SIEMENS
Ingenuity for life

White Paper

Connecting two worlds

Securing the connection between industrial communication networks and enterprise IT

Abstract

To keep up with the rise of digitalization and the growing volume of data, industrial companies are looking to reliable and future-viable communications for a competitive edge. Automation networks, tailored to meet unique business requirements, must deliver dependable connections between “the automation level and enterprise IT. Working with the right partner on planning, designing and implementing industrial networks can lead to a digital transformation – efficient, digitalized processes and unfailing end-to-end communication, from the sensor to the management level.

1. The significance of industrial communication networks for digitalization

Digitalization gives industry new opportunities for profits and efficiency. Intelligent data analysis, for example, helps companies plan and optimize production processes ahead of time. It increases resource and cost efficiencies in the process industry, implements pioneering energy supply concepts and controls road and rail traffic.

Keeping up with the promises of digitalization requires gathering an ever increasing amount of data that must be recorded, stored, processed and communicated.

High-performance industrial communication networks allow the continuous, real-time exchange of data along the entire value chain and vertically to various corporate levels. These networks must meet strict performance requirements to handle the digital information load, including high availability and rugged and flexible components. They must also provide data security and plant functional safety and address the need for deterministic communication.

These requirements are especially important when establishing a secure connection between the industrial network and enterprise IT. Unless special concepts take into account the requirements of both worlds, such a connection can endanger both data security and network stability.

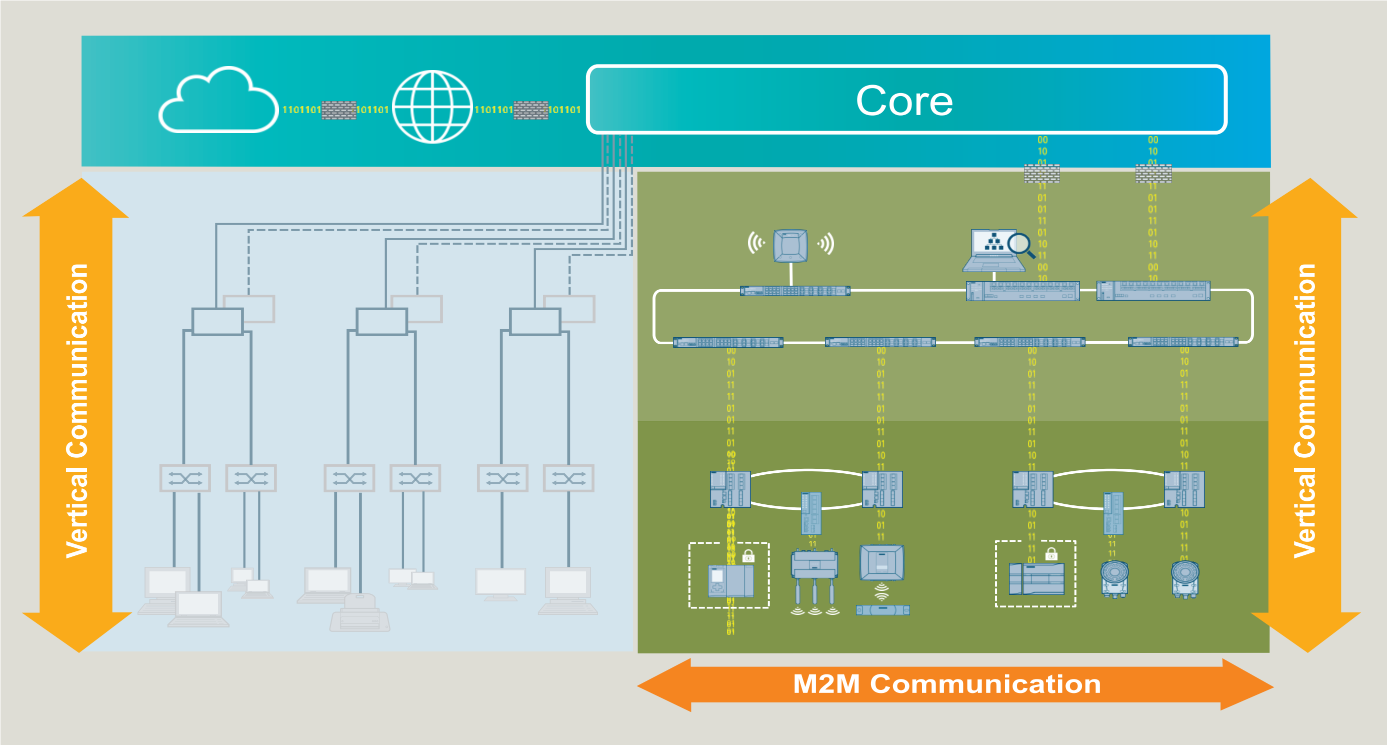
Designing, planning, and implementing industrial communication networks, and connections to enterprise IT, require a high level of expertise. It also demands a comprehensive knowledge of the specific application. Industrial networks cannot meet the requirements of the digital industry unless they are professionally planned with a view to fulfilling the specific requirements of industry and IT.

