2 subnet
Field PGs (DHCP range, Cell1-2-2) *10.2.20.201 to 10.2.20.254*	Engineering VMs *10.0.30.100 to 10.0.30.254*	TCP/UDP 3389	Remote desktop connection to engineering VMs

5.9.2 Rules for access to the SIMATIC S7-1200/1500 CPUs

The following firewall configurations are necessary for configuration access to the CPUs:

DMZ firewall

Table 5-63

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	CPUs *10.1.10.4* *10.1.20.4* *10.2.10.4* *10.2.20.4*	TCP 102	Diagnostic and download access from the engineering VMs to the CPUs
		TCP 443	Web server access from the engineering VMs to the CPUs
		TCP 4840	OPC UA server access from the engineering VMs to the CPUs
Field PGs (DHCP range, WLAN-Engineering-	CPUs	TCP 102	Diagnostic and download access from the Field PGs in the aggregation level to the CPUs

Source	Destination	Destination port	Use
Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	*10.1.10.4* *10.1.20.4* *10.2.10.4* *10.2.20.4*	TCP 443	Web server access from the Field PGs in the aggregation level to the CPUs
		TCP 4840	OPC UA server access from the Field PGs in the aggregation level to the CPUs

Cell1-1-1 firewall

Table 5-64

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	CPU Cell1-1-1 *10.1.10.4*	TCP 102	Diagnostic and download access from the engineering VMs to the CPU
		TCP 443	Web server access from the engineering VMs to the CPU
		TCP 4840	OPC UA server access from the engineering VMs to the CPU
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	CPU Cell1-1-1 *10.1.10.4*	TCP 102	Diagnostic and download access from the Field PGs in the aggregation level to the CPU
		TCP 443	Web server access from the Field PGs in the aggregation level to the CPU
		TCP 4840	OPC UA server access from the Field PGs in the aggregation level to the CPU

Cell1-1-2 firewall

Table 5-65

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	CPU Cell1-1-2 *10.1.20.4*	TCP 102	Diagnostic and download access from the engineering VMs to the CPU
		TCP 443	Web server access from the engineering VMs to the CPU
		TCP 4840	OPC UA server access from the engineering VMs to the CPU
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	CPU Cell1-1-2 *10.1.20.4*	TCP 102	Diagnostic and download access from the Field PGs in the aggregation level to the CPU
		TCP 443	Web server access from the Field PGs in the aggregation level to the CPU
		TCP 4840	OPC UA server access from the Field PGs in the aggregation level to the CPU

Cell1-2-1 firewall

Table 5-66

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	CPU Cell1-1-2 *10.2.10.4*	TCP 102	Diagnostic and download access from the engineering VMs to the CPU
		TCP 443	Web server access from the engineering VMs to the CPU
		TCP 4840	OPC UA server access from the engineering VMs to the CPU
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	CPU Cell1-1-2 *10.2.10.4*	TCP 102	Diagnostic and download access from the Field PGs in the aggregation level to the CPU
		TCP 443	Web server access from the Field PGs in the aggregation level to the CPU
		TCP 4840	OPC UA server access from the Field PGs in the aggregation level to the CPU

Cell1-2-2 firewall

Table 5-67

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	Cell1-2-2 CPU *10.2.20.4*	TCP 102	Diagnostic and download access from the engineering VMs to the CPU
		TCP 443	Web server access from the engineering VMs to the CPU
		TCP 4840	OPC UA server access from the engineering VMs to the CPU
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	Cell1-2-2 CPU *10.2.20.4*	TCP 102	Diagnostic and download access from the Field PGs in the aggregation level to the CPU
		TCP 443	Web server access from the Field PGs in the aggregation level to the CPU
		TCP 4840	OPC UA server access from the Field PGs in the aggregation level to the CPU

5.9.3 Rules for accessing the Industrial Edge components

The following firewall configurations are necessary for configuration access to the Industrial Edge components:

DMZ firewall

Table 5-68

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IEM *10.0.20.10*	TCP 443	IEM web interface access from the engineering VMs
Engineering VMs *10.0.30.100 to 10.0.30.254*	IEDs *10.1.10.201* *10.1.20.201* *10.2.11.201* *10.2.20.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	IEM *10.0.20.10*	TCP 443	IEM web interface access from the Field PGs in the aggregation level

