

SIMATIC NET

Industrial Ethernet / PROFINET Industrial Ethernet

System Manual

Preface

Basics of communication
with Industrial Ethernet

1

Network structures and
network configuration

2

Examples of applications

3

SCALANCE network
components

4

Communications processors
for PCs

5

Communications processors
for SIMATIC S7

6

Compact switch module

7

Gateways

8

Appendix

A

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Preface

Target group and motivation

The networking manual accompanies you through all phases of preparation and implementation of network projects. It gives you an overview of the structure and configuration of Industrial Ethernet networks using SIMATIC NET components.

On the one hand, the target groups are decision makers and planners; with this document, they can gain an overview of the technical principles, the SIMATIC NET product range and the most important practical applications.

Structure of the document

The book consists of several parts, structured as follows:

Table 1 Structure of the Networking Manual

Segment	Content and target group
Basics Chapters 1 - 3	In Chapters 1 and 2, the basics of network communication, the special features of Industrial Ethernet and the essential characteristics of SIMATIC NET products are presented. Chapter 3 contains examples of the most common network topologies and use cases and describes the components required for them. The chapter is not only instructive; you can also use it as a practical starting point for planning your own systems.
SIMATIC NET product lines Chapters 4 - 8	These chapters introduce the product lines of SIMATIC NET. You will find information on the SCALANCE series and on the modules for PCs and programmable logic controllers (PLCs).

Orientation in the documentation

Apart from the System Manual you are currently reading, the following documentation is also available from SIMATIC NET on the topic of Industrial Ethernet networks:

- "Industrial Ethernet / PROFINET - Passive network components" system manual

This system manual contains technical information and installation instructions on most network components of SIMATIC NET, for example cables and connectors.

- System manual "RCoax"

This system manual contains both an explanation of the fundamental technical aspects as well as a description of the individual RCoax components and their functionality. Installation/commissioning and connection of RCoax components and their operating principle are explained. The possible applications of the various SIMATIC NET components are described.

- System manual - "Passive Network Components IWLAN"

This system manual explains the entire IWLAN cabling that you require for your IWLAN application. For a flexible combination and installation of the individual IWLAN components both indoors and outdoors, a wide ranging selection of compatible coaxial accessories are available. The system manual also covers connecting cables as well as a variety of plug-in connectors, lightning protectors, a power splitter and an attenuator.

Operating Instructions and other documents

Despite every effort being made to provide a complete and thorough picture, this System manual cannot replace the Operating Instructions and reference documents of the individual devices and components. You will find the detailed documentation of the individual components on the Manual Collection DVD.

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

The DVD ships with certain SIMATIC NET products.

- On the Internet under the following address:

50305045 (<http://support.automation.siemens.com/WW/view/en/50305045>)

Table of contents

	Preface	3
1	Basics of communication with Industrial Ethernet	11
1.1	Terminology	11
1.2	Industrial Ethernet.....	12
1.2.1	Basics of Industrial Ethernet	12
1.2.2	PROFINET	14
1.2.2.1	Basics of PROFINET	14
1.2.2.2	PROFINET IO and PROFINET CBA	16
1.2.3	SIMATIC NET	17
1.2.4	Transmission procedures and real-time response	19
1.3	Technologies of Industrial Ethernet	21
1.3.1	Communications media	21
1.3.2	Basics of communication with IP	22
1.3.2.1	IPv4 address	22
1.3.2.2	Structure of an IPv6 address	24
1.3.2.3	IPv4 / IPv6.....	26
1.3.2.4	IPv6 terms	30
1.3.3	Active and passive network components.....	31
1.3.4	Management functions.....	34
1.3.5	Power over Ethernet	35
1.3.6	Fault tolerance and redundancy	37
1.3.7	Access Methods.....	38
1.3.8	Layer 3 functions.....	39
1.3.9	EtherNet/IP	41
1.4	Switches and switched LANs.....	42
1.5	Wireless LAN	44
1.5.1	What is wireless LAN?	44
1.5.2	Differences between wireless LAN and wired networks.....	44
1.5.3	Preferred areas of application for WLANs	45
1.5.4	The standards of the "IEEE 802.11" series	45
1.5.5	IEEE 802.11n	46
1.5.6	Encryption and data security	50
1.5.7	Avoiding collisions in wireless networks	51
1.5.8	Structure of an IWLAN	52
1.5.9	Network structures	53
1.5.9.1	Infrastructure mode.....	53
1.5.9.2	Ad hoc networks	59
1.5.10	Other wireless technologies.....	59
2	Network structures and network configuration	61
2.1	Network structures	61
2.1.1	Network topologies	61
2.1.2	Linear structure	61

2.1.3	Star structure.....	62
2.1.4	Ring structure.....	65
2.1.5	Redundant linking of network segments with electrical and FO components	67
2.1.6	VLAN.....	69
2.2	Media redundancy	70
2.2.1	Options of media redundancy	70
2.2.2	Media redundancy in ring topologies	70
2.2.3	MRP	72
2.2.4	MRPD.....	73
2.2.5	HRP	74
2.2.6	RNA.....	75
2.2.7	PRP	75
2.2.8	STP / RSTP / MSTP	77
2.2.9	Link aggregation.....	78
2.3	Network security.....	79
2.3.1	SIMATIC NET products for network security	79
2.3.2	Firewalls	82
2.3.3	"Virtual Private Networks" (VPNs)	83
2.3.4	Cell protection concept	84
3	Examples of applications	85
3.1	Optimization of a power screwdriver control.....	85
3.2	Process automation in hazardous areas	87
3.3	Automation of gantry cranes	89
3.4	Controlling material transportation with SCALANCE components	91
3.5	Crane carriage control for a high-bay warehouse.....	93
3.6	Using Power over Ethernet.....	95
3.7	Connecting a PROFIBUS network to a PROFINET installation	97
3.8	Redundant coupled rings with a connection to an office network.....	99
3.9	Data protection during mobile communication.....	101
3.10	Protection of the production network when networking with the office network	103
3.11	Gigabit network in the pharmaceuticals industry	105
3.12	Communications components for extreme climatic conditions.....	107
4	SCALANCE network components	109
4.1	Product families.....	109
4.2	Common properties of all SCALANCE devices	110
4.3	Web Based Management for configuring networks	112
4.4	SCALANCE X switches and media converters.....	114
4.4.1	Type designations and properties.....	114
4.4.2	Functions of SCALANCE X devices	118
4.4.3	SCALANCE X005	120
4.4.3.1	Description	120
4.4.3.2	Functions.....	121

