



Leading the World in
Industrial Networking
and Communications

PROFINET AND IT

Table of Contents

EXECUTIVE SUMMARY

MOTIVATION – NEW TRENDS IN AUTOMATION

INDUSTRIAL ETHERNET – PROFINET

Different approaches for Industrial Ethernet
PROFINET – Overview

SPECIFIC CONDITIONS IN AUTOMATION

Fact 1 – Network structure and network nodes
Fact 2 – Communication structure
Fact 3 – Bit rate and packet rate
Fact 4 – Addressing and subnetting
Fact 5 – Protocols used
Fact 6 – Realtime communication
Fact 7 – Environmental conditions
Fact 8 – Installation requirements
Fact 9 – Availability and redundancy
Fact 10 – Security
Fact 11 – Operation / management / diagnostics / remote access
Summary of specific conditions

NETWORK CONNECTION OF AUTOMATION AND OFFICE

Important planning aspects
Scenario 1 – Separate physical and logical networks
Scenario 2 – Logical integration into the overall network
Scenario 3 – Separate logical networks (closed user group)
Summary of network connection

APPENDIX

References
Abbreviations

EXECUTIVE SUMMARY

PROFINET, a market-leading Industrial Ethernet protocol, encompasses all levels of a network, ranging from the physical infrastructure to the Ethernet network access layer and the TCP/IP layer and finally to the application layer. The structures and topologies of conventional network technology used in IT and in automation differ only in the machine-level area of the automation system; the superordinate levels of the network are essentially identical. As a result, PROFINET can be easily integrated into existing network environments.

The integration or connection of automation areas does not affect the superordinate network communication to any significant degree because the data traffic, which is mainly cyclical in nature, is predominantly limited to local data traffic. Increasingly, communication with centralized devices is becoming necessary, but this constitutes neither the major portion of the automation applications nor the major portion of the superordinate network. The communication demands of automation do not require faster data transmission rates on the overall network. In this regard, the PROFINET-generated communication can be categorized the same as any other additional application.

Like Office applications, PROFINET applications use the TCP/IP protocol and IP services. Depending on the number of automation areas to be integrated, the number of IP subnets to be addressed within the overall network can increase significantly. This necessitates use of a comprehensive address concept for office and automation areas, which also takes into consideration the use of private IP addresses, if applicable.

PROFINET allows applications with a wide range of different realtime requirements to be implemented. In the automation environment, realtime requirements exceeding those specified in the multimedia environment must often be met. PROFINET satisfies these specific requirements by adapting different realtime scenarios in which, however, communication still remains limited to the machine level, i.e., in one logical subnet and in one broadcast domain, so that no special preparation of the superordinate network is necessary.

Passive and active PROFINET components meet all requirements anticipated in harsh industrial environments. However, these unfavorable environments cannot be assumed as the blanket condition for all types of communication in industry, and as a result components suitable for IT use can also be considered up to a certain point. In terms of cabling, the international standards have been expanded for industrial cabling. However, these standards do not necessarily apply at the machine level. The specific cabling standards in the PROFINET specifications must be considered there.

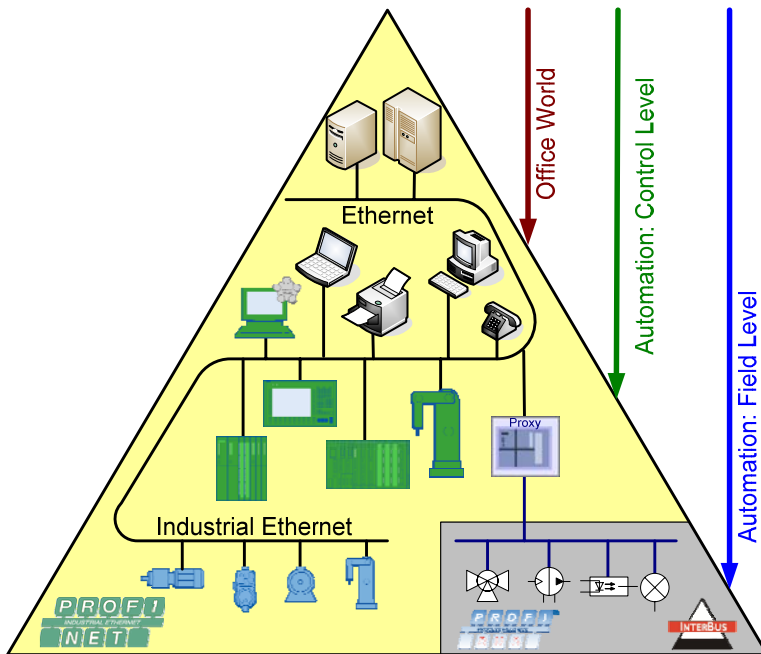
As long as the data communication occurs independently within the automation cells, the availability of the superordinate network plays no crucial role here. Specific measures for increasing the availability are not necessary. The availability within the automation cells themselves can be improved by taking suitable measures. For example, components with a longer lifetime and with simplified replacement and repair possibilities can be used. Redundancy mechanisms can also be introduced.

The operation of automation systems is dominated by the requirement of simplicity. In addition to simple options for replacement and configuration, PROFINET also provides comprehensive diagnostics. In addition, it is possible to link to the central SNMP management of the overall network in order to monitor the network technology.

A significant technical challenge associated with introduction of PROFINET is related to the separation or connection of the IT world and the automation world. Security and operation aspects, among other factors, play a large role here when planning the overall network.

MOTIVATION – NEW TRENDS IN AUTOMATION

In most companies, the days of operating automation systems as isolated systems are long past. For a number of years, automation components such as controllers and control PCs have been communicating with centralized computers and servers. These centralized computers are normally located in centralized network areas, same as in the IT world, and must therefore be accessible via the network administered by IT personnel. With rising flexibility of the automation, this communication is constantly increasing, and the growing penetration of this communication is becoming an integral part of entire automation. Thus, the stepped-up integration of automation areas is becoming an increasingly important criterion for company success.

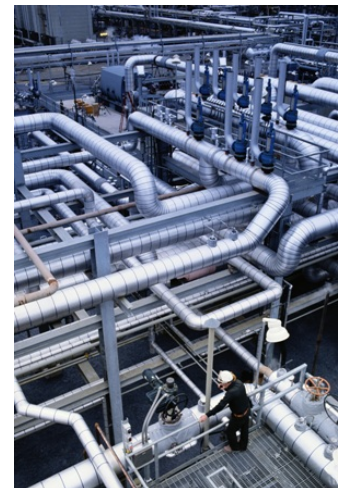


In addition, more and more automation system components, such as IO devices, valves, and drives, are connected to controlling components via Ethernet. Due to this trend, the use of Ethernet is becoming more and more common for connecting the devices of the field level. However even so, the great number of Ethernet-linked automation devices requires rethinking network structures: the line structures frequently dictated through the use of fieldbus systems are being replaced by switching structures (same as in the IT world). Line structures are retained only at the machine level and are now implemented using cascaded switching components. The large flat networks, which represent one broadcast domain, give way to a network structure divided into logical subnets. Here, many companies are benefiting from synergy effects between IT and automation by taking advantage of IT experience in the effective operation of large networks with many nodes.

Automation systems require specific network structures at the machine level, whereas the used Ethernet structures for superordinate levels of the network are similar for IT and automation. For this reason, many companies prefer a comprehensive integration of the automation areas into the IT. Large network areas can be set up, used, and operated together, thus enabling the best possible return on investment for the complete network.

Closely tied to the use of Ethernet is the use of the TCP/IP protocols – ubiquitous in the IT world. The stability and long-standing experience associated with TCP/IP applications make the TCP/IP protocol a widely sought-after basis for non-time-critical applications, even in automation applications. Optimized protocols are being used for time-critical applications, which mostly communicate within automation cells.

This is accompanied by the increasing interaction of management and diagnostics of automation systems resulting from the growing permeability of communication and the integration of networks. More and more automation cells are monitored and configured by centralized diagnostic servers located in the central areas of the



overall network. Integration of automation network components into a centralized SNMP management is increasingly common.

Besides the numerous similarities, during network implementation, specific circumstances of automation must also be considered. In addition to the installation of automation devices in different environments, the different communication requirements, such as realtime behavior, must be taken into consideration. The next section highlights the specific requirements and circumstances associated with automation, and defines options for integrating the two heretofore different worlds - one dominated by office applications and the other defined by automation applications. Ethernet and TCP/IP are used in both worlds. The term "Industrial Ethernet" is given to the adaptation of Ethernet to the specific conditions in automation.

This document should not be viewed as an installation guideline or a planning document. Rather, it describes the fundamental differences of the two network worlds and illustrates the principle for integrating Ethernet-based automation communication into an overall network that is also used for office environments, telecommunication, building services, and logistics (hereinafter referred to as the "office world").