Source	Destination	Destination port	Use
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	IEDs *10.1.10.201* *10.1.20.201* *10.2.11.201* *10.2.20.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.1.10.201 to 10.1.10.254* *10.1.20.201 to 10.1.20.254* *10.2.10.201 to 10.2.10.254* *10.2.20.201 to 10.2.20.254*	IEM *10.0.20.10*	TCP 443	IEM web interface access from the Field PGs in the Automation-Cell subnets

Cell1-1-1 firewall

Table 5-69

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-1-1 *10.1.10.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-1) *10.0.130.201 to 10.0.130.254*	IED Cell1-1-1 *10.1.10.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.1.10.201 to 10.1.10.254*	IEM *10.0.20.10*	TCP 443	IEM web interface access from the Field PGs in the Automation Cell1-1-1 subnet

Cell1-1-2 firewall

Table 5-70

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-1-2 *10.1.20.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-1) *10.0.130.201 to 10.0.130.254*	IED Cell1-1-2 *10.1.20.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.1.20.201 to 10.1.20.254*	IEM *10.0.20.10*	TCP 443	IEM web server access from the Field PGs in the Automation Cell1-1-2 subnet

Cell1-2-1 firewall

Table 5-71

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-2-1 *10.2.11.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-2) *10.0.230.201 to 10.0.230.254*	IED Cell1-2-1 *10.2.11.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.2.10.201 to 10.2.10.254*	IEM *10.0.20.10*	TCP 443	IEM web server access from the Field PGs in the Automation Cell1-2-1 subnet

Cell1-2-2 firewall

Table 5-72

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-2-2 *10.2.20.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-2) *10.0.230.201 to 10.0.230.254*	IED Cell1-2-2 *10.2.20.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.2.20.201 to 10.2.20.254*	IEM *10.0.20.10*	TCP 443	IEM web server access from the Field PGs in the PROFINET-Cell1-2-2 subnet

5.9.4 Rules for access to the SIMATIC HMI

DMZ firewall

Table 5-73

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	HMI Panel *10.1.10.202* *10.2.11.202*	TCP 5001	This service is used to transmit images and runtime to Panels.
		TCP 161	The SNMP client functionality is used by STEP 7 to read status information from PROFINET devices.
Engineering VMs *10.0.30.100 to 10.0.30.254*	Unified PC RT *10.0.20.10*	TCP 20008	This service is used to load the runtime
Engineering VMs *10.0.30.100 to 10.0.30.254*	WinCC V7.x RT *10.0.20.10*	TCP 2308 Alternative: 50523	Transfer (via Ethernet; CE stub; PC loader; PC)

Cell1-1-1 firewall

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	SIMATIC Unified Comfort Panel Cell1-1-1 *10.1.10.202*	TCP 5001	This service is used to transmit images and runtime to Panels.
		TCP 443	Web server access from the engineering VMs to the SIMATIC Unified Comfort Panel

Source	Destination	Destination port	Use
		TCP 4840	OPC UA server access from the engineering VMs to the SIMATIC Unified Comfort Panel
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	SIMATIC Unified Comfort Panel Cell1-1-1 *10.1.10.202*	TCP 5001	Diagnostic and download access from the Field PGs in the aggregation level to the SIMATIC Unified Comfort Panel
		TCP 443	Web server access from the Field PGs in the aggregation level to the SIMATIC Unified Comfort Panel
		TCP 4840	OPC UA server access from the Field PGs in the aggregation level to the SIMATIC Unified Comfort Panel

Cell 1-2-1 firewall

Table 5-74

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	SIMATIC Comfort Panel Cell1-2-1 *10.2.11.202*	TCP 5001	This service is used to transmit images and runtime to Panels.
		TCP 443	Web server access from the engineering VMs to the SIMATIC Comfort Panel
		TCP 4840	OPC UA server access from the engineering VMs to the SIMATIC Unified Comfort Panel
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	SIMATIC Comfort Panel Cell1-2-1 *10.2.11.202*	TCP 5001	Diagnostic and download access from the Field PGs in the aggregation level to the SIMATIC Comfort Panel
		TCP 443	Web server access from the Field PGs in the aggregation level to the SIMATIC Comfort Panel

5.9.5 Rules for access to the network components

DMZ firewall

Note The address ranges given here encompass the ranges specified during IP planning. The rule set should be adjusted to fit the specific number of devices once the network has been built.