4.4.3.3	Interfaces	121
4.4.4	SCALANCE XB000	122
4.4.4.1	Description	122
4.4.4.2	Characteristics	122
4.4.4.3	Interfaces	122
4.4.5	SCALANCE XC100-4OBR	124
4.4.5.1	Description	124
4.4.5.2	Features and functions	124
4.4.5.3	Interfaces	125
4.4.6	SCALANCE XB-200	126
4.4.6.1	Description	126
4.4.6.2	Features and functions	127
4.4.6.3	Interfaces	128
4.4.7	SCALANCE X200/X200 IRT	129
4.4.7.1	Description	129
4.4.7.2	Features and functions	131
4.4.7.3	Interfaces	132
4.4.8	SCALANCE X300	135
4.4.8.1	Description	135
4.4.8.2	Features and functions	136
4.4.8.3	Interfaces	138
4.4.8.4	Media modules and SFP transceivers	141
4.4.9	SCALANCE XM-400	143
4.4.9.1	Description	143
4.4.9.2	Features and functions	144
4.4.9.3	Interfaces	145
4.4.9.4	Extender modules	146
4.4.9.5	SCALANCE PS-900	148
4.4.10	SCALANCE X500	149
4.4.10.1	Description	149
4.4.10.2	Features and functions	150
4.4.10.3	Interfaces	151
4.5	SCALANCE W components for Industrial Wireless LAN	156
4.5.1	SCALANCE W devices	156
4.5.2	Type designations	159
4.5.3	Functions of WLAN devices	159
4.5.4	SCALANCE W760/W720	161
4.5.4.1	Description	161
4.5.4.2	Features and functions	161
4.5.4.3	Interfaces	163
4.5.5	SCALANCE W770/W730	163
4.5.5.1	Description	163
4.5.5.2	Features and functions	164
4.5.5.3	Interfaces	165
4.5.6	SCALANCE W788/W748	166
4.5.6.1	Description	166
4.5.6.2	Features and functions	167
4.5.6.3	Interfaces	168
4.5.7	SCALANCE W786	169
4.5.7.1	Description	169
4.5.7.2	Features and functions	170
4.5.7.3	Interfaces	171

4.5.8	SCALANCE WLC711, W788C and W786C	172
4.5.8.1	Description	172
4.5.8.2	Features and functions	173
4.5.8.3	Interfaces	175
4.5.9	Antennas	176
4.5.9.1	How it works	176
4.5.9.2	Product overview	178
4.6	SCALANCE M routers and modems	185
4.6.1	SCALANCE M devices	185
4.6.2	SCALANCE M812-1, M816-1 and M826-2	188
4.6.2.1	Description	188
4.6.2.2	Features and functions	189
4.6.3	SCALANCE M874-3 and M-876-4	191
4.6.3.1	Description	191
4.6.3.2	Features and functions	192
4.6.4	SCALANCE M875	194
4.6.4.1	Description	194
4.6.4.2	Features and functions	195
4.6.5	Teleservice adapter IE	197
4.6.5.1	Description	197
4.6.5.2	Features and functions	198
4.6.6	Modem MD720	199
4.6.6.1	Description	199
4.6.6.2	Features and functions	200
4.6.7	SINEMA Remote Connect	202
4.6.8	Antennas for mobile wireless	202
4.6.8.1	Product overview	202
4.7	SCALANCE S security module	206
4.7.1	Introduction	206
4.7.2	Technical basics	207
4.7.3	Description	210
4.7.4	Features and functions	213
4.7.5	Interfaces	214
4.7.6	SOFTNET Security Client	215
4.8	Network management software	218
4.8.1	SINEMA server	218
4.8.2	Primary Setup Tool	219
4.9	Accessories	222
4.9.1	C-PLUG Configuration Memory	222
4.9.2	KEY-PLUG	223
5	Communications processors for PCs	225
5.1	CP 1604	227
5.2	CP 1616	229
5.3	CP 1612 A2	231
5.4	CP 1613 A2	233
5.5	CP 1623	235
5.6	CP 1628	237

6	Communications processors for SIMATIC S7	239
6.1	Communications processors for SIMATIC S7-200	242
6.2	Communications processors for SIMATIC S7-300	244
6.3	Communications processors SINAUT ST7 for SIMATIC S7-300	251
6.4	Communications processors for SIMATIC S7-400	253
6.5	Communications processors for SIMATIC S7-1200	260
6.6	Communications processors for SIMATIC S7-1500	263
7	Compact switch module	267
7.1	CSM 377	269
7.2	CSM 1277	271
7.3	LOGO! CSM	274
8	Gateways	277
8.1	IE/PB Link PN IO	280
8.2	IE/AS-i Link PN IO	281
8.3	IE/WSN-PA Link	282
A	Appendix	285
A.1	Overview of the standards relevant for network installation	285
A.2	Content of the standards	287
A.3	Application of the standards	288
	Index	291

Basics of communication with Industrial Ethernet

1.1 Terminology

Industrial Ethernet

The term "Industrial Ethernet" covers a series of expansions to the Ethernet standard IEEE 802.3 with which communication suitable for an industrial environment is implemented. The main aims are as follows:

- Deterministic data transmission - guaranteed response times and data rates
- Safeguarding against component failure
- Network topologies adapted to a particular plant with the emphasis on linear (bus), redundant network structures.

The components must meet the following requirements:

- Equipment designed for industry, for example signaling contacts, protected cables and connectors
- Capability of withstanding extreme environmental conditions, for example extreme temperatures, vibration, dust, dampness, electromagnetic interference.

PROFINET

PROFINET is the name of the standard for Industrial Ethernet (IEC 61158/61784) developed and maintained by the PROFIBUS user organization.

PROFINET unites protocols and specifications with which Industrial Ethernet meets the requirements of industrial automation technology.

These include, for example:

- Real-time conditions
- Environment strongly affected by EMI
- Demanding requirements for safety, reliability and availability.

This world is in stark contrast to an office environment where high data throughput and large-area networking are the main objectives. Further differences between the two network types can be found in the numbers and heterogeneity of the nodes and their intermeshing.

SIMATIC NET

SIMATIC NET stands for a wide range of **network components** grouped under the motto "Totally Integrated Automation" to reflect the modern fully integrated implementation of automation solutions. PROFINET is the protocol used by SIMATIC NET components within the framework of Industrial Ethernet.

1.2 Industrial Ethernet

1.2.1 Basics of Industrial Ethernet

Properties of Industrial Ethernet

Industrial Ethernet is a powerful communication medium complying with the international standard IEEE 802.3 (Ethernet) and was designed for the requirements in an industrial environment.

Ethernet was developed for the office environment and is subject to certain restrictions due to its origins. Industrial Ethernet therefore offers significant expansions of the Ethernet technology for the industrial environment:

- Protection of investment by connecting existing fieldbus systems
- Network components for use in a tough industrial environment
- Rugged and simple connection on-site
 - FastConnect cabling system with RJ-45 and M12 technology
 - Assembly of POF, PCF and MM fiber-optic cable
- High transmission performance even with large numbers of nodes thanks to the end-to-end availability of components with 100 Mbps transmission rates complying with Fast Ethernet and 1000 Mbps with Gigabit Ethernet.
- Ethernet with real-time capability that meets high requirements for the reaction time.
- Integrated security concepts for protection against unauthorized access
- High availability of the networks thanks to redundant functionality, for example ring redundancy and redundant power supply
- Permanent monitoring of the network components with simple and effective signaling concept
- Almost unlimited communication performance with scalable performance available when necessary with switching technology.
- Networking of different areas of application such as office and production
- "Rapid Roaming" in Industrial Wireless LAN (IWLAN) for extremely fast handover of mobile nodes between different access points and therefore fast cyclic data communication (iPCF and iPCF-MC).
- Communication throughout the enterprise with the options of linking over WAN (Wide Area Network, for example DSL or mobile wireless).
- Precise time stamping of events in the entire system with plant-wide timekeeping

Fast Ethernet

The Fast Ethernet standard IEEE 802.3u is an expansion of the existing standard (IEEE 802.3). Fast Ethernet is based essentially on the classic Ethernet standard for twisted pair cable.