INDUSTRIAL ETHERNET – PROFINET

Industrial Ethernet generally refers to networks that use Ethernet as defined in IEEE 802.3, supplemented by mechanisms for assuring quality of service, for the purpose of networking nodes in automation systems. Industrial Ethernet is also used to describe variants that use Ethernet with modifications or that use radio technologies. Actual Industrial Ethernet implementations include not only the media access layer, i.e., Ethernet or radio technology, but also the entire OSI stack from the physical layer with cabling systems, plugs, and components adapted to automation environments, up to the application layer. OSI layers 3 and 4 use the TCP/IP protocol or proprietary protocols to ensure realtime communication; the specific automation applications are based on these.

In pursuit of this trend, various manufacturers and associations have expanded their fieldbus variants to include an Industrial Ethernet variant, in which automation applications known up to now in fieldbus networks can continue to be used. One of the most widely used Industrial Ethernet variants is PROFINET, developed by PNO, which covers all aspects of industrial communication.

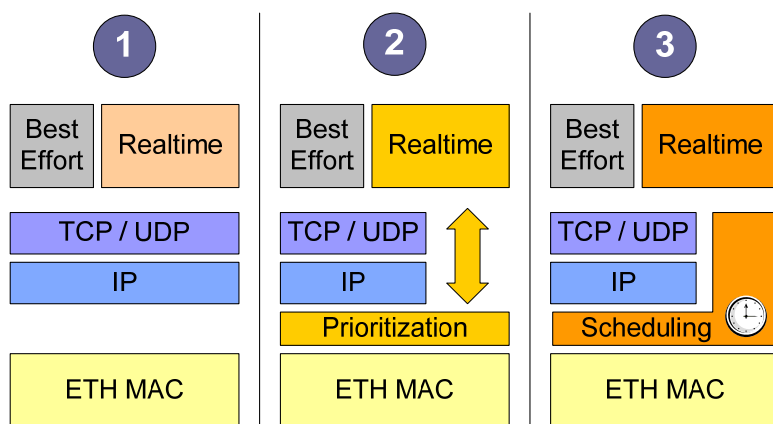
Different approaches for Industrial Ethernet

Three basic approaches for Industrial Ethernet can be identified. These are characterized by the different types of adaptations made to Ethernet and the TCP/IP protocol.

1. Use of standard Ethernet as defined in IEEE 802.3 and TCP/IP

This approach precisely corresponds to implementations in the office world. The office-specific applications are replaced by automation-specific applications on the application layer only. This type of solution can be used in environments whose performance requirements are equivalent to those in the office world.

2. Use of standard Ethernet as defined in IEEE 802.3 and prioritization according to IEEE 802.1Q as well as TCP/IP and specific automation protocols on OSI layers 3 and 4



Dependent on the performance requirements for automation communication, this approach provides different "communication channels" – one TCP/IP channel for applications whose performance requirements are equivalent to those of the office world (Best Effort), and one realtime channel that bypasses or replaces the TCP/IP protocol to enable use of applications with more stringent realtime performance requirements.

3. Use of optimized Ethernet stack as well as TCP/IP and specific automation protocols on OSI layers 3 and 4

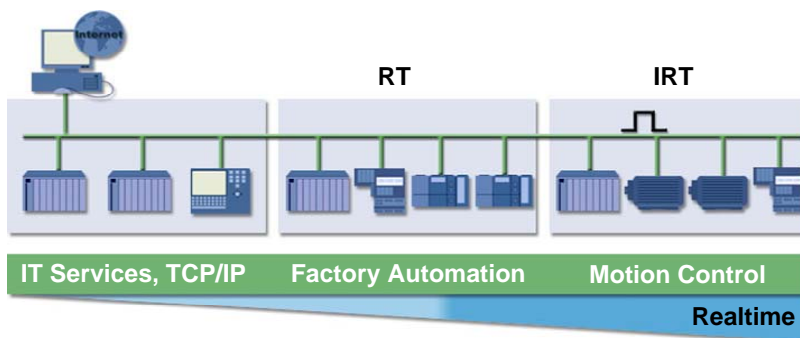
This type of approach is required for automation systems if applications with deterministic data transmission and maximum realtime performance requirements must be implemented, e.g., axis control. However, this approach also covers all communication types by

offering various communication channels that can be used in parallel: Based on adaptation of the Ethernet stack and scheduling, one TCP/IP channel and one or more realtime channels that bypass the TCP/IP protocol are available. Determinism is implemented through the use of a time slot procedure (scheduling) that provides fixed transmission cycles of the highest performance class and through cyclic synchronization of all nodes. This approach normally requires use of special switches.

PROFINET conforms to variants 2 and 3 and thus enables realization of many different automation scenarios having the full range of realtime performance requirements. PROFINET includes all aspects of industrial communication and is standardized as an open system in IEC 61158.

PROFINET – Overview

The modular PROFINET concept distinguishes among different types of communication for satisfying various response time requirements:



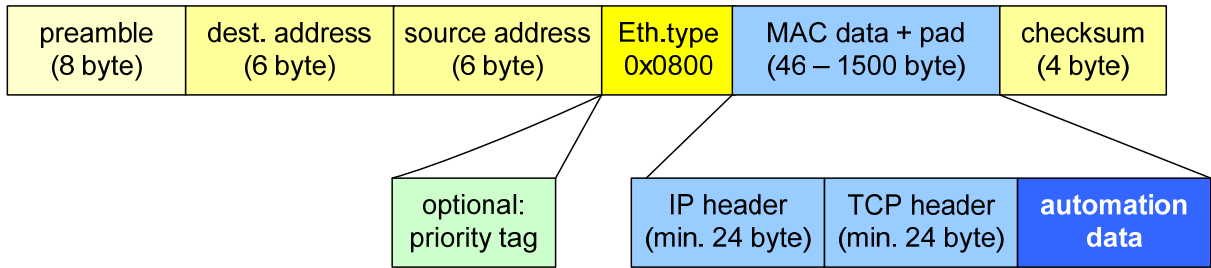
- No specific performance requirements
- Increased performance requirements – Realtime (RT)
- Maximum performance requirements – Isochronous Realtime (IRT)

In addition, PROFINET distinguishes between different types of communication according to the nodes to be connected:

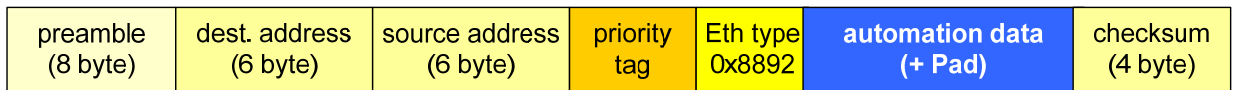
- PROFINET IO implements communication between controllers and IO devices with RT and IRT requirements.
- PROFINET CBA (Component Based Automation) is suitable for communication among controllers via TCP/IP as well as additional RT requirements.

It is possible to use all types of communication in parallel on the same network, and proxy components can be used for transition to nodes in traditional fieldbus topologies, e.g., PROFIBUS. Likewise, PROFINET supports communication via radio technologies, e.g., WLAN, for connecting IO devices.

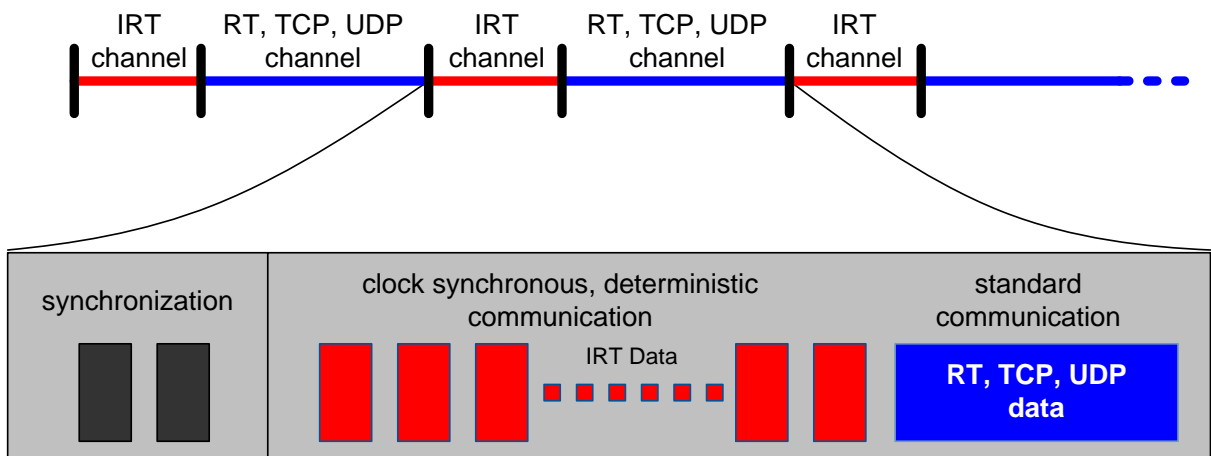
Most PROFINET communication occurs via Ethernet and TCP/IP packets without any modification. This enables integration into a common network with office applications without limitations.