Table 5-75

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	Network components in the Monitoring and Management subnet *10.0.10.1 to 10.0.10.99*	TCP 443	Web interface access from engineering VMs and Field PGs in the aggregation level to network components in the backbone
	Network components in the Management-DMZ subnet *10.0.99.1 to 10.0.99.99*		Web interface access from engineering VMs and Field PGs in the aggregation level to network components in the DMZ
	Network components in the Transfer&Management-Aggregation subnets *10.0.100.1 to 10.0.100.99* *10.0.200.1 to 10.0.200.99*		Web interface access from engineering VMs and Field PGs in the aggregation level to network components in the aggregation level
Field PGs (DHCP range, WLAN-Engineering-Aggregation) *10.0.130.201 to 10.0.130.254* *10.0.230.201 to 10.0.230.254*	Network components in the Automation-Cell subnets *10.1.10.1 to 10.1.10.99* *10.1.20.1 to 10.1.20.99* *10.2.10.1 to 10.2.10.99* *10.2.20.1 to 10.2.20.99*	TCP 443	Web interface access from engineering VMs and Field PGs in the aggregation level to network components in the cells
	Network components in the PROFINET subnets *[IP addresses of the switches]*		Web interface access from engineering VMs and Field PGs in the aggregation level to network components in the PROFINET networks
Field PGs (DHCP range, cell level) *10.1.10.201 to 10.1.10.254* *10.1.20.201 to 10.1.20.254* *10.2.10.201 to 10.2.10.254*	Network components in the Monitoring and Management subnet *10.0.10.1 to 10.0.10.99*	TCP 443	Web interface access from the Field PGs in the cells to network components in the backbone
	Network components in the Management-DMZ subnet *10.0.99.1 to 10.0.99.99*		Web interface access from the Field PGs in the cells to network components in the DMZ

Source	Destination	Destination port	Use
10.2.20.201 to 10.2.20.254	Network components in the Transfer&Management-Aggregation subnets *10.0.100.1 to 10.0.100.99* *10.0.200.1 to 10.0.200.99*	TCP 443	Web interface access from the Field PGs in the cells to network components in the aggregation level

Cell1-1-1 firewall

Table 5-76

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-1-1 *10.1.10.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-1) *10.0.130.201 to 10.0.130.254*	IED Cell1-1-1 *10.1.10.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.1.10.201 to 10.1.10.254*	IEM *10.0.20.10*	TCP 443	IEM web interface access from the Field PGs in the Automation Cell1-1-1 subnet

Cell1-1-2 firewall

Table 5-77

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-1-2 *10.1.20.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-1) *10.0.130.201 to 10.0.130.254*	IED Cell1-1-2 *10.1.20.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level

Source	Destination	Destination port	Use
Field PGs (DHCP range, cell level) *10.1.20.201 to 10.1.20.254*	IEM *10.0.20.10*	TCP 443	IEM web server access from the Field PGs in the Automation Cell1-1-2 subnet

Cell1-2-1 firewall

Table 5-78

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-2-1 *10.2.11.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-2) *10.0.230.201 to 10.0.230.254*	IED Cell1-2-1 *10.2.11.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.2.10.201 to 10.2.10.254*	IEM *10.0.20.10*	TCP 443	IEM web server access from the Field PGs in the Automation Cell1-2-1 subnet

Cell1-2-2 firewall

Table 5-79

Source	Destination	Destination port	Use
Engineering VMs *10.0.30.100 to 10.0.30.254*	IED Cell1-2-2 *10.2.20.201*	TCP 443	IED web interface access from the engineering VMs
Field PGs (DHCP range, WLAN-Engineering-Aggregation1-2) *10.0.230.201 to 10.0.230.254*	IED Cell1-2-2 *10.2.20.201*	TCP 443	IED web interface access from the Field PGs in the aggregation level
Field PGs (DHCP range, cell level) *10.2.20.201 to 10.2.20.254*	IEM *10.0.20.10*	TCP 443	IEM web server access from the Field PGs in the PROFINET-Cell1-2-2 subnet

5.10 Appendix X – Proxy configuration

The following system accounts are recommended for the proxy server. Communication flows are described in greater detail in the pertinent chapters.