Ethernet and Fast Ethernet have the following common features:

- the CSMA access method
- the glass fiber-optic cable used and category 5 twisted pair cables

Fast Ethernet includes the following expansions / modifications:

- Data transmission rate up to 100 Mbps
- Autosensing, automatic detection of the transmission rate
- Autonegotiation, automatic detection of the functionality of the interface of the partner
- Full duplex mode
- Auto polarity exchange, automatic adaptation of the polarity if the wires of a cable pair are swapped over.
- MDI/MDIX autocrossover, prevents malfunctions if transmit and receive cables are crossed over.

Gigabit Ethernet

Gigabit Ethernet is an expansion of the Ethernet specifications to increase the data transmission rate to 1000 Mbps, 1Gbps or 10 Gbps.

The relevant standards are as follows:

- IEEE 802.3z for transfer via glass fiber
- IEEE 802.3ab for electrical cable.

The increase in the transmission speed is achieved not only by adaptation of the protocol but also by using category "5e" or "6" twisted pair cables that are particularly immune to interference.

Differences compared with PROFINET

PROFINET expands Industrial Ethernet with the following additional properties:

- Transmission mode and real-time response:
It can be guaranteed that frames are transferred within a specified time.
- Deterministic; put simply:
The same conditions always lead to the same results and there are no undefined statuses.

See also

Transmission procedures and real-time response (Page 19)

Fault tolerance and redundancy (Page 37)

Access Methods (Page 38)

1.2.2 PROFINET

1.2.2.1 Basics of PROFINET

What is PROFINET?

PROFINET is the innovative and open Industrial Ethernet standard (IEC 61918, for PROFINET also IEC 61158/61784) for industrial automation.

PROFINET uses the existing IT standards and allows end-to-end communication from the field level to the management level as well as plant-wide engineering.

Aims of PROFINET

The aims of PROFINET are as follows:

- Open Ethernet standard for automation based on Industrial Ethernet. Industrial Ethernet and standard Ethernet components can be used together, however Industrial Ethernet devices are more rugged and therefore better suited to an industrial environment (temperature, noise immunity etc.).
- Use of TCP/IP and IT standards
- Automation of applications with real-time requirements
- Seamless integration of fieldbus systems

PROFINET communication

PROFINET communication is divided into non real time (NRT), real time (RT) and isochronous real time (IRT) communication, see section "Transmission procedures and real-time response (Page 19)".

PROFINET profiles

PROFINET transfers data transparently. The interpretation of the data is the responsibility of the user. The profiles are stipulations agreed by manufacturers and users relating to certain properties, performance characteristics and behavior of devices and systems.

- PROFIdrive

The PROFIdrive profile (IEC 61800-7) defines the device behavior and the method of accessing internal device data for electric drives on PROFIBUS and PROFINET.

The profile describes in detail how the communications functions direct data exchange, constant bus cycle time and isochronous real time should be used in drive applications. It also specifies all the device properties that influence the interface to a controller connected via PROFIBUS or PROFINET. These include the state machine (sequence control), the encoder interface, the standardization of values, the definition of standard frames, access to drive parameters etc.

The PROFIdrive profile supports both central and distributed motion control concepts.

- PROFIsafe

The PROFIsafe profile (IEC 61508 / EN 954-1) defines how the safety-related devices achieve fail-safe communication so that they can be used for safety-related applications.

The profile is a software solution that is implemented as an additional layer (PROFIsafe layer) in the devices (e.g. operating system of the CPU). The safety-relevant data is included in the frame in addition to the standard data and forms the PROFIsafe frame. Existing solutions can be expanded without needing to change cabling.

PROFIsafe prevents errors such as address corruption, loss, delay etc when transferring messages by consecutively numbering the PROFIsafe data, time monitoring, authenticity monitoring using passwords and optimized CRC protection.

- PROFInergy

With the PROFInergy profile, individual consumers or entire production units can be turned off and on. This is coordinated centrally by a higher-level controller; networking is via PROFINET. During long pauses, this allows as much energy as possible to be saved. Plant sections that are turned off for a short time contribute to the uniform distribution of energy and optimum use of energy.

It is also possible to read out measurement variables relating to consumption.

PROFInergy is defined so that the necessary function blocks can be included easily in existing automation solutions.

Implementation of PROFINET in SIMATIC

PROFINET is implemented in the SIMATIC products as follows:

- Communication between field devices is implemented in SIMATIC with **PROFINET IO**.
- Communication between the controllers as components in distributed systems is implemented in SIMATIC by **PROFINET CBA** (Component-Based Automation).

- Installation technology and network components are available under the **SIMATIC NET** brand name.
- For remote maintenance and network diagnostics, the tried and tested IT standards from the office world are used (e.g. SNMP = Simple Network Management Protocol for network parameter assignment and diagnostics).

Documentation of PROFINET on the Internet

Numerous publications on the topic of PROFINET can be found at the Internet address (<http://www.profibus.com>) of PROFIBUS International.

You will find further information on the Internet (<http://www.siemens.com/profinet>).

1.2.2.2 PROFINET IO and PROFINET CBA

What is PROFINET IO?

Within the framework of PROFINET, PROFINET IO is a communications concept for the implementation of modular, distributed applications.

With PROFINET IO, you create automation solutions in the same way as familiar from PROFIBUS DP.

Implementation of PROFINET IO is implemented by the PROFINET standard for programmable controllers (IEC 61158-x-10).

The STEP 7 engineering tool supports you when setting up and configuring an automation solution.

In STEP 7, you therefore have the same application view regardless of whether you are configuring PROFINET devices or PROFIBUS devices. The user program looks the same for PROFINET IO and PROFIBUS DP. The same function blocks and system status lists are used (were expanded for PN IO).

What is PROFINET CBA?

Within the framework of PROFINET, PROFINET CBA (Component-Based Automation) is an automation concept concentrating on the following aspects:

- Implementation of modular applications
- Machine-machine communication

With PROFINET CBA, you create a distributed automation solution based on off-the-shelf components and partial solutions. This concept meets the requirements for greater modularization in mechanical engineering and plant engineering with extensive distribution of intelligent processing.

With Component-Based Automation, you implement complete technological modules as standardized components that can be used in large plants.

You create the modular, intelligent components in PROFINET CBA in an engineering tool that may differ from device manufacturer to device manufacturer. Components made up of SIMATIC devices are created with STEP 7 and interconnect these with the SIMATIC iMAP tool.

Interaction between PROFINET IO and PROFINET CBA

PROFINET IO systems can be included in machine-machine communication with the aid of PROFINET CBA. From a PROFINET IO system, a PROFINET component is created, for example in STEP 7. With SIMATIC iMAP you can configure plants made up of several such components. The communications connections between the devices are simply configured graphically as interconnection lines.

The following figure shows a distributed automation solution with several components that communicate via PROFINET. The right-hand component contains IO devices and an IO controller on PROFINET IO.