RT communication not only uses prioritization of Ethernet packets but also an optimized protocol stack on OSI layers 3 and 4. This protocol stack does not have any routing capability. This means that RT communication is restricted to one logical subnet. However, a layer 3 topology enables parallel TCP/IP communication with centralized computers on the overall network.



IRT communication for maximum realtime requirements, especially for isochronous applications, is based on an extension of the Ethernet stack for the purpose of synchronizing all communication partners and on the use of scheduling, i.e., a time-slot technology. IRT communication requires the relevant network area to be equipped with special IRT switches that reduce the integration into the overall network to the connection of closed communication areas based on layer 2. The topology can have a transition to the overall network and can enable parallel TCP/IP communication.



SPECIFIC CONDITIONS IN AUTOMATION

The term "automation" is associated first of all with factory floors where vehicles, printing equipment, and the like are produced. But automation also applies to many more industries where Industrial Ethernet is used. The main branches of automation are:

Factory automation



Manufacturing automation is involved first and foremost in automotive industry, mechanical engineering, plant manufacturing, and the electrical industry. It represents an important driving force behind the dissemination of Industrial Ethernet. The number of nodes in these types of production facilities, together with highly-flexible manufacturing that requires communication between automation devices and centralized production control systems, has soon been a motivation for the use of well-established office technologies like Ethernet.

Even special conditions for communication in tunnels, in building and underground construction sites, during transport, and in traffic (rail, road, and water) are taken into consideration within Industrial Ethernet.

Process automation

Process automation is involved in a wide variety of industries, ranging from chemical and pharmaceutical manufacturing and mining operations to paper and food processing. Process automation is also used in highly sensitive industries such as refineries, oil and gas processing plants, and water and wastewater treatment plants.



A common factor in all branches of automation is the strong dependency on plants manufacturers. The plants manufacturer's specifications regarding operating system, remote maintenance, etc., are frequently binding and must be taken into account through use of suitable measures in this specific application area. Devices with a heavily restricted application scope and a specific realtime operating system (high performance with little memory requirement) are normally used. Often, exactly one application per device is used. However, there are also devices that are based on a universal operating system and thus are subject to the same risks as components in the office world.

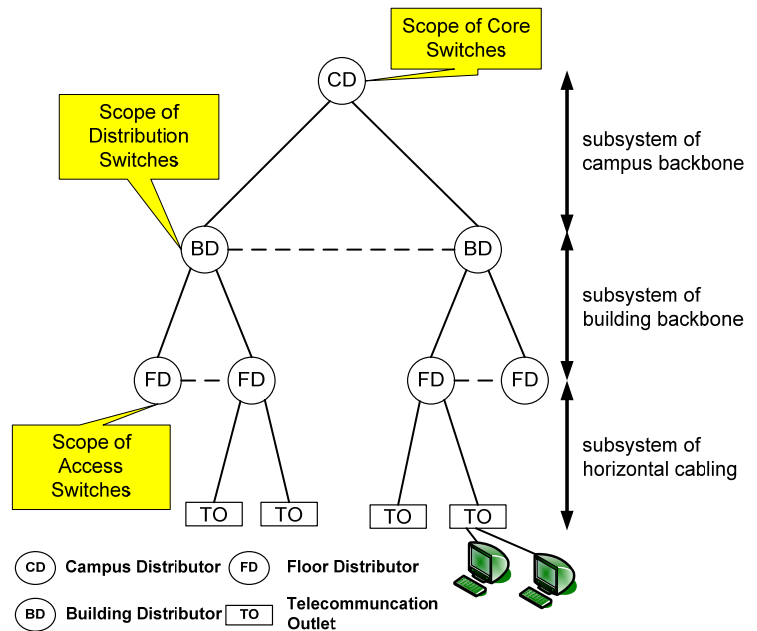
The specific circumstances and the resulting conditions and requirements are grouped into various "Facts" and presented below. A brief description of the situation as it exists in the IT world (office world) is presented for each fact along with information highlighting how the situation differs in automation. Finally, consequences for the IT world as a result of integration are presented in each case.

Fact 1 – Network structure and network nodes

The network structure encompasses the passive network topology, i.e., star, ring, or line, as well as the logical network design with active network elements, i.e., layer 3 and layer 2 switches.

In the office world, a hierarchically intermeshed network topology becomes accepted, which is based on layer 2 and layer 3 switching and provides for a star-shaped connection of end devices. These end devices are comparatively homogeneous with regard to intelligence and comprise PCs, work stations, servers, hosts, and multimedia devices such as IP phones. An important characteristic of office world technology are the short innovation cycles. In some cases, these measure only a few years and involve frequent replacement of system, operating system, and network components.

In automation, control processes are predominantly run in series. An automobile assembly line provides a very good simplistic image of this process. This serial process results in a line-shaped arrangement of machines and, thus, of communication nodes. Nodes can thus be linked in the simplest possible manner using a line or tree topology. Line topology is used preferentially in the horizontal area, while star-shaped topology in the primary (campus) and secondary (building) areas remains unaffected by this.

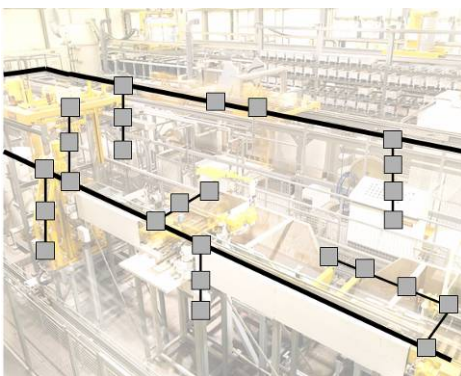


Devices in automation differ significantly. In addition to intelligent devices for control and monitoring of automation systems, such as

- robots,
- controllers, and
- the user's interface to monitor and control the machine or process (HMI devices),

there are also simple devices used at the field level, such as

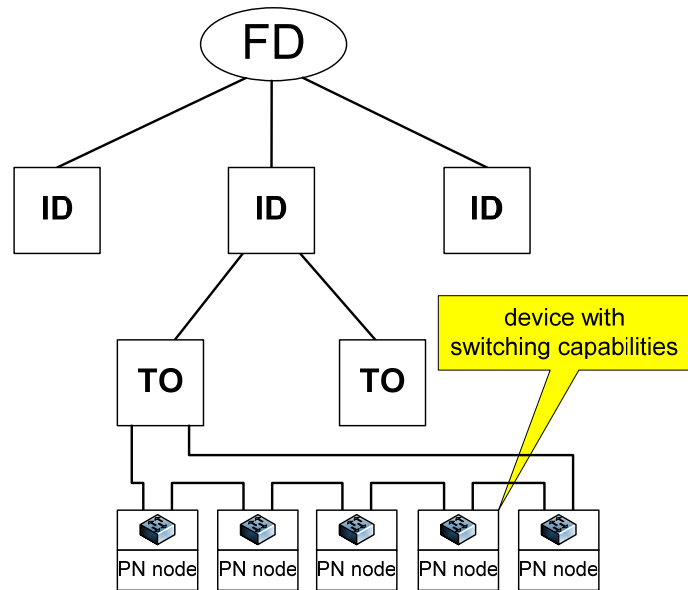
- I/O devices (sensors and switches),
- drives, and
- embedded systems.



A special type of network node is represented by devices that function both as a terminal and as a network switch. In the office world, such devices are only known in form of IP phones with integrated switches. Automation systems frequently contain devices that are used as input/output devices for control elements while simultaneously having an integrated switch. They can be operated as an IO device within the required PROFINET communication, and they can also forward a data packet to the next network node. This "combo-function" enables simple implementation of

a line topology, which is especially suited for use in automation. Pure network elements corresponding to conventional switches used in the office world can often be avoided.

In discussions of many standards committees regarding integration of topologies typically found in automation, such as line topology, attention was given to the method for connecting this environment to the 3-level hierarchical topology established in EN 500173-1 (cabling standard). As a result, the 3-level hierarchy was expanded to include a further level – the intermediate distributor (ID) and the intermediate cabling leading from it (for specification, see EN 50173-3).



The scope of the current cabling standards EN 50173-1 and 50173-3 for IT communication cabling thus extends up to and including the TO (telecommunication outlet) element. In contrast to the office world, however, not only end devices are connected to this element. Instead, a further network, e.g., with PROFINET devices, is normally set up starting from this point. It must be noted that the associated cabling components are no longer subject to the specifications in EN 50173-3 and in many cases the operating staff for the overall network is no longer in charge.