Table 5-80

System	Chap.	Proxy user	Required URLs
TIA server	3.4.8	TiaServ	https://www.automation.siemens.com/swdl/
Industrial Edge Management	3.14	EdgeMqmt	portal.eu1.edge.siemens.cloud portalhub.eu1.edge.siemens.cloud artifacts.eu1.edge.siemens.cloud portal-relay.eu1.edge.siemens.cloud
SIMATIC Automation Tool	3.4.4	Sat	https://support.industry.siemens.com/cs/de/en/view/109746530
SINEC NMS	3.4.2	SINECNMS	
WSUS	3.4.7	Wsus	http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.windowsupdate.com https://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://go.microsoft.com http://dl.delivery.mp.microsoft.com https://dl.delivery.mp.microsoft.com

5.11 Appendix XI – Firewall rules for cloud connection

The cloud connection described in chapter 3.10 necessitates the following rules.

5.11.1 External firewall in the office network

Table 5-81

Source	Destination	Destination port	Use
External interface of the enterprise firewall *[depends on office network]*	URL of the MindConnect IoT Extension *[depends on MindSphere]*	TCP 8883	MQTT connection from the enterprise firewall to MindConnect IoT Extension

5.11.2 Enterprise firewall

Table 5-82

Source	Destination	Destination port	Use
CPU Cell1-1-1 *10.1.10.4*	URL of the MindConnect IoT Extension *[depends on MindSphere]*	TCP 8883	MQTT connections from the CPUs to MindConnect IoT Extension
CPU Cell1-2-1 *10.2.10.4*			

5.11.3 DMZ firewall

Table 5-83

Source	Destination	Destination port	Use
CPU Cell1-1-1 *10.1.10.4*	URL of the MindConnect IoT Extension *[depends on MindSphere]*	TCP 8883	MQTT connections from the CPUs to MindConnect IoT Extension
CPU Cell1-2-1 *10.2.10.4*			

5.11.4 Cell1-1-1 firewall

Table 5-84

Source	Destination	Destination port	Use
CPU Cell1-1-1 *10.1.10.4*	URL of the MindConnect IoT Extension *[depends on MindSphere]*	TCP 8883	MQTT connections from the CPUs to MindConnect IoT Extension

5.11.5 Cell1-2-1 firewall

Table 5-85

Source	Destination	Destination port	Use
CPU Cell1-2-1 *10.2.10.4*	URL of the MindConnect IoT Extension *[depends on MindSphere]*	TCP 8883	MQTT connections from the CPUs to MindConnect IoT Extension

6 Appendix

6.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible 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:

siemens.com/SupportRequest

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

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

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

support.industry.siemens.com/cs/ww/en/sc/2067

6.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

6.3 Links and literature

Table 6-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109802750
\3\	Industrial Edge Management – Getting Started https://support.industry.siemens.com/cs/ww/en/view/109779989
\4\	How to configure a firewall for Active Directory domains and trusts https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts
\5\	Central User Management with "User Management Component (UMC)" https://support.industry.siemens.com/cs/ww/en/view/109780337
\6\	Static routes in Microsoft Windows https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/route_ws2008
\7\	Which IO controllers and IO devices support the following functions in STEP 7 (TIA Portal): IRT, prioritized startup, MRP, MRPD, PROFIenergy, Shared device, MSI/MSO, I-Device, clock-synchronized mode, system redundancy and option handling? https://support.industry.siemens.com/cs/ww/en/view/102325771
\8\	Segmenting a Network Using VLANs https://support.industry.siemens.com/cs/ww/en/view/109749844
\9\	What properties, advantages and special features does the S7 protocol offer? https://support.industry.siemens.com/cs/ww/en/view/26483647
\10\	SIMATIC S7-1500 communication function manual https://support.industry.siemens.com/cs/ww/en/view/59192925
\11\	What properties, advantages and special features are offered by the protocols TCP, ISO-on-TCP, UDP and ISO Transport? https://support.industry.siemens.com/cs/ww/en/view/26171811
\12\	SIMATIC PROFINET with STEP 7 V16 https://support.industry.siemens.com/cs/de/en/view/49948856
\13\	Configuration of a Ring Topology Based on "MRP" https://support.industry.siemens.com/cs/de/en/view/109739614