2. Differences between standard IT and industrial communication networks

IT and automation networks have basically different communication design goals. For example, IT generally focuses on frames transmission while production looks for optimum uptime. Consequently, differing requirements placed on network components and topologies must be considered to meet plant availability expectations.

2.1 Data flow

With few exceptions, office PCs communicate with one or more client or host servers. As a result, network topology is designed for much heavier, high bandwidth communication in one direction versus the other. As a rule, failures of individual clients do not impact the business and are not considered critical.



The left side of the diagram depicts a typical office structure with vertical communication relationships. The right side shows a suggested topology in production networks to meet requirements of horizontal M2M communication and vertical management system communication .

In automation, the focus is on machine-to-machine (M2M) communication and the specific application. All devices require continuous data exchange. If data is lost or delayed, it can cause plant downtime that directly impacts the business. Therefore, inter-device network communication must be performed and verified within a defined response time.

This deterministic design of communication is one of the essential differences between automation networks and standard IT. It is the prerequisite for reliable M2M communication and industrial cyclic control processes. If network components cannot meet these requirements, it may not be possible, for example, for safety applications to be reliably executed. The plant will not function correctly and will repeatedly revert to a safe, unproductive state.

2.2 Infrastructure

The differences in data flow design also affect the infrastructure of industrial communication networks.

It is difficult for a network designed purely for vertical communication with a core layer, distribution layer and access layer (as is typical of classic IT) to guarantee a continuous flow of data to the production level devices. This opens the possibility of delays that can endanger the reliable operation of the plant. Experience has shown that disruptions sometimes occur only after the plant has been in operation for some time and are often very difficult to diagnose.

Since the proliferation of Ethernet-based communication (a historical IT standard) into industrial communication networks, special network designs have been established that are specifically tailored to the applications in the various industrial sectors. This creates a natural and necessary connection between industrial communication networks and enterprise IT.

2.3 Service

Industrial ambient conditions in data centers and offices are significantly different. Consequently, industrial network components must also reliably function under harsh environmental conditions, and those including extreme heat or cold, proximity to high EMI, potentially explosive environments or even high vibration and shock, e.g. in transportation applications.

Additionally, office components are generally not tailored to the requirements of the industrial environment in terms of their design or maintenance and service-friendliness. Conversely, industrial communication networks must possess two central, service-friendly components. First, network components must be accessible to automation personnel for maintenance. Second, suitable integrated diagnostic and monitoring tools must provide fast, straightforward fault localization, especially in more complex network infrastructures.

2.4 Personnel

Fast recovery from an error or maintenance/service situation is top priority for every plant. There is often no time to wait for the IT service provider to locate and correct the problem.

Whereas outsourcing is common practice for standard IT applications, in the case of industrial communication networks company employees are often responsible for minimizing downtime from maintenance and failures. However, not every company has IT experts on call 24/7, so automation technicians must also master the network technology. It is essential in any case that this role be fulfilled by experts who can serve both as an interface between automation technology and IT, while acting as qualified contacts for both areas.