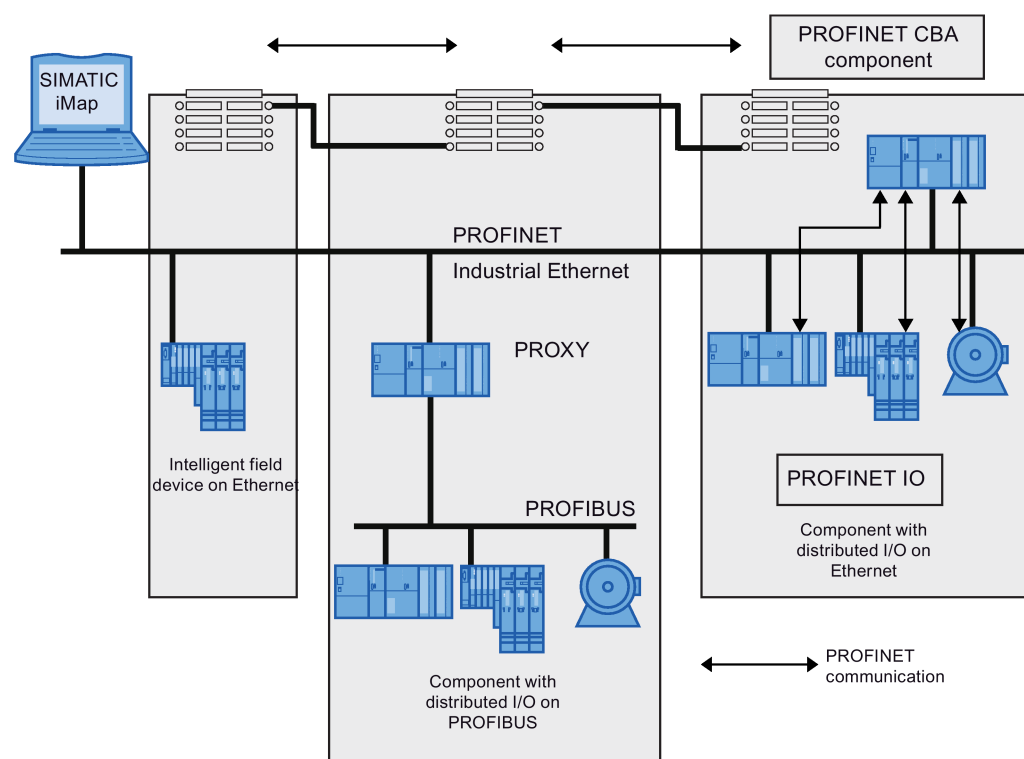


Figure 1-1 PROFINET CBA - modular concept

1.2.3 SIMATIC NET

SIMATIC NET in the automation world

SIMATIC NET is the product name for networks and network components. The network solutions of SIMATIC NET are an integral component of Totally Integrated Automation (TIA). With TIA, Siemens is the only manufacturer to provide a totally integrated basis for implementing customer-specific automation solutions.

The data can be exchanged between all levels - from the field level to the production management level right through to the enterprise management level.

The SIMATIC NET network components have uniform system interfaces and are coordinated with each other. In addition to the previous wired solutions, wireless

communication is gaining ground in industry. SIMATIC NET provides products for enterprise-wide transmission of data over local area networks, intranet, Internet or wireless networks.

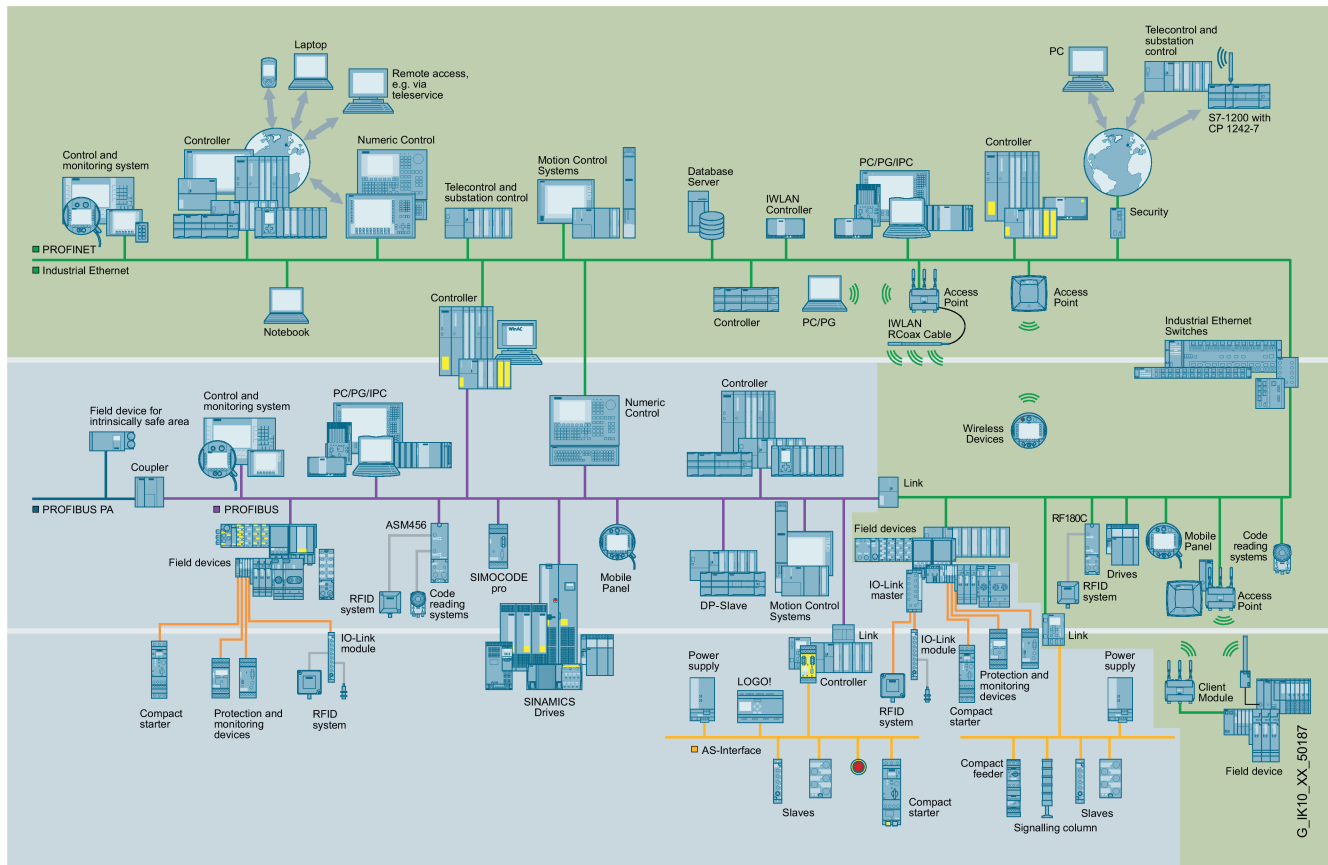


Figure 1-2 Industrial Ethernet and PROFINET in the SIMATIC NET environment

The distinguishing properties of SIMATIC NET include the following:

- Complete integration from the field level to the enterprise level,
- Coverage of the field area with Industrial Ethernet,
- Promotion of mobile communication,
- Integration of the IT technologies.