No.	Topic
\14\	What should you watch out for when configuring the PROFINET MRP ring with regard to RSTP packages (Rapid Spanning Tree Protocol)? https://support.industry.siemens.com/cs/de/en/view/109759619
\15\	SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication https://support.industry.siemens.com/cs/de/en/view/59192925
\16\	C2C Communication via OPC UA PubSub with SIMATIC S7-1500 on the Basis of UDP https://support.industry.siemens.com/cs/at/en/view/109782455
\17\	DOTW: Issues with asymmetric routing https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSHCA0
\18\	PROFIsafe system description https://www.profibus.com/index.php?eID=dumpFile&t=f&f=51719&token=3ddb13f215c62bfc35ca8a5e4c4071e0c4bd006c
\19\	SIMATIC Industrial Software SIMATIC Safety - Configuring and Programming Safety-related I/O controller I-Device communication https://support.industry.siemens.com/cs/ww/en/view/54110126
\20\	Application example: Configuring Flexible F-Link Communication https://support.industry.siemens.com/cs/ww/en/view/109768964
\21\	FAQ "Configuration examples for unique network-wide and CPU-wide PROFIsafe addresses" https://support.industry.siemens.com/cs/ww/en/view/109740240
\22\	Configuring Flexible F-Link Communication https://support.industry.siemens.com/cs/de/en/view/109768964
\23\	Configuration and Application of the PROFINET I-Device Function https://support.industry.siemens.com/cs/de/en/view/109478798
\24\	SIMATIC Bus links PN/PN coupler https://support.industry.siemens.com/cs/de/en/view/44319532
\25\	Modeling the S7-1200 OPC UA Server interface in TIA Portal https://support.industry.siemens.com/cs/ww/en/view/109781701
\26\	Siemens OPC UA Modeling Editor (SiOME) for implementing OPC UA companion specifications https://support.industry.siemens.com/cs/ww/en/view/109755133
\27\	OPC UA methods for the SIMATIC S7-1500 OPC UA server https://support.industry.siemens.com/cs/de/en/view/109756885
\28\	S7 user block for the OPC UA client of a SIMATIC S7-1500 https://support.industry.siemens.com/cs/ww/en/view/109762770
\29\	How do you configure the OPC UA client of a SIMATIC S7-1500 to establish a connection via FQDN or to bypass the FQDN? https://support.industry.siemens.com/cs/ww/en/view/109771693
\30\	SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16 - Working with the TIA project server https://support.industry.siemens.com/cs/ww/en/view/109773506/128228346635
\31\	Manual – Automation License Manager https://support.industry.siemens.com/cs/de/en/view/102770153
\32\	IWLAN: Setup of a Wireless LAN in the Industrial Environment https://support.industry.siemens.com/cs/ww/en/view/22681042
\33\	PI – PROFINET & PROFIBUS user organization https://profibus.com/
\34\	PI – PROFINET Conformance Classes https://www.profibus.com/download/PROFINET-io-conformance-classes
\35\	PI – PROFINET Installation Guidelines https://www.profibus.com/download/PROFINET-installation-guidelines
\36\	Manual: SIMATIC S7-1500 Isochronous mode https://support.industry.siemens.com/cs/ww/en/view/109755401