> *Training and certification programs are available, including those offered by Siemens Industrial Networks Education, that provide plant automation personnel with comprehensive communication network education.*

2.5 Safety and security

There is a distinction between functional safety and data security in the industrial environment. The term safety describes all functionalities relating to the protection of people, machine, and plants. In an emergency, it must be possible to take individual machines, plant segments or entire plant complexes to a secure state. Such an action requires an immediate and direct data transfer to the key control elements. Safety signals need to be reliably transferred with the highest priority, regardless of the media.

Industrial safety has priority over security. Nevertheless, the increase in office and automation networks demands industrial communication network operators also pay close attention to data security. In fact, security issues are where communication networks encounter the most frequent pitfalls and risks. The necessary and beneficial features in office networks can cause substantial damage in an industrial setting. Antivirus software, updates and network analyses can lead to unforeseeable problems, including plant shutdowns. Software or hardware incompatibilities can bring headaches as well.

Industrial communication networks require comprehensive, staggered safety and security concepts that cover the physical protection of the plant. They also prevent attacks by unauthorized users or non-company personnel.

With defense-in-depth, Siemens is offering a multi-layered security concept based on the three pillars of plant security, network security and the protection of system integrity that extends into the control level.

2.6 Availability

Industrial plants depend on high availability to avoid economic consequences. To this end, industrial communication network connections must be redundantly designed. Mechanisms such as duplicate devices, special network protocols and multi-path topologies, must enable and support the corresponding redundancy procedures.

Industrial backbone
The most important way to ensure high availability by means of redundancy is via the industrial backbone. The backbone must be adapted to meet the requirements of an industrial environment and installed within the industrial area so it can be accessible to trained automation personnel.

The primary task of the industrial backbone is the fast exchange of data between enterprise IT and the industrial communication network. This requires that individual cells of the industrial communication network be redundantly connected to the industrial backbone. Ring structures are generally used for this purpose. Experience has shown these structures to be a stable, clear and highly available method for setting up industrial communication networks.

The function of layer 2 redundancy protocol is to block one path of the ring and, at the same time, monitor all the other connections for correct ring functioning. If a disruption or failure of a device is detected, the blocked path is opened and a new connection established. Once the fault has been corrected, the topology returns to its original state.

2.6.1 MRP

MRP is a layer 2 ring redundancy protocol that is part of the PROFINET standard. It has a convergence time of less than 200 ms with up to 50 devices in the ring. The MRP frames move only within the ring and are not transferred between individual rings. Due to standardization, MRP exists both in automation devices and in network components.

2.6.2 HRP

Like MRP, HRP is a layer 2 ring redundancy protocol. The convergence time is less than 300 ms within a ring with up to 50 devices. The HRP frames move only within each ring and are not transferred between individual rings. With standby connections, multiple rings can be redundantly connected.

2.6.3 RSTP and MSTP

In contrast to MRP and HRP, RSTP is a point-to-point protocol, which means information is exchanged only between neighboring devices. Depending on the problem, the number of devices involved and the type of failure, the convergence times range between several milliseconds and several seconds. In the most unfavorable situation, the network requires the longest convergence time and cannot transport any data packets for several seconds. For that reason, RSTP is not the preferred protocol when it comes to real-time applications or to automation networks with the requirement of deterministic behavior.

MSTP is an enhancement to RSTP and supports different topologies for different VLANs in one physical network.

3. Connecting industrial communication networks to enterprise IT

Considering the differences between automation networks and standard IT, the question is how can organizations combine these two environments if dependable, end-to-end data transmission is a basic prerequisite for more efficient, digitalized processes?

The answer is not a matter of combining the two worlds, but of separating them. The key is to separate and decouple the industrial communication networks from the corporate network. Layer 3 separation provides a secure and cleanly designed connection between the industrial backbone and the core, thus preventing the corporate network and industrial communication network from influencing one another.

When connecting the industrial backbone to the core, care must be taken.