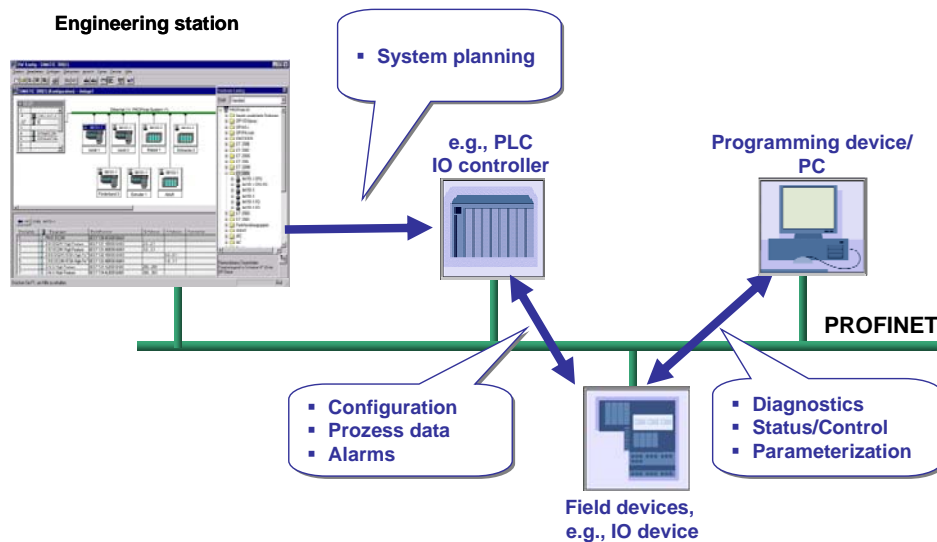
Automation networks are integrated or connected using current structuring approaches of the office world without any modification. In particular, EN 50173-3 points out the possibility for combining the two worlds in terms of the cabling structure. The multi-level approach well-proven in the Ethernet world for setting up an active network using core, distribution, and access switches can also be used to a large degree. However, the structure differs significantly in the direct area of automation communication, i.e., at the machine level. Here, line or ring topologies are used preferentially.

Automation networks are integrated or connected using current structuring approaches of the office world without any modification. In particular, EN 50173-3 points out the possibility for combining the two worlds in terms of the cabling structure. The multi-level approach well-proven in the Ethernet world for setting up an active network using core, distribution, and access switches can also be used to a large degree. However, the structure differs significantly in the direct area of automation communication, i.e., at the machine level. Here, line or ring topologies are used preferentially.

Fact 2 – Communication structure

Office communication is dominated by client-server communication with mostly long packets produced by file transfers and multimedia data prevalent there. Smaller data packets are produced exclusively in database or terminal applications. A common factor in all types of office communication is the ability to transmit packets acyclically and the lack of specific requirements for determinism, delay, and jitter (exception: multimedia applications).

The architecture of complex automation systems means that communication flows vary widely within the automation world. Such complex automation systems are frequently subdivided into multiple automation cells.



- In controller-device structures, one control component within an automation cell, e.g., the controller in a robot, controls multiple devices at the field level that communicate exclusively with this master.
- Peer-to-peer communication takes place between control components within one automation cell as well as between different automation cells.
- The client-server communication typical in the office world also takes place in the automation world in conjunction with automation processes (engineering) between control components and central hosts as well as for downloading software and performing backups.
- Direct data exchange occurs between devices at the field level, i.e., forwarding of process data within an automation cell.

PROFINET applications generally differentiate between cyclic and acyclic data traffic, whose transmission via Industrial Ethernet must be reliable and deterministic according to performance requirements, mostly within an automation cell. The majority of packets are allotted to cyclic data exchange, e.g., measured values or general process data are transmitted at fixed times. These cyclic data must be transferred at fixed times within the required time blocks (delay, jitter, see Fact 6) according to the realtime requirements. With the most stringent realtime requirements, e.g. PROFINET applications with IRT, PROFINET also uses continuous synchronization of nodes within an automation cell as defined in IEEE 1588. Among other things, acyclic data include alarm messages that are used by sensors to inform the controller about critical states. For the most part, PROFINET applications produce symmetrical communication both within an automation cell and within the overall network, i.e., approximately the same amount of data is transmitted in both communication directions.

In controller-device and peer-to-peer communication, most data packets have the minimum length according to Ethernet and contain little process or alarm data. Long packets for parameterization or backup occur with client-server communication, but are much less common. Applications that communicate based on broadcasts and multicasts also affect the structure to be selected for the overall network. While multicasts have become more common in IT networks and commonly used network elements offer support for this, broadcasts still require establishment of a single broadcast domain or a logical subnet for all nodes involved.

There are consequences on the network structuring, since PROFINET applications use broadcast or multicast packets.

For broadcast communication, the nodes involved should be separated in one logical subnet so that nodes not involved do not have to process the broadcast messages. When networks for such automation environments are planned, the broadcast areas must be carefully planned to avoid oversized subnets. Experience in the office world suggests that subnets should be limited to a manageable number of nodes in automation areas, as well. Exceptional cases that require large subnets must be carefully planned and monitored.

Multicast-based communication requires similar consideration when selecting network elements.

Fact 3 – Bit rate and packet rate

The first step in examining the expected bit rate is to distinguish between non-time-critical communication and realtime communication (both IRT and RT). The latter is characterized by a large number of short packets that are mainly transmitted within an automation cell. Therefore, a high bit rate is not to be expected within automation cells. This is reflected in the rather conservative demand for transmission media with moderate transmission capacity required by automation. Up to now, a bit rate of 100 Mbps is viewed as completely adequate for automation. If an application requires non-time-critical communication between an automation cell and centralized control computers, TCP/IP-based communication will normally be used, e.g., download of a CNC program with modest bandwidth requirements.

If one or more automation cells are connected to the superordinate network, a maximum transmission rate of 100 Mbps is also frequently required. Still, the current market situation is that Gigabit uplinks are the de facto standard for switches, and this Gigabit data rate is preferred in spite of the fact that it is not required. The length restrictions of Gigabit technology must be taken into consideration during the network planning phase. Trends in the office world toward even higher data rates – up to multiples of 10 Gbps – has no relevance in automation.

In addition to planning of uplinks and integration of automation cells into the overall network, an evaluation must be made to determine whether the backbone switches and server connections in the overall network must anticipate higher packet loads. Now, not only the established office communication, i.e., data, voice, multimedia, have to take place over the overall network but also the communication of automation applications. A significant increase in the network and component load is not to be expected since the main automation communication remains locally restricted.

There is no need to prepare or expand the overall network to transmit higher data rates when automation systems are integrated, since typical backbone architectures have sufficient capacity reserves.

Fact 4 – Addressing and sub-netting

The address structure typical in the office world can be applied only conditionally to automation. The office world with comparatively few connected end devices per floor unit do not require static addresses as a result of their solely client-server communication but use dynamic addresses assigned via DHCP. In Contrast to this, the automation world uses addressing that is more like address assignment of server areas. Static addresses are customary or even mandatory in both areas. However, PROFINET devices can also obtain the configuration from a memory stick, a superordinate node, or a server when the system is started.

In addition to intelligent nodes with DHCP capacities, the automation also comprises a number of very simple components that are configured only via local mechanisms (memory stick, manual configuration) or within a PROFINET cell via DCP (Discovery and Configuration Protocol) – the PROFINET service for reading out and setting device parameters, such as names and IP addresses. In order to simplify the installation and configuration of such components to the maximum degree possible, e.g., to allow replacement of components by personnel without special training, the devices are pre-installed in many cases or the system configuration is 100% copied. In some cases, different parts of the plant are given the same address ranges, and the same components even receive identical IP addresses. Nevertheless, these address ranges must be integrated into the overall network. Suitable measures such as the use of an intermediate NAT component [Network Address Translation] can ensure the communication of the subsystem within the overall network.

The large number of nodes in automation means that an adapted subnet structure is required on the overall network. Depending on the size of the automation area, the number of additional automation subnets to be integrated can exceed that of the office area several times over. The number of automation subnets cannot be reduced or can be reduced only conditionally, because a flat address and subnet structure with few logical subnets should only be used in exceptional cases. Subnets containing a maximum of 254 nodes represent the rule for automation, just as in the office world.

When automation areas are integrated into the overall network, the address and subnet structure of the overall network must be checked in advance and adapted, if necessary. Besides the number of subnets to be integrated, the security concept also plays a decisive role when planning the address structure. Different alternatives must be weighed here and these also have a bearing on which IP services (DHCP, DNS, and possibly NAT) can be used. Possible alternatives include:

- Use of registered or private address ranges for automation
- Separation of the office and automation areas into different address ranges
- Structuring of subnets according to organizational or geographical aspects

The increasingly recognizable trend toward IPv6 in the office world cannot be noticed in automation; many devices cannot process the complex IPv6 headers on account of their limited memory and processor capacities. For integration into an overall network, this constitutes no restriction because a migration from IPv4 to IPv6 lasting years or even decades using appropriate proxy components can be expected throughout the IT world.