With these communication network options, SIMATIC products and intelligent devices can be combined locally according to your requirements. Flexibility and openness of the standards of SIMATIC communications networks make it possible to link different systems and to implement extensions.

Thanks to its scalable performance, SIMATIC NET allows the implementation of enterprise-wide communication – from the simplest device to the complex system. The SIMATIC NET components used with Industrial Ethernet are particularly powerful. The devices of the SCALANCE product family represent the latest and most advanced generation of active SIMATIC NET network components.

Technical requirements

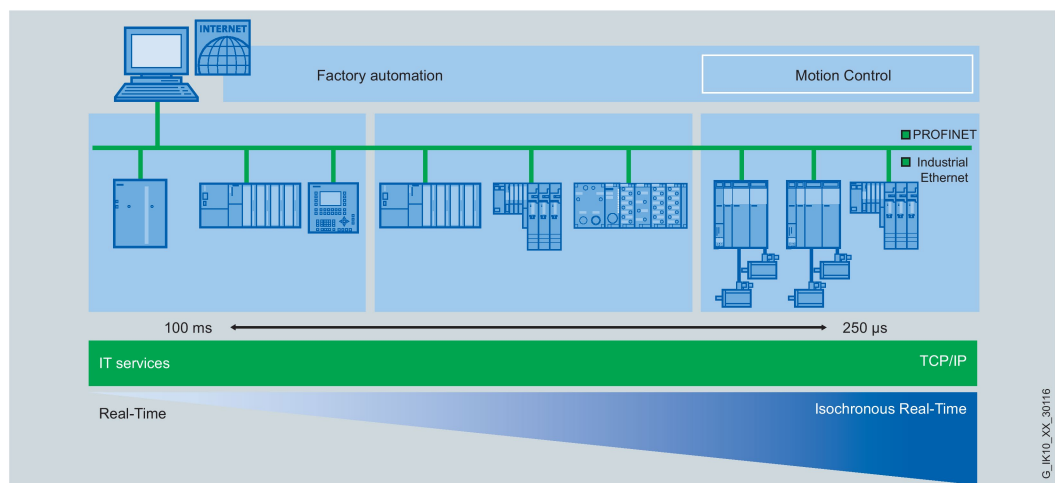
Communications networks are a central component of modern automation solutions. Industrial networks have to fulfill special requirements, for example:

- Linking of automation systems, PCs as well as simple sensors, actuators and computers
- Robust against electromagnetic interference, mechanical stress and pollution
- Integration of existing systems and expandability
- IT communication to integrate modern information technology
- Simple cabling technology
- Flexible adaptation to the production requirements
- Availability of information at any location
- Correct transfer of information and at the right time
- Integrated diagnostics
- Deterministic - no undefined statuses
- Fast data exchange between parts of the plant
- Integrated security functions preventing unauthorized access
- Safe standard communication over the same connection

Industrial networks belong to the LANs (Local Area Networks) and allow communication within a limited area.

1.2.4 Transmission procedures and real-time response

Overview



Non real-time communication (NRT communication)

NRT communication is non-time -critical communication and corresponds to the communication of Industrial Ethernet with the protocol family TCP/IP. Everything that is transferred using Industrial Ethernet can also be transferred via PROFINET, for example HTTP, TCP, UDP, SNMP, ARP.

Real-time communication (RT communication)

Real time means that a system processes external events within a specific time. If the reaction is predictable, this is known as a deterministic system.

A high data rate alone is no guarantee for real-time response, since delays are possible at "bottlenecks" in the network. Instead, the network protocol must ensure that time critical frames are given preferential treatment.

RT communication is suitable for transfer of alarms and cyclic data. Special switches must be used here. All SIMATIC NET switches are suitable for this. There is, however, not yet any need for particular communication planning in the form of a special configuration.

In RT communication the cyclic data are transferred between the IO controller and IO device, however, without the "best possible synchronicity".

Unsynchronized IO devices automatically exchange data using RT communication.

Isochronous real-time communication (IRT communication)

In PROFINET with IRT, communication over Ethernet is divided into individual cycles. Each cycle consists of two phases, an IRT channel reserved for extremely time-critical data, and an "open channel", within which RT and non-time critical frames can be sent.

This allows time-critical and uncritical data to be sent on the same connection. At the same time, however, a certain data rate (and therefore a transmission time) is reserved for the critical data and real-time capability can therefore be guaranteed.

Properties of isochronous real time

With the implementation of the data transfer procedure IRT in Ethernet controllers, the ERTEC ASICs (Enhanced Real-Time Ethernet Controller), update times of 250 µs and a jitter accuracy of the transmit clock of less than 1 µs can be achieved.

In PROFINET V2.3, the methods fast forwarding, dynamic frame packing and fragmentation were implemented. With these methods, update times of up to 31.25 µs can be reached.

IRT is used in areas with particularly stringent requirements for response times that cannot be exceeded. This is the case, for example, for motion control applications, which require reaction and update times in the range of a few milliseconds. Special switches must be used here. In SIMATIC NET, the suitable switches have "IRT" in their names.

1.3 Technologies of Industrial Ethernet

1.3.1 Communications media

Selection of media

Industrial Ethernet provides you with three different technologies to solve your automation task:

- Electrical cabling
- Fiber-optic cables
- Wireless/radio

Guide to selection

The following table shows with of the three communications media is best suited to which requirements:

	Twisted pair network	Fiber-optic network	Wireless linking
Suitability for high transmission rates	•	* 1)	*
Inter-building networking	--	•	*
EMC	*	•	•
Simple cable installation	•	*	
Range of cables for special use cases	• Cables for indoors and outdoors according to the cable characteristics • Trailing cable • Cable free of halogens • Marine cable • FastConnect cables	• Cables for indoors and outdoors • Trailing cable • Cable free of halogens	--
The effect of failure of a network section	With a ring, no effect; with simple structures the network breaks down into two isolated subnetworks	With a ring, no effect; with simple structures the network breaks down into two isolated subnetworks	If there are overlapping wireless cells, the client roams to another AP

	Twisted pair network	Fiber-optic network	Wireless linking
Maximum distance between two network nodes / access points	100 m	FE (100 Mbps) • 50 m POF • 100 m PCF • 5000 m multimode • Up to 200 km single mode GE (1000 Mbps) • 750 m multimode • 120 km single mode 10 GE (10000 Mbps) • 750 m multimode • 40 km single mode	Up to several kilometers depending on the environmental conditions, testing with www.siemens.de/snst
Preassembled cables	yes	yes	--
Redundant network structures	electrical ring or duplication of the infrastructure (bus, star, tree)	electrical ring or duplication of the infrastructure (bus, star, tree)	--

• Suitable

* Suitable to some extent

-- Unsuitable / not relevant

1) Longer distances possible

1.3.2 Basics of communication with IP

1.3.2.1 IPv4 address

Range of values for IP address

The IP address consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 141.80.0.16

Range of values for subnet mask

The subnet mask consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 255.255.0.0

The binary representation of the 4 subnet mask decimal numbers must contain a series of consecutive 1s from the left and a series of consecutive 0s from the right.

The 1s specify the network number within the IP address. The 0s specify the host address within the IP address.