- Only mutual network access is permitted to maintain the industrial applications in data exchange and communication relationships
- Protection of both the data center and the office, as well as automation network, are guaranteed
- Availability and end-to-end communication consistency are guaranteed
- It is possible to monitor and control data exchange

3.1 Access rules

As described above, connecting the industrial backbone to the data center core allows direct communication isolated from the office network.

This enables MES (Manufacturing Engineering System) and ERP (Enterprise Recourse Planning) systems to exchange data directly with the automation level without unnecessary detours via the office network.

In this case, however, it makes sense to structure the industrial communication network and regulate the data exchange. This is generally done by dividing industrial communication networks into logically separated segments known as Virtual Local Area Networks (VLANs).

This type of functional segmentation of the network allows specific access rules to be implemented for each subnet in order to protect against unauthorized access. If specific individual subnets (VLANs) are not permitted to communicate with each other, this must be prevented by a suitable industrial firewall or Access Control List (ACL).

3.2 Connection types

Different methods have been established for setting up a secure connection between the industrial communication network and the corporate network: static routing and dynamic routing. In rare cases, a layer 2 connection to the core can also be used. The three connection methods are described in more detail below.

3.2.1 Static routing in combination with VRRP

In the case of static routing, the bidirectional routes between the backbone and core are entered manually. The advantage is that only the networks whose connections are desired are routed. Nevertheless, the management of static routes can be very time-consuming for large and complex networks.

Virtual Routing Redundancy Protocol (VRRP) is used with static routing. VRRP permits several routers to be combined into a logical and redundant router under virtual IP (Internet Protocol) and MAC (Media Access Control) addresses.

One router is active and works with the virtual IP and MAC address as master. The passive router (slave) monitors the active router. If the slave detects that the active router is no longer responding, it adopts the virtual IP and MAC address and, therefore, ensures the functionality of the network and the gateway. This occurs without the notice of the terminals.

3.2.2 Dynamic routing

Dynamic routing paths between the individual networks are learned automatically, an advantage found in larger or complex networks. If individual connections fail, alternative paths are automatically searched for, or known paths are enabled, for communication. Siemens SCALANCE XM-400 and XR-500 families support the RIP and OSPF industry standard protocols for the dynamic creation of the routing table.

RIP is a “distance vector” protocol characterized by ease of use and implementation. RIP automatically exchanges its routing tables with the neighboring routers. This is achieved by means of “advertisements” that are sent every 30 seconds. Due to the long-time span, however, routing changes reach the network slowly. For this reason, the RIP protocol is mostly used for compatibility reasons.

In contrast to RIP, OSPF is a “link state” protocol characterized by extreme scalability and fast switchover times in the event of an error. Each router participating in OSPF automatically sets up a network topology database for its area and synchronizes it with neighboring routers. Changes are synchronized incrementally. Based on this topology database, each router independently calculates the optimal path through the network.

With good planning, OSPF can also be used to set up very large, complex networks. This makes it an excellent choice for connecting the industrial communication network to the corporate network.

3.2.3 Layer 2 connection

In exceptional cases, a layer 2 connection can also be implemented between the industrial communication network and the corporate network. However, this should be a carefully considered and well-thought-out choice, because there is a risk that the corporate network and industrial communication network will interfere with one another, thus endangering network stability.

If network errors occur, the layer 2 connection makes troubleshooting much more difficult because the sources of the errors cannot be clearly assigned to a segment. All areas of the network can be affected. In terms of plant availability, therefore, a layer 2 connection should not be the first choice and should only be considered after careful planning.