Fact 5 –Protocols used

Nodes in IT structures of the office world use TCP/IP exclusively as the basis for communication, irrespective of the underlying network access layer and the application being run on it. All applications in the office world and similar fields are meanwhile migrated to the TCP/IP protocol. Even "dinosaurs" such as the SNA protocol, which was long used for mainframe computer communication, have been using TCP/IP-based communication for many years. A similarly homogeneous communication protocol basis does not yet exist in the automation world and will not be available any time soon either due to the realtime requirements. Approaches can be identified in many cases in which the synergy effects resulting from TCP/IP can be exploited for as many use scenarios as possible, even in automation. Older production-related, proprietary protocols, such as DECnet IV have been successfully migrated to TCP/IP, and new applications without specific realtime requirements are being developed directly on the basis of TCP/IP.

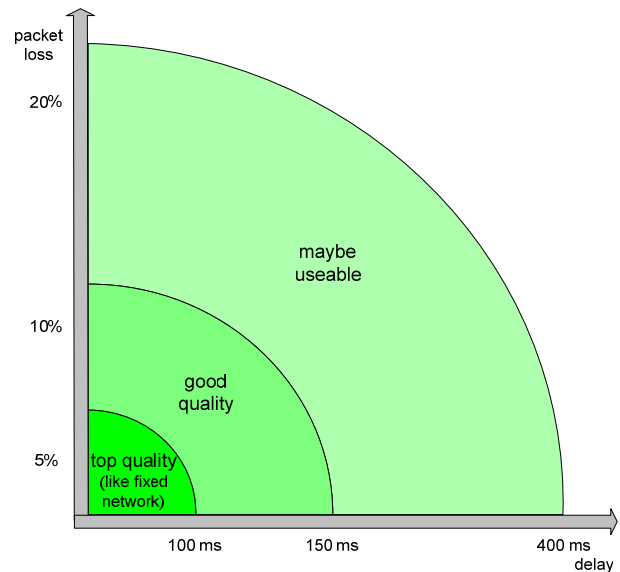
The following protocols are generally used (also in parallel) with PROFINET applications:

- For non-time-critical communication, PROFINET generally uses TCP/IP. Such communication takes place during system engineering, for production process diagnostics, and via the Human Machine Interface (HMI). This type of communication can be transmitted on the overall network without any limitations. In addition, the connection between the controller and subordinate devices is established via TCP/IP.
- If realtime adaptation is necessary, additional protocols are used that bypass the TCP/IP stack, e.g., PROFINET with RT and IRT. These types of protocols can only communicate within a broadcast domain because routing capability was eliminated in favor of faster transmission.
- Automation applications use the Link Layer Discovery Protocol (LLDP) – a layer 2 protocol conforming to IEEE 802.1AB – for diagnostic purposes and for topology detection. Each LLDP device sends cyclic information about itself to the local link in the form of an Ethernet multicast; however, this multicast is terminated at the next switch, i.e., it is not transmitted further.

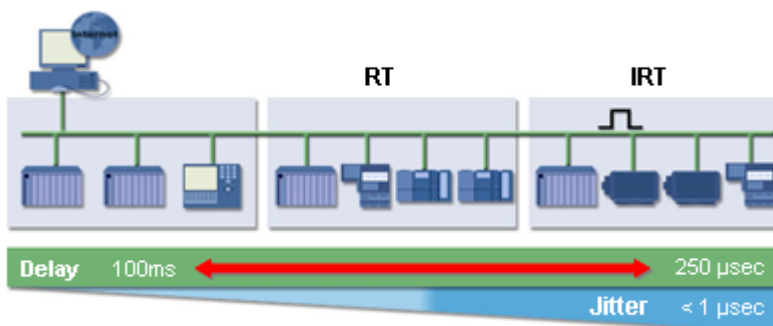
Automation areas with industrial protocols such as PROFINET can generally be integrated into the overall network without any problem. However, realtime communication must be considered when structuring the network. PROFINET with RT or IRT communication can communicate only within a layer 2 domain, which must also be taken into account in the network design. PROFINET communication via TCP/IP fully satisfies the routing capability requirements of the overall network and, thus, no specific adaptation of the overall network is required. Supplemental QoS mechanisms (Quality of Service), such as use of the priority byte in the Ethernet packet (IEEE 802.3Q), are also used in many office environments for purposes of ensuring VoIP via MAN/WAN and thus do not limit the integration of Industrial Ethernet or PROFINET.

Fact 6 – Realtime communication

Realtime communication is also a known concept in office applications. The transmission of voice and multimedia data is generally referred to as realtime communication, and the protocols used are called RTP/RTCP (Realtime Transport (Control) Protocol, based on UDP). The maximum delay required for VoIP and other multimedia data does not match the requirements of automation applications. While a 150 ms delay in VoIP is still enough to guarantee good quality for voice communication, realtime in the context of PROFINET means a delay of less than 100 ms. PROFINET applications with IRT, i.e., with maximum performance requirements, require an even shorter delay of 250 μ sec.



Besides the delay, another critical variable for ensuring deterministic transmission of cyclic data, e.g., for isochronous drives, is the jitter, meaning the variation in the delay. PROFINET applications with IRT requirements may necessitate jitter values less than or equal to 1 μ sec. In automation, cyclic data mainly take the form of regularly exchanged process data of IO devices, sensors, etc., which must be transmitted at fixed times. The tolerance for variations in the arrival time of data is extremely low for RT and IRT applications. Too much variation can shut down entire automation systems.



In order to guarantee deterministic transmission of cyclic data for applications with the most stringent realtime requirements, PROFINET uses an extension to the Ethernet stack (IEEE 1588) to ensure that the nodes of an automation cell are in synchronism.

A possible solution for integrating time-critical applications such as VoIP in the office world and realtime applications in automation is the introduction of prioritization mechanisms for the corresponding application packets. Numerous tests to determine voice readiness in IT networks have concluded that modern IT networks meet the requirements of VoIP even without prioritization and that no benefit is gained by introducing prioritization. An evaluation must always be performed to determine whether new applications on the network necessitate introduction of QoS due to stringent requirements for jitter and delay. According to the PROFINET specification, applications that use PROFINET with RT or IRT must use Ethernet prioritization, but are expected to play a subordinate role on the overall network due to the fact that the data traffic is concentrated locally.

The realtime requirements of PROFINET applications based on TCP/IP communication having realtime requirements correspond to the requirements for delay and jitter of voice and multimedia applications. Thus, in spite of realtime requirements for introduction of network-based PROFINET applications, no new design or even implementation of QoS techniques in the existing superordinate network is necessary.

Fact 7 – Environmental conditions

By far the largest market share of network elements has been developed primarily for the office world. The conditions are ideal; often, only network elements, i.e., switches, are placed in their own wiring closets or cabinets. It is understandable that these ideal conditions disappear as the proximity to machines increases and the distance from these types of protected areas increases. In particular, the following conditions must be assumed in industrial environments:

- High quantities of dirt and dust in solid and liquid states
- High mechanical loads in the form of vibrations and shocks
- High or low temperatures ranging from -40°C to +70°C
- Very limited assembly space
- High humidity of up to 95%
- High electromagnetic loads

The increasing networking of communication nodes in the automation area increases the number of data connections and, thus, links. In order to place the network elements, such as switches, in a central location, very long cables would be required, which would increase the cabling effort significantly. As a result, network elements (mainly switches) are needed that can be installed and operated close to the machines. The more stringent requirements described for these components preclude the use of standard office switches at the machine level. The particular operational environment determines whether LAN components must be protected against "environmental adversities" and, if so, which ones.

A further difficulty posed by the use of standard office switches is the ability to install them in or on the machine. Here, space-consuming 19" technology cannot be used. Instead, space-saving technology must be selected that can make use of the installation infrastructure on-site. As a consequence, smaller switches, typically having fewer than 10 ports and suitable for DIN rail mounting, are used. Typically, a 24 V DC power supply is used at the machine level, i.e., in automation cells, rather than a 230 V AC supply. Special switches are required to support this type of power supply.

In contrast to the office world, the switching functionality is not ensured primarily through use of components that exclusively connect other network nodes. Rather, the line topology makes it necessary to assume that not only "pure" switches are integrated in the line but also automation devices that exhibit a switching functionality consisting of one input port and an output port. This is comparable to the switching functionality of VoIP phones.

In spite of the resulting provision for adapted components close to the machines, it must not be assumed that the statement "Industry = harsh environment" is valid for all industrial areas. Actually, office-like conditions can often be found in manufacturing locations, e.g., at chip manufacturers. For this reason, it is inappropriate to categorically reject office-suitable components in industrial environments caused by the presence of harsh environmental conditions. Instead, the specific conditions should be identified in advance for each installation site. If applicable, simple measures, such as installation in an air-conditioned and sealed cabinet, can be taken to create new environments conditions, thereby obviating the need for expensive special switches, e.g., IP67 class switches with especially high leak-tightness properties.

Full compliance with standardized interfaces according to IEEE 802.3 means that industrial switches can be connected to existing office switches without any problems. However, it may be necessary to use specific plugs according to the installation site and the connector used for the industrial switch. For example, while M12 connectors are used in the automation world, they are unheard of in the office world.