Example:

Correct values:

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000 0000 B

Incorrect value:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

Relationship between the IP address and subnet mask

The first decimal number of the IP address (from the left) determines the structure of the subnet mask with regard to the number of "1" values (binary) as follows (where "x" is the host address):

First decimal number of the IP address	Subnet mask
0 to 127	255.x.x.x
128 to 191	255.255.x.x
192 to 223	255.255.255.x

Classless Inter-Domain Routing (CIDR)

CIDR is a method that groups several IP addresses into an address range by representing an IP address combined with its subnet mask. To do this, a suffix is appended to the IP address that specifies the number of bits of the network mask set to 1. Using the CIDR notation, routing tables can be reduced in size and the available address ranges put to better use.

Example:

IP address 192.168.0.0 with subnet mask 255.255.255.0

The network part of the address covers 3 x 8 bits in binary representation; in other words 24 bits.

This results in the CIDR notation 192.168.0.0/24.

The host part covers 1 x 8 bits in binary notation. This results in an address range of 2 to the power 8, in other words 256 possible addresses.

Value range for gateway address

The address consists of four decimal numbers taken from the range 0 to 255, each number being separated by a period; example: 141.80.0.1

Range of values for IP address and gateway address

The only parts of the IP address and network transition address that may differ are those in which "0" appears in the subnet mask.

Example:

You have entered the following: 255.255.255.0 for the subnet mask; 141.30.0.5 for the IP address and 141.30.128.0 for the gateway address. Only the fourth decimal number of the IP address and gateway address may be different. In the example, however, the 3rd position is different.

You must, therefore, change one of the following in the example:

The subnet mask to: 255.255.0.0 or

the IP address to 141.30.128.5 or

the gateway address to: 141.30.0.0

1.3.2.2 Structure of an IPv6 address

IPv6 address format - notation

IPv6 addresses consist of 8 fields each with four-character hexadecimal numbers (128 bits in total). The fields are separated by a colon.

Example:

fd00:0000:0000:ffff:02d1:7d01:0000:8f21

Rules / simplifications:

- If one or more fields have the value 0, a shortened notation is possible.

The address fd00:**0000:0000**:ffff:02d1:7d01:0000:8f21 can also be shortened and written as follows:

fd00::**ffff**:02d1:7d01:0000:8f21

To ensure uniqueness, this shortened form can only be used once within the entire address.

- Leading zeros within a field can be omitted.

The address fd00:0000:0000:ffff:**02d1**:7d01:0000:8f21 can also be shortened and written as follows:

fd00::**ffff:2d1**:7d01:0000:8f21

- Decimal notation with periods

The last 2 fields or 4 bytes can be written in the normal decimal notation with periods.

Example: The IPv6 address fd00::ffff.125.1.0.1 is equivalent to fd00::ffff:7d01:1

Structure of the IPv6 address

The IPv6 protocol distinguishes three types of address: Unicast, anycast and multicast. The following section describes the structure of the global unicast addresses.

IPv6 prefix		Suffix
Global prefix: n bits	Subnet ID m bits	Interface ID 128 - n - m bits
Assigned address range	Description of the location, also subnet prefix or subnet	Unique assignment of the host in the network. The ID is generated from the MAC address.

The prefix for the link local address is always fe80:0000:0000:0000. The prefix is shortened and noted as follows: fe80::

IPv6 prefix

Specified in: RFC 4291

The IPv6 prefix represents the subnet identifier.

Prefixes and IPv6 addresses are specified in the same way as with the CIDR notation (Classless Inter-Domain Routing) for IPv4.

Design

IPv6 address / prefix length

Example

IPv6 address: 2001:0db8:1234::1111/48

Prefix: 2001:0db8:1234::/48

Interface ID: ::1111

Entry and appearance

The entry of IPv6 addresses is possible in the notations described above. IPv6 addresses are always shown in the hexadecimal notation.

1.3.2.3 IPv4 / IPv6

What are the essential differences?

	IPv4	IPv6
IP configuration	• DHCP server • Manual	• Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) – It creates a link local address for every interface that does not require a router on the link. – It checks the uniqueness of the address on the link that requires no router on the link. – It specifies whether the global addresses are obtained via a status-free mechanism, a mechanism with status or via both mechanisms. (Requires a router on the link.) • Manual • DHCPv6
Detecting duplicate IP addresses		<i>Duplicate address detection</i> Procedure to ensure that within the framework of the stateless automatic address configuration an IP address is only assigned to one interface. What happens if the address is duplicated? An LLA must then be assigned manually.
Available IP addresses	32-bit: $4, 29 \cdot 10^9$ addresses (32-bit)	128-bit: $3, 4 \cdot 10^{38}$ addresses
Address format	Decimal: 192.168.1.1 with port: 192.168.1.1:20	Hexadecimal: 2a00:ad80::0123 with port: [2a00:ad80::0123]:20
Loopback (local computer)	127.0.0.1	::1

	IPv4	IPv6
IP addresses per interface	One IP address	Multiple IP addresses • LLA: Link Local Address (formed automatically) fe80::/64 Unique in the link, can however occur more than once globally. With IPv6 is generated automatically for every interface, serves for setting up the network by IPv6. A ping to an LLA address requires specification of the ping "interface" with %interfacenumber at the end of the destination address. Here,, the host obtains information about other IPv6 hosts and routers • ULA: Unique Local Address - intended for NAT that adopt the private addresses and may be routed but not but not globally unique. According to RFC 4193 routers and firewalls should not pass these into the global Internet • GA: Global Unicast Address that are globally unique and can be routed, currently every address from the range 2000::/3 with the exception of the ranges reserved for special purposes.
Header	• Checksum • Variable length • Fragmentation in the header • No security	• Checking at a higher layer • Fixed preset size • Fragmentation in the extension header • IPsec via extension header
Security	For encryption in IPv4 which is required for example with VPN, is always the responsibility of the higher layers	With IPsec, IPv6 brings a direct integration via the extension header
Fragmentation	Host and router	Only endpoint of the communication
Checksum in the header	yes	no
Options in the header	yes	no

	IPv4	IPv6
ICMP	ICMP	ICMPv6 Router Solicitation (ICMPv6 type 133) Sent by a client to localize servers. Router Advertisement Messages (ICMPv6 type 134) Sent by a server as response to a Solicit message to indicate availability. Neighbor Solicitation Messages (ICMPv6 type 135) Node send Neighbor Solicitation messages to obtain the data link layer address of a neighbor node. Neighbor Solicitation messages are used to establish whether a neighbor node is still reachable via a buffered data link layer address. Neighbor Solicitation messages are also used to recognize duplicate addresses. Neighbor Advertisement Messages (ICMPv6 type 136) A node sends Neighbor Advertisement messages as a reaction to a Neighbor Solicitation message. The node can also send unsolicited Neighbor Advertisement messages, to make a change in the data link layer address known. Redirect Messages (ICMPv6 type 137) Use Redirect messages to inform hosts of a better first hop to a destination or to inform them that the destination is located on the same link.
Ports	UDP RIP: UDP 520	DHCP, ports client 546 & server 547 RIPng: 521
Router discovery	optional	mandatory When router discovery is used in addition, the node is informed of the following • further IPv6 addresses • router addresses • further configuration parameters e.g. via DHCP
Quality of Service	Type of Service (ToS) for prioritization	The prioritization is specified in the header field "Traffic Class".
Types of frame	Broadcast, multicast, unicast, anycast	Multicast, unicast, anycast
Identification of DHCPv6 clients/server	Client ID: MAC address	DUID + IAID(s) = exactly one interface of the host DUID = DHCP unique identifier identifies server and clients uniquely and should not change, no change when replacing network components! IAID = Identity Association Identifier at least one per interface is generated by the client and remains unchanged when the DHCP client restarts Three methods of obtaining the DUID • DUID-LLT • DUID-EN • DUID-LL