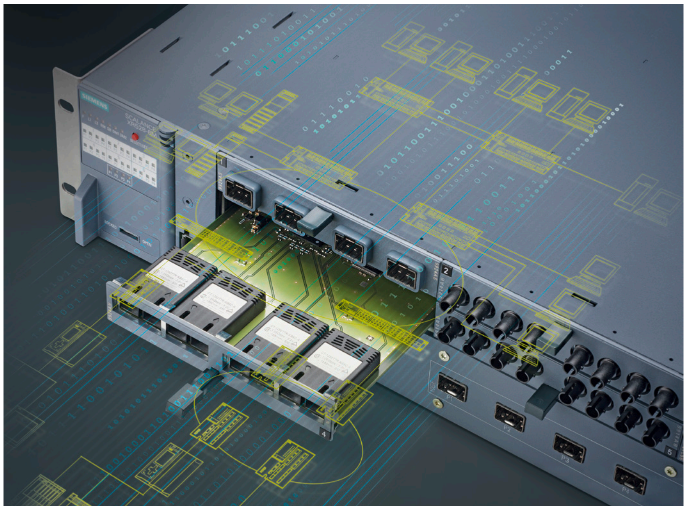
4. Securely connecting corporate networks and industrial communication networks by choosing the right partner

Industrial communication networks are more important than ever. They are essential for digitalized processes and the ability to compete in dynamic markets. These networks are more than just the sum of their components. They involve detailed planning and analysis as well as customized designs to securely and reliably connect to enterprise IT.

This includes implementing leading edge Ethernet solutions for secure, reliable and flexible communication. It requires qualified support to make the most of today’s complex industrial communication networks.

Tailor-made products

Siemens knows the requirements companies place on the connection between an industrial backbone and a corporate network. For connecting to the corporate network , Siemens offers SCALANCE XR-500 industrial Ethernet switches connecting to the corporate network. These high-performance products meet requirements for an office switch as well as the special challenges of industrial devices.



www.siemens.com/x-500

Properties of the SCALANCE XR-500

- Highly flexibility for network expansions and retrofitting as well as reduced warehousing costs as a result of the fully modular design. Electrical or optical networking via combo-ports (SCALANCE XR-524 8C/XR-526 8C) are possible even while in operation (hot-swappable)
- Optional retrofitting of Layer 3 functions via a key plug without changing the hardware
- High availability through redundant power supply, C plug removable medium and redundancy functions
- Models with different power input (AC/DC) and optionally redundant power supply
- Transmission of large amounts of data with 10 Gbit/s ports
- The modular switches SCALANCE XR-528 and XR-552 feature high connection density and flexibility for different transmission

Professional Services

Siemens Professional Services for Industrial Networks offers comprehensive services and support to help plan and implement industrial communication networks. Expect consulting services related to network design, detailed site analyses, implementation services to ensure fast commissioning and training courses that ensure performance. Professional Services team supports you every step of the way.

On-site Service and Support

Where does your current network stand? Let us take a comprehensive look, make an assessment and provide best recommendations for a plan that works for you.

Integration and Deployment

When it's time to install and deploy, don't take any chances. Ensure success with our proven pre-configuration, testing and implementation services.

Design and Consulting

If you are ready to expand or upgrade, we can help you get going. This is one way to avoid a piecemeal approach and realize improvements throughout the entire network.

Training

Round out your in-house expertise by filling any knowledge gaps within your organization. We offer standard or customized training to meet your unique needs.

www.usa.siemens.com/industrial-networks-services

A White Paper issued by: Siemens.

Training and certification offerings

Our Industrial Networks Education training and certification program helps companies train personnel in industrial communication networks. The program includes switching and routing, security, all the way to wireless networks. Industrial Networks Education communicates expert knowledge in all relevant areas. Automation personnel are perfectly equipped to work with industrial communication networks and become the interface between automation technology and IT.

Technical Training

Siemens Industrial Networks Education	Customized Trainings
• Industrial requirements • Technical deep drive • Hands-on • Interdisciplinary topics • Certification	• Training courses tailored to customer-specific needs

www.usa.siemens.com/industrial-networks-education

Siemens offers a comprehensive portfolio of network products, services and certified training programs. As a solution provider, Siemens has many years of experience and in-depth expertise designing and implementing future-proof industrial network solutions, all supported worldwide by certified and well-established Siemens industrial partners.

Siemens Industry, Inc.
5300 Triangle Parkway
Norcross, GA 30092

For more information, please contact
our Customer Support Center.

Phone: 1-800-241-4453
E-mail: info.us@siemens.com

usa.siemens.com/industrial-networks

A White Paper issued by: Siemens.