Network elements at the machine level must be adapted to the difficult conditions. Products for PROFINET environments are optimized in this regard and are characterized by a significantly more robust design and simplified installation method. The previously much-described multifunctionality of Industrial Ethernet switches, i.e., their use as a device for forwarding data packets combined with their function as an IO device for control devices, means that standard office switches can hardly ever be used in this environment. However, Industrial Ethernet does not signify that the use of office products in industrial networks has to be ruled out entirely. By all means, they can be used in areas that are not in proximity to machines, taking into consideration the environmental conditions.

Fact 8 – Installation requirements

The specific environmental conditions at the machine level described in Fact 7 result in the use of adapted components both for active and passive elements. The cabling components for the intermediate cabling (see Fact 2) are specified in EN 50173, which applies throughout Europe. However, the main focus here is on the specification of electrical properties for elements in industrial facilities. Due to the requirement for use of "Ethernet-suitable" network elements below the TO in field level, there are explicit specifications regarding properties, which are specified for PROFINET in IEC 61784-5-3. For example, connection of PROFINET devices with Fast Ethernet using copper also requires compliance with Class D. This corresponds fully to the state of the art in the office world. In addition, in order to ensure performance quality of electrical properties, additional component properties are needed, which deviate significantly from the properties of office components in some cases. Examples include:

- Installation cables must be resistant to chemical attacks from oils and the like.
- Connecting cables and plugs are subject to significantly more stringent mechanical requirements in industrial environments (as a result of frequent bending, shocks and vibrations) than in the office environment.
- When assembled outside a cabinet (electrical cabinet or IT cabinet), plugs must be protected to prevent fluids entering into plugs, and electrical or optical properties must be ensured.

In order for the design of passive network elements in machines, i.e., below the TO, to be optimized to the installation, a simple connection method that can be site-assembled is necessary, especially for cabling directly in or on the machine. The PROFINET channel defined in IEC 61784-5-3 comprises the entire transmission path from one active device (switch or field device) to the other. Special PROFINET-compliant cables and plugs allow the simplest possible installation, corresponding to Cat. 5 (two-pair). To achieve optimum interoperability, manufacturers provide a manufacturer's declaration, which can be viewed via the PNO. Typically, a precisely selection must be

	Copper	Fiber optics
IP 20	  	 
IP 67	  	 

made in the case of network elements from the office environment are used in industrial environments. This pre-selection has already been made for PROFINET cabling.

Basically, both copper (twisted pair) and fiber-optic cable are available as transmission media. Compared to copper, a fiber-optic cable has the advantage of a higher transmission range and resistance against electromagnetic interferences. Nevertheless, twisted pair is mostly preferred for interfaces in network devices, even for Industrial Ethernet. Only twisted pair cables allow the use of technologies such as Power over Ethernet or automatic data rate adaptations (autonegotiations). As described previously, the electrical requirements in this case are 100% identical to those of the office world.

The use of fiber-optic cables offers advantages when intermediate distributors are linked to floor distributors. In this case, fewer cables over greater distances can be expected and the length restriction of 100 m for twisted pair would complicate planning considerably. In contrast to the office environment, plastic or HCS (Hard Clad silica) fiber play a role in the automation environment, especially at the machine level. In spite of the limited range compared to glass fiber or even copper technology, POF (polymeric optical fiber) or HCS fiber is characterized by simplified installation methods and, as mentioned previously, EMC insensitivity. These technologies are not included in the product portfolio of components for the office world because IEEE standards do not exist for them. On the other hand, they represent an available option for PROFINET.

A further difference compared to the office world, even for passive elements, is of greater significance: the simplicity of assembling. In the office area a structured, area-wide cabling is performed only once. The cabling is permanently installed in protected cable runs and the exposure to damaging effects after installation will be negligible. These specific conditions are hardly found in automation areas. Cabling is not performed as pre-cabling with a clearly defined permanent link. Rather, cabling is carried out as part of installation of machines and systems. In particular, factory-assembled cords cannot be used for systems. RJ45 plugs and connection technologies that are easy to assemble on-site are often required.

In addition to short-term changes related to production, high mechanical loads of materials can also be expected. Even the use of adapted components can not rule out failure of individual connections. In many cases, these lines are repaired or replaced under extreme time pressure. For this reason, the availability of simple assembly technology is very important for passive and active components.

Despite the standardized electrical requirements for copper and optical requirements for glass fiber, particularly unfavorable environmental conditions can necessitate the use of optimized outlets. The standards for industrial cabling normally offer more robust variants in addition to the conventional technology with plug types used in the office world. Often, these cables are incompatible with office products (e.g., M12) or compatible only with restrictions (e.g., IP67-RJ45). This must be taken into consideration if common office products are used at the machine level.

The specific properties for materials used close to the machines are ensured by various manufacturers in a wide range of products. PROFINET-suitable components satisfy these requirements without any limitations.

Fact 9 – Availability and redundancy

In office networks as well as automation networks, the availability of the network is a critical factor in the acceptance of users. In the automation, an unavailable network almost always results in shutdown of the entire system or a part of the system, which is associated with high failure costs. Availability can be increased by:



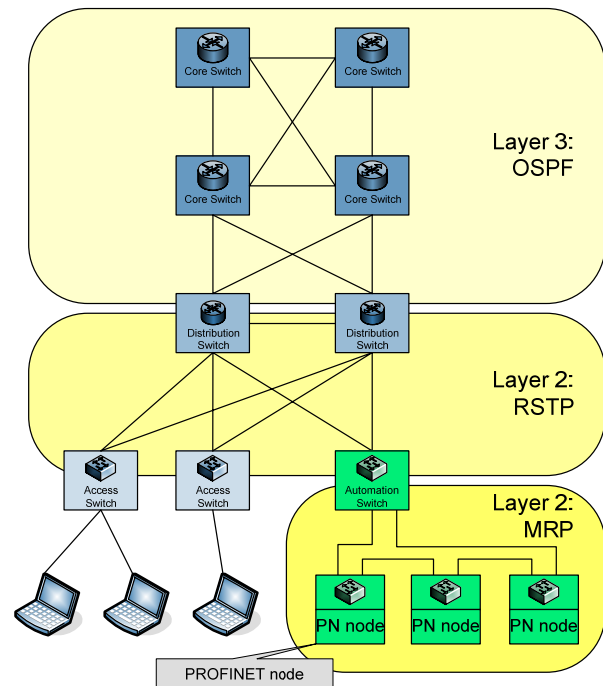
- Use of network elements with higher MTBF (Mean Time Between Failure) values
- Use of network elements that can be repaired or replaced very quickly and easily
- Use of redundancy mechanisms that can bypass the failure of a network element through automatic mechanisms

Standardized redundancy mechanisms with very short failover times have only recently become available for automation. This requires network elements offering very high MTBF – considerably exceeding the MTBF in the office world. In many cases, this completely circumvents the need for redundancy mechanisms.

The importance of optimum ease-of-operation has already been discussed. However, it must be noted again that cabling elements in automation networks can always be repaired more quickly than their office counterparts due to their simpler assembly technology. This also applies to active network elements. PROFINET-compatible devices are designed to allow simple replacement with automatic configuration (configuration stick or network-based).

Redundancy mechanisms are an established means for increasing availability in office and industrial environments. Both cables and active components are provided in a redundant manner and controlled via a redundancy protocol. In the office world, meshed network topologies with OSPF on layer 3 and STP/RSTP on layer 2 have been widely accepted. When an error occurs, the failover times of these protocols are in the range of 1 s to 10 s for OSPF and approximately 3 s for RSTP and, thus, satisfy the requirements of office application but not automation applications with realtime requirements.

For this reason, ring topologies with very fast failover times (less than 500 ms) have been established in automation, in which the used redundancy protocols operate on OSI layer 2. PROFINET makes use of standardized MRP (Media Redundancy Protocol, IEC 62439), which uses mechanisms similar to RSTP, but achieves failover times of less than 200 ms as a result of optimized mechanisms. Yet, even these failover times are insufficient for a redundant network with RT or IRT requirements. For ring topologies, MRRT (Media Redundancy for Real-Time) is used



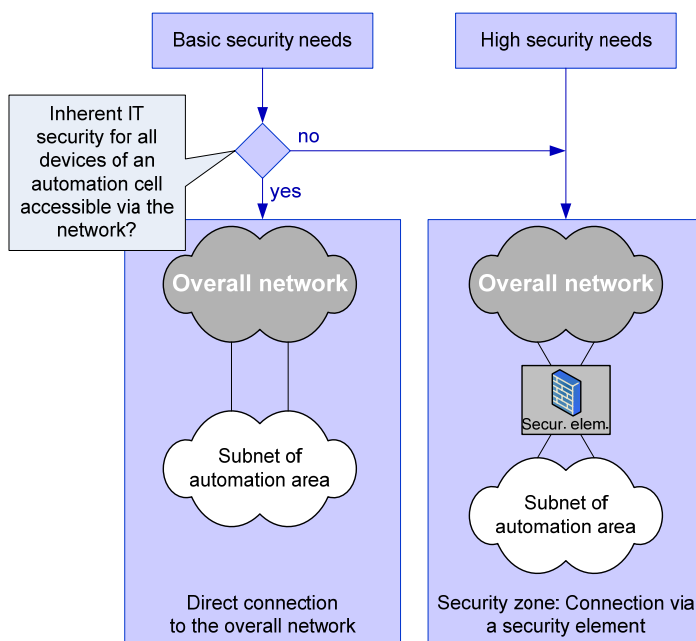
in PROFINET. MRRT is based on transmission of packets in both ring directions and thus ensures interruption-free redundancy.