	IPv4	IPv6
DHCP	via UDP with broadcast	via UDP with unicast Clients normally send their queries to the so-called "all DHCP relay agents and servers" multicast address (FF02::1:2). This is a link-local multicast address and the all servers and relay agents long to the corresponding group. These in turn listen on port 547. Local servers and relay agents reach a client using a link-local unicast address that was generated with the help of stateless autoconfiguration. Clients listen on port 546
Link layer address resolution	ARP ARP request (broadcast)	NDP Neighbor Solicitation packet (multicast, ICMPv6 type 135) to solicited node addresses
Neighbor nodes		IPv6 Neighbor Discovery protocol Router detection – Supports hosts when localizing routers on the local link. Automatic address configuration - allows a node to configure the IPv6 addresses for its own interfaces automatically. Prefix detection – Allows nodes to recognize known subnet prefixes assigned to a link. Nodes use prefixes to distinguish between destinations on the local link from destinations that can only be reached via a router. Address resolution – Helps nodes when determining the link local address of a neighboring node assuming only the IP address of the destination exists. Determination of the next hop - uses an algorithm to determine the IP address of a packet recipient located one hop over the local link. The next hop can be a router or destination node. Neighbor unreachability detection - helps nodes to determine whether a neighbor node is still reachable. With routers and hosts the address resolution can be repeated. Detection of duplicate addresses – Allows a node to determine whether an address wanted by a node is already being used by another node. Diversion - allows a router to inform a host about a node in the first hop via which a certain destination can be reached better.

1.3.2.4 IPv6 terms

Network node

A network node is a device that is connected to one or more networks via one or more interfaces.

Router

A network node that forwards IPv6 packets.

Host

A network node that represents an end point for IPv6 communication relations.

Link

A link is, according to IPv6 terminology, a direct layer 3 connection within an IPv6 network.

Neighbor

A network node located on the same link as the network node.

IPv6 interface

Physical or logical interface on which IPv6 is activated.

Path MTU

Maximum permitted packet size on a path from a sender to a recipient.

Path MTU discovery

Mechanism for determining the maximum permitted packet size along the entire path from a sender to a recipient.

LLA

Link local address FE80::/10

As soon as IPv6 is activated on the interface, a link local address is formed automatically. Can only be reached by accounts located on the same link.

ULA

Unique Local Address

Defined in RFC 4193. Via this address, the IPv6 interface can be reached in the LAN.

GUA

Global Unicast Address Via this address, the IPv6 interface can be reached, e.g. via the Internet.

Interface ID

The interface ID is formed with the EUI-64 method or manually.

EUI-64

Extended Unique Identifier (RFC 4291); method for forming the interface ID. In Ethernet, the interface ID is formed from the MAC address of the interface. Divides the MAC address into the manufacturer-specific part (OUI) and the network-specific part (NIC) and inserts FFFE between the two parts.

Example:

MAC address = AA:BB:CC:DD:EE:FF

OUI = AA:BB:CC

NIC = DD:EE:FF

EUI-64 = OUI + **FFFE** + NIC = AA:BB:CC:**FF:FE**:DD:EE:FF

Scope

Defines the range of the IPv6 address.

1.3.3 Active and passive network components

Active and passive network components

Industrial Ethernet networks are created using *active* and *passive* network components:

- Active network components are for example switches, access points, client modules, media converters and link modules.
- Passive network components are, for example, power cables and plug connectors.

The following tables contain a selection of network components for PROFINET/Industrial Ethernet.

Table 1- 1 Active network components for PROFINET/Industrial Ethernet

	Components	Remarks
Copper (electrical)	SCALANCE X switches	To interconnect nodes on Industrial Ethernet and to set up networks with more complex topologies
	PN/IO Link	Used to couple PROFINET to PROFIBUS
	SCALANCE S	"Security Module" to secure networks against unauthorized access
	Media and extender modules	To expand the functionality of SCALANCE X switches
Fiber-optic cable (optical)	SCALANCE X switches	see above
Radio (wireless)	SCALANCE W access point and client modules	Components for wireless transmission of Ethernet
	IWLAN/PB Link PN IO	For wireless coupling of Industrial Ethernet to PROFIBUS DP
	SCALANCE M	For the wireless linking of Industrial Ethernet-based programmable controllers on the UMTS/GSM mobile wireless network

Table 1- 2 Passive network components for PROFINET/Industrial Ethernet

Medium	Connectors	Cable type / transmission medium Standard
Copper (electrical)	RJ-45 plug-in connector IE FC RJ-45 plug 90/145/180 M12 cable connector D-coded	Two-pair, symmetrical and shielded copper cable: IEC 61158 IE FC TP standard cable GP 2x2 IE FC TP robust standard cable GP2x2 IE FC TP flexible cable GP 2x2 IE FC TP robust flexible cable GP 2x2 IE FC TP trailing cable GP 2x2 IE FC festoon cable GP 2x2 IE FC TP food cable 2x2 IE TP torsion cable GP 2x2 IE TP train cable 2y2 IE FC TP trailing cable 2x2 IE FC TP marine cable 2x2 IE FC TP FRNC cable GP 2x2 IE TP ground cable 2x2 8-wire cable for Gigabit Ethernet: IE FC TP standard cable (22 AWG) 4x2 IE FC TP standard cable GP (24 AWG) 4x2
Fiber-optic cable (optical)	SC RJ plug ISO/IEC 61754-24	POF FO cable (Plastic Optical Fiber) ISO/IEC 60793-2-40
		PCF FO cable (Plastic Cladded Fiber) ISO/IEC 60793-2-30 PCF standard cable GP PCF trailing cable PCF trailing cable GP (for SC RJ plug)
	BFOC (Bayonet Fiber Optic Connector) ISO/IEC 60874-10 SC plug ISO/IEC 60874-14	Glass fiber cable - multimode fiber (62.5/125 µm) ISO/IEC 60793-2-10 Fiber-optic standard cable INDOOR fiber-optic indoor cable Flexible fiber-optic trailing cable SIENOPYR shipping duplex FO cable (for BFOC connectors) Glass fiber cable - multimode fiber (50/125 µm) ISO/IEC 60793-2-10 FO standard cable GP FO trailing cable FO trailing cable GP FO ground cable (for BFOC and SC connectors)

Medium	Connectors	Cable type / transmission medium Standard
Radio (wireless)	N-Connect R-SMA SMA QMA	IEEE 802.11/mobile wireless (2G, 3G, 4G) Antenna cables (in each case standard cable and cables suitable for railway applications): • N-Connect/R-SMA male/male flexible connection cable for connecting antennas to SCALANCE W700 devices with R-SMA connector. • N-Connect male/male flexible connection cable e.g. for connecting antennas to SCALANCE W700 devices with N connector. • N-Connect/SMA male/male flexible connection cable for connecting antennas to SCALANCE M800 devices • QMA/N-Connect male/female adapter cable for antennas with a QMA socket. Antennas: • Antennas for IWLAN acc. to IEEE802.11n with 1 connector, 2 connectors or 3 connectors (MIMO). • Antennas for mobile wireless (2G, 3G and 4G). • IWLAN RCoax cable.