No.	Topic
\37\	Application example: High-performance measurement technology in PROFINET environment https://support.industry.siemens.com/cs/ww/en/view/109748759
\38\	Manual: SIMATIC High-precision input/output with Time-based IO https://support.industry.siemens.com/cs/ww/en/view/82527590
\39\	Manual: SINETPLAN Siemens Network Planner https://support.industry.siemens.com/cs/ww/en/view/109485570
\40\	SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication https://support.industry.siemens.com/cs/de/en/view/59192925
\41\	SIMATIC NET: Industrial Ethernet Security SCALANCE S615 Web Based Management V7.1 https://support.industry.siemens.com/cs/ww/en/view/109751632
\42\	How do you configure and enable S7 Routing in STEP 7 (TIA Portal)? https://support.industry.siemens.com/cs/ww/en/view/109736340
\43\	Safety Reaction Time Table SIMATIC S7-1500F / S7-1200F https://support.industry.siemens.com/cs/de/en/view/93839056
\44\	Installation and operation of WinCC in a Microsoft domain environment https://support.industry.siemens.com/cs/ww/en/view/78346833
\45\	Sending SYSLOG messages with a SIMATIC S7 CPU https://support.industry.siemens.com/cs/de/en/view/51929235
\46\	SIMATIC NET: Network management SINEC INS https://support.industry.siemens.com/cs/de/en/view/109781023
\47\	Industrial DMZ Infrastructure https://support.industry.siemens.com/cs/de/en/sc/5595
\48\	User management for SCALANCE devices with RADIUS protocol https://support.industry.siemens.com/cs/de/en/view/98210507
\49\	Libraries for Communication for SIMATIC Controllers https://support.industry.siemens.com/cs/de/en/view/109780503
\50\	Connecting SIMATIC S7-1200 /S7 1500 CPUs to the MindConnect IoT Extension https://support.industry.siemens.com/cs/de/en/view/109772284
\51\	Using Certificates with TIA Portal https://support.industry.siemens.com/cs/de/en/view/109769068
\52\	Dynamic certificate management with OPC UA GDS Push https://support.industry.siemens.com/cs/de/en/view/109799888
\53\	What are the causes when connection to an OPC UA server fails? https://support.industry.siemens.com/cs/ww/en/view/109766709
\54\	Configuring standard machines in TIA Portal (configuration control) https://support.industry.siemens.com/cs/ww/en/view/29430270
\55\	Which NAT scenarios can you realize with SCALANCE SC-600 / M-800 / S615? https://support.industry.siemens.com/cs/de/en/view/109744660
\56\	SIMATIC NET: Industrial Ethernet switches SCALANCE XM-400/XR-500 Web Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109798663
\57\	S120 manual https://support.industry.siemens.com/cs/ww/en/view/109762626
\58\	S210 manual https://support.industry.siemens.com/cs/ww/en/view/109792683
\59\	Link Aggregation and LACP basics: https://www.thomas-krenn.com/en/wiki/Link_Aggregation_and_LACP_basics
\60\	SIMATIC Virtualization as a Service: https://siemens.com/sivaas

No.	Topic
\61\	SIMATIC PCS 7 Virtualization https://support.industry.siemens.com/cs/ww/en/view/51975791 WinCC Virtualization https://support.industry.siemens.com/cs/ww/en/view/49368181
\62\	PROFINET at Siemens. https://siemens.com/profinet
\63\	OPC UA PubSub with SIMATIC S7-1500 based on MQTT https://support.industry.siemens.com/cs/ww/en/view/109797826
\64\	SIMATIC NET Basics of IWLAN https://support.industry.siemens.com/cs/ww/en/view/90880063
\65\	PRONETA in SIOS https://support.industry.siemens.com/cs/ww/en/view/67460624
\66\	URLs to Siemens Industrial Edge Hub https://portal.eu1.edge.siemens.cloud/ https://portalhub.eu1.edge.siemens.cloud/ https://artifacts.eu1.edge.siemens.cloud/
\67\	https://portal-relay.eu1.edge.siemens.cloud/
\68\	Configuration of HRP rings with Standby Coupling https://support.industry.siemens.com/cs/ww/en/view/109739600
\69\	SINEC NMS for industrial networks siemens.com/sinec-nms
\70\	SINEC NMS download https://support.industry.siemens.com/cs/ww/en/view/109776939

6.4 Change documentation

Table 6-2

Version	Date	Change
V1.0	05/2022	First edition
	09/2022	Corrections in SINAMICS and SINEMA RC chapter