The integration of Industrial Ethernet switches into an overall network with already implemented redundancy mechanisms also requires the integration into these mechanisms, mostly STP or RSTP. Even without integration into the existing redundancy technology, it is often necessary to ensure compatibility or an unobstructed parallel operation, at a minimum. This functionality should always be checked in advance. Industrial Ethernet switches used with PROFINET support parallel use of RSTP and automation-specific mechanisms such as MRP.

Fact 10 – Security

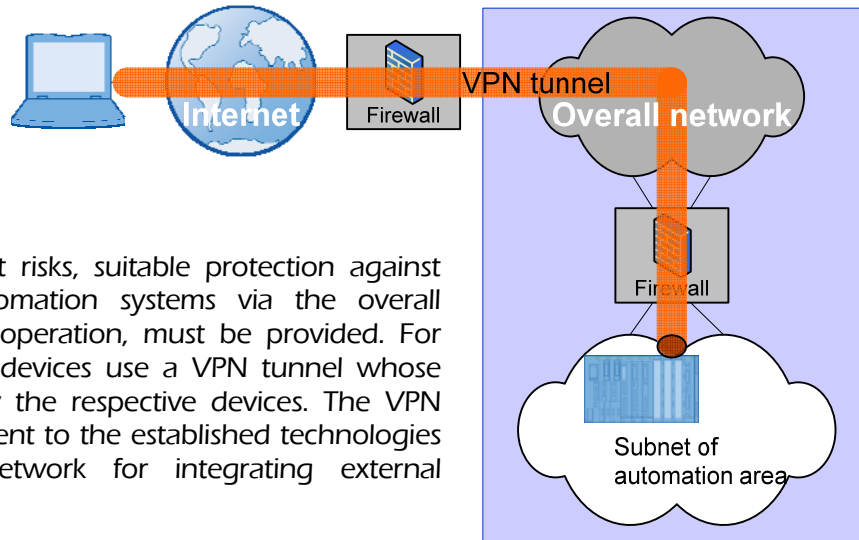
When automation systems are integrated into an overall network, the automation network must be protected against threats from the superordinate IT network, while the overall network must be protected from threats posed by the automation network. The security measures to be taken are identified based on an evaluation of the security needs and risks of the components in the automation area. In this process, adequate protection of the overall network is assumed since these measures represent the de facto standard for basic security needs.

A general risk is posed by programming devices of external vendors that connect directly to the network in the automation area. These types of devices are normally not subject to the security specifications of the overall network and can therefore disseminate malicious software (malware). If components in the automation area are based on universal operating systems (e.g., Windows, Unix), the risks that exist for these operating systems are passed on to the entire component. A security incident can be caused by malicious software or generally as a result of an unauthorized access to the component from the overall network. If current security patches are not available for these devices or are not used due to specific operating system adaptations, a suitable security design must be created for these network areas in order to protect the overall network.



To evaluate the required security measures, the inherent IT security of the components must be determined. A component is inherently IT-secure if it has protection against unauthorized or malicious access appropriate for the basic security needs. This pertains particularly to devices with specific realtime operating systems for which risks have not previously been identified. Such devices, which also frequently contain embedded systems, can normally be classified as inherently IT-secure. For devices based on a universal operation system, the usual basic measures in the IT world, such as system hardening, current virus protection, host-based intrusion prevention system, etc. are mandatory for security purposes.

In the case of increased security needs or the existence of non-inherently IT-secure components that can be accessed via the overall network, a security zone must be created for the relevant automation area. The use of security elements, such as a firewall, allows the entire automation area or parts of the automation area to be separated from the overall network in terms of security.



In addition to these direct risks, suitable protection against external accesses to automation systems via the overall network, e.g., for remote operation, must be provided. For remote access, PROFINET devices use a VPN tunnel whose end points are formed by the respective devices. The VPN technology used is equivalent to the established technologies used on the overall network for integrating external communication partners.

Fact 11 – Operation / management / diagnostics / remote access

An essential condition in all networks is the efficient operation of network elements. While office networks only allow use of access switches as plug-and-play components, PROFINET supports a simple replacement with simplified parameterization for all devices. As a result, the replacement can be carried out by personnel without special training.

PROFINET networks are managed by means of specific PROFINET diagnostic mechanisms that require specific diagnostic information to be exchanged between the controller and field devices within an automation cell. This polling occurs at very short intervals and is supplemented to include optional alarm messages. In addition, like in the office world, it is possible to use Web mechanisms to configure and diagnose PROFINET devices from any computer on the overall network or via the Internet (remote access). If necessary, this can be carried out under the protection of standardized VPN mechanisms.

In the office world, management is based on an integrated, cross-network SNMP management, which monitors both the network components and the system components. The duration of typical polling cycles in office networks is on the order of seconds. PROFINET devices can also be integrated into a centralized SNMP management but the integration is limited to only the communication parameters contained in the standard SNMP MIBs. A detailed representation of PROFINET devices, especially "combo devices", including all automation parameters on an SNMP management server is currently not possible without an unreasonable amount of effort.

If the management solutions for office devices and for PROFINET devices are to be integrated, the following points must be considered during the planning phase:

- Automation system operators will often require that access to automation devices by overall network operators is restricted to read-only access.
- Overall network operators will often require monitoring of network parameters through mechanisms normally found on the overall network.
- To ensure system operation in automation, the polling cycle usually used for the overall network is not sufficient, meaning that an additional management or diagnostic system is required in the automation area without exception.

Summary of specific conditions

Implementation of automation communication infrastructures using PROFINET, which is based on Ethernet and TCP/IP, turns out to be easily achieved from a technical perspective. The structure of automation networks at the machine level can differ significantly from the structure of office networks; this applies for the network structure, the hardware and software requirements, and the protocols used. New solutions not known heretofore in the office world are necessary for automation networks and can be realized appropriately only by using specific "industry-suitable" components and technology. Such solutions are offered by the PROFINET technology.

"Office-like" technology can also be used in industrial environments in areas not directly closed to the machines (field level), while considering the exceptions. Current standards provide planning rules for the design of connection between the standard IT environment and the specific environment of an automation cell.

NETWORK CONNECTION OF AUTOMATION AND OFFICE

By now, connection of the office and automation network areas is an integral part of a network design. Taking advantage of synergy effects in a common network technology is one goal. Besides that, many business processes cannot be divided into separate portions without loss. In many companies, Ethernet and TCP/IP have been used in the office world for many years and efficient operating procedures have thereby been established. Automation areas must be integrated into these structures in many cases.

The manner in which the two areas are connected is particularly important when networks are connected. There are several different alternatives, ranging from complete separation of the physical networks with an individually-specified transition point to a separate connection between each automation cell and the superordinate IT network. The decision-making process must not focus on technical factors only but also on organizational conditions. For example, who has operational responsibility for the automation network will greatly impact the various solution options.

In the descriptions of the most important aspects and scenarios, a essential starting element is the well-accepted network structure of the office world with its 3-level hierarchy as described in Fact 1, consisting of Layer 3 switches in the core and distribution levels and layer 2 switches in the access level. The scenarios presented below represent the main alternatives but should be viewed as examples only.

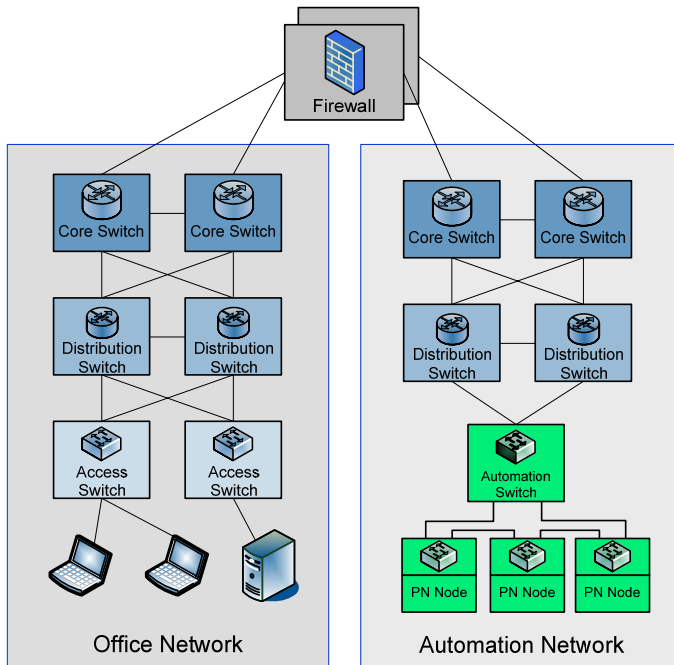
Important planning aspects

Integration of automation areas requires careful planning to avoid restrictions in communication and to prevent security-related incidents. Important aspects for this planning include:

- Identification of nodes to be integrated, required communication flows, and PROFINET communication methods (TCP/UDP, Realtime, Isochronous Realtime)
- Evaluation of the existing IP address structure in office and automation areas as well as planning of required IP services
- Analysis of security needs: firewalls, intrusion prevention systems for preventing denial-of-service attacks, required security measures for devices
- Integration of office terminals and PROFINET devices in one subnet, or separation into separate subnets
- Defining of required accesses for management, diagnostics, remote operation, etc.
- Specification of responsibility for operation of network components and definition of management interfaces, etc.

Scenario 1 – Separate physical and logical networks

The automation area of the network gets its own physical and logical network with separate passive and active infrastructure, in parallel to the rest of the network. Both networks are implemented in accordance with the requirements for PROFINET applications and the office world, respectively. This separate automation network is given a dedicated logical transition point to the office network via a security element, e.g. a firewall.

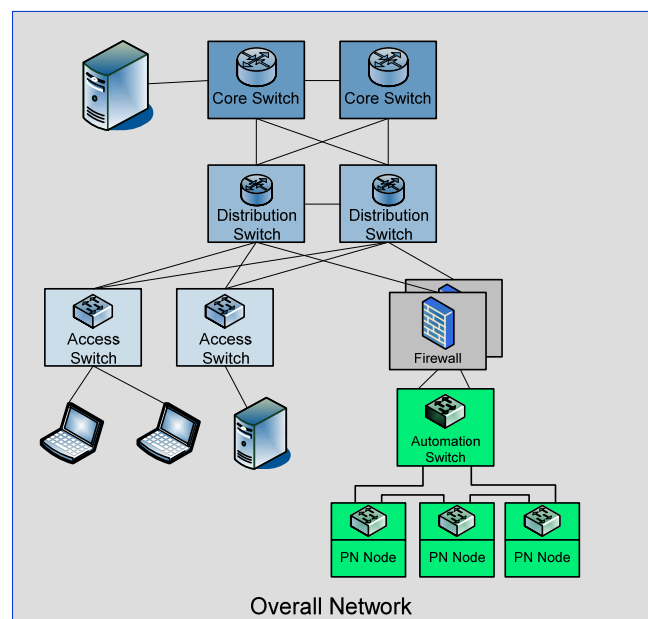


In the case of an application structure in which communication between the overall network and the automation area are heavily intertwined, the centralized firewall instance must be sufficiently dimensioned. In addition to doubling the procurement of network elements, this alternative requires higher investment and operating costs, but in turn provides a clear separation between the networks and, thus, the optimum conditions for protecting the networks, as well as easy-to-govern operating responsibility.

Scenario 2 – Logical integration into the overall network

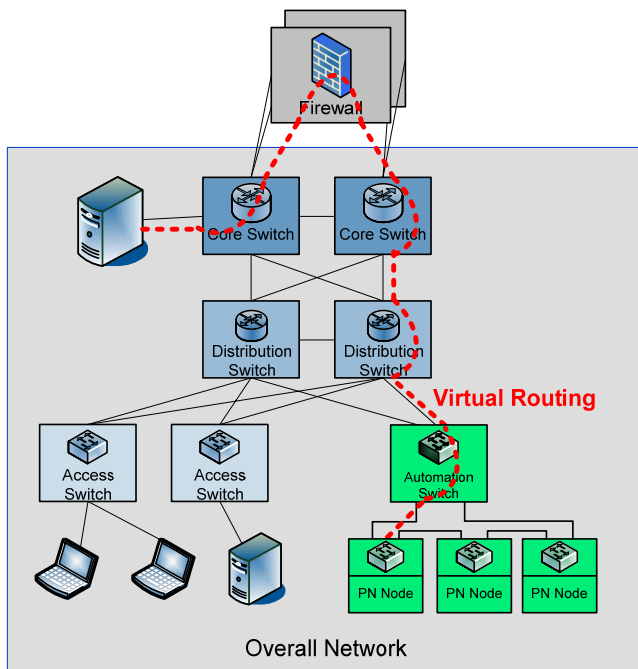
Automation areas are connected in the same way as access switches of the office world to layer 3 switches in the building or hall. Therefore, they use the same superordinate components of the overall network. Depending on its security needs, an automation cell is separated from the rest of the network via a security element, e.g., firewall. Such a firewall can also be used for multiple automation cells.

In addition to simple integration of automation cells into an existing network infrastructure, a connection of this type also offers simple expansion options – if the overall network is equipped accordingly. The investment costs are reduced significantly due to the complete sharing of primary and secondary network elements; on the other hand, higher investment and operating costs can be expected due to the necessity of multiple firewall instances. From the perspective of automation network operators, this solution exhibits a greater dependency on the superordinate IT network than the previous solution. Regulations, e.g., in the form of service level agreements, can be necessary in this case.



If an increased security requirement is not defined for an automation cell of this type, this scenario also allows a complete integration of all nodes, i.e., office devices and automation devices can be connected to a layer 2 switch, taking into consideration the specific conditions presented above.

Scenario 3 – Separate logical networks (closed user group)



A separate logical network is defined within the overall network for the entire automation network, i.e., for all automation cells. The office network and the automation network use a common physical infrastructure for communication and are connected at only a single transition point via a security element, e.g., a firewall.

This alternative provides a clear logical separation of the networks and, thus, optimum protection against risk factors such as unauthorized access or viruses. However, mechanisms providing separation or connection based on software configurations result in very complex network designs accompanied by increased operating costs and effort for analysis/elimination of network errors. This solution also exhibits an elevated dependency on the superordinate network.

Summary of network connection

In today's company structures, connection of the office world and the automation world is indispensable and technically feasible without constraints, provided the described specific conditions are taken into account.

In-depth planning is required in advance, including both technical and non-technical aspects, especially in regard to security-related connection of the two worlds. In particular, the organizational delimitation between the automation area and the overall network is of great importance when choosing the best solution considering aspects like security, management, and availability.

Without question, separate physical and logical networks (scenario 1) simplify the definition of responsibilities and thus avoid responsibility problems. Configuration and operation of two completely independent networks, however, significantly erodes the cost advantage associated with network convergence. Therefore, this solution will not become established over the long-term. The choice between logical integration (scenario 2) or logical separation (scenario 3) depends on the individual circumstances. The lower complexity of scenario 2 argues for its use.

An open and collaborative dialog between representatives of both worlds, requiring explanation and acceptance of all different points of view, will facilitate this integration and will allow the synergy effects of the future convergence to be put to use quickly.

APPENDIX

References

- Pictograms for IE Devices: © Siemens AG 2008, All rights reserved
- EN 50173-1 Information technology - Generic cabling systems –
Part 1: General requirements
- EN 50173-3: Information technology - Generic cabling systems –
Part 3: Industrial premises
- Enhancing the High Performance of PROFINET, PI, 2008
- Industrial Communication with PROFINET, Manfred Popp, PNO, 2007
- PROFIBUS + PROFINET – Strategic Overview, PI, 2008
- PROFINET Security Guideline; PI 2005
- PROFINET Technologie und Anwendung – Systembeschreibung [PROFINET Technology and Application – System Description]; PI, 2006

Abbreviations

CBA	Component Based Automation
DCP	Discovery and Configuration Protocol
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
EMC	Electromagnetic Compatibility
EN	European Standard
HCS	Hard Clad Silica
HMI	Human Machine Interface
IE	Industrial Ethernet
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IO	Input/Output
IP	Internet Protocol
IRT	Isochronous RealTime
MRP	Media Redundancy Protocol, IEC 62439
MRRT	Media Redundancy for Real-Time
NAT	Network Address Translation
OSI	Open System Interconnection
OSPF	Open Shortest Path Forwarding
QoS	Quality of Service
(R)STP	(Rapid) Spanning Tree Protocol
RT	RealTime
RTCP	Realtime Transport Control Protocol
RTP	Realtime Transport Protocol
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over IP (Internet Protocol)

©2008 PROFIBUS and PROFINET International. All rights reserved. The PROFINET Logo is a registered trademark. Members of PROFIBUS and PROFINET International are entitled to use the logo in all their written or electronic publications and promotional material. The use of the PROFINET Logo in connection with PROFINET products is allowed only under the conditions of the PROFINET Runtime Software license. All other trademarks and registered trademarks are the property of their respective owners.

Published by: PROFIBUS Nutzerorganisation e.V., Haid-und-Neu-Str. 7, 76131 Karlsruhe, Germany.