Note

Cable assembly

FastConnect cables can be assembled particularly fast and simply on site. This means that RJ-45 cabling technology, an existing standard, is also available in a version suitable for industry.

Product overview

You will find detailed overview of the available modules and accessories in the chapters 4 - 8.

Passive components for Industrial Ethernet and accessories

You will find an overview of the passive components and further accessories in the system manual Industrial Ethernet/PROFINET Passive Network Components.

Passive components for IWLAN

You will find detailed overview of the passive components in the "Passive network components IWLAN" system manual.

See also

SCALANCE X switches and media converters (Page 114)
SCALANCE W components for Industrial Wireless LAN (Page 156)
SCALANCE M routers and modems (Page 185)
SCALANCE S security module (Page 206)
Communications processors for PCs (Page 225)
Communications processors for SIMATIC S7 (Page 239)
Compact switch module (Page 267)
Accessories (Page 222)

1.3.4 Management functions

SNMP

With the aid of the Simple Network Management Protocol (SNMP), you can monitor and control the network elements (e.g. routers, servers, switches, printers, computers etc.) from a central station. SNMP controls the communication between the monitored devices and the monitoring station.

SNMPv1 and SNMPv2c

In versions v1 and v2c, SNMP has no security mechanisms. Each user in the network can access data and also change parameter assignments using suitable software.

For the simple control of access rights without security aspects, community strings are used. The community string is transferred along with the query. If the community string is correct, the SNMP agent responds and sends the requested data. If the community string is not correct, the SNMP agent discards the query.

SNMP data packets are not encrypted and can easily be read by others. The monitoring is handled by "SNMP agents". SNMP agents are programs that execute on the devices to be monitored and send SNMP data packets to an SNMP manager. The data is described in a Management Information Base (MIB). The RFC 1213 document contains the definition of the MIB-2 important for SNMP.

SNMP v3

Compared with the previous versions SNMP v1 and SNMP v2c, SNMP v3 introduces a comprehensive security concept.

SNMP v3 supports

- Fully encrypted user authentication
- Encryption of the entire data traffic
- Access control of the MIB objects at the user/group level

Note

To further improve security, separate the administration network from the remaining network as a separate unit if this is possible.

DynDNS

Dynamic Domain Name Servers (DynDNS) allow applications to be reached on the Internet using a host name, for example myHost.org. Even if these applications do not have a fixed IP address and the host name is not registered. If, for example, you register a SCALANCE device for a DynDNS service, you can reach the device from the external network using a host name, for example SCALANCE.dyndns.org.

1.3.5 Power over Ethernet**Power supply via the Ethernet cable**

In the IEEE 802.3af/at standard, the option of supplying devices with direct current was standardized. To achieve this, either the wire pairs of the network cable not used for data transfer are used or the supply voltage is modulated onto the data lines (phantom power).

The supply voltage and the load specified in the 802.3af standard differs from the 802.3at standard. The standards are abbreviated as PoE or PoE plus.

The following voltages or power are available:

Table 1- 3 PoE parameters

Characteristic	802.3af (also 802.3at type 1 or PoE)	802.3at type 2 (also PoE plus)
Power available on PDs - powered devices	12.95 W	25.50 W
Maximum power output of the power sourcing equipment (PSE)	15.40 W	34.20 W
Voltage range on the power sourcing equipment (PSE)	44.0-57.0 V	50.0-57.0 V
Voltage range on the end device (PD)	37.0-57.0 V	42.5-57.0 V
Maximum current flow	350 mA	600 mA per node
Maximum cable resistance	20 Ω (category 3)	12.5 Ω (category 5)
Power management	When the connection is first established, 3 power classes are negotiated	When the connection is first established, 4 power classes are negotiated or there is continuous negotiation in steps of 0.1 W
Reduction of the maximum operating temperature of the cable	None	5 °C for an active mode (2 pairs)
Supported cable types	CAT 3 and CAT 5	CAT 5, CAT 5e, CAT 6
Supported modes	Mode A (endspan), mode B (midspan)	Mode A (endspan), mode B (midspan)

Modes

- Mode A
Phantom power via the data wires with
 - 10BASE-T
 - 100BASE-TX
 - 1000BASE-T
- Mode B
Wire feed in via the unused wires with
 - 10BASE-T
 - 100BASE-TX

In both cases, a 4-pair Ethernet cable is required since the contacts 4-5 and 7-8 are used for power supply. All CAT 5 and CAT 5e cables meet these requirements.

Safety circuit to protect devices without PoE capability

To ensure that you do not damage any devices without PoE capability by using PoE or PoE plus, a safety circuit is defined:

- If the PSE identifies a resistance of 25 k Ω between the power wires, the end device is capable of PoE. The power voltage is raised slowly by the PSE.
- If the PSE detects other resistance values, the power is not increased or it is turned off.

Classification of the power sourcing equipment (PSE)

- Endspan
With endspan, the power is supplied via a switch that can reach a device over an Ethernet cable. The switch must be capable of PoE. The two modes can be used in parallel if the devices with PoE capability support this.
- Midspan
Midspan is used when the switch is not PoE-compliant. The power is supplied by an additional device between the switch and end device. In this case, only data rates of 10/100 Mbps can be achieved because the power is supplied on redundant wires.

SIMATIC NET devices with PoE

Some devices of the SCALANCE W und SCALANCE X series are capable of PoE. The abbreviations in brackets describe the way in which PoE is supported.

- **PSE** stands for Power Source Equipment, the device can take over the power supply.
- **PD** stands for Powered Device, the device is a power consumer.

PoE according to 802.3af (also 802.3 type 1)

- SCALANCE W7xx RJ-45 (PD)
- SCALANCE W786-x RJ-45 (PD)

- SCALANCE W774-1 RJ-45 (PD)
- SCALANCE W734-1 RJ-45 (PD)
- SCALANCE X108PoE (PSE)
- SCALANCE X308-2M PoE
- SCALANCE XR300 PoE (PSE)

PoE plus according to IEEE 802.3at type 2

- SCALANCE W7xx RJ-45 (PD)
- SCALANCE W786-x RJ-45 (PD)
- SCALANCE W774-1 RJ-45 (PD)
- SCALANCE W774-1 M12 EEC (PD)
- SCALANCE W734-1 RJ-45 (PD)
- SCALANCE X108PoE (PSE)
- SCALANCE X308-2M PoE
- SCALANCE XR300 PoE (PSE)
- SCALANCE XM-400 (PSE), when a port extender PE408PoE is used.
- SCALANCE XR528-6M (PSE), when media modules MM992-4 PoE or MM992-4 PoEC are used.
- SCALANCE XR552-12M (PSE), when media modules MM992-4 PoE or MM992-4 PoEC are used.

1.3.6 Fault tolerance and redundancy

Overview

Fault-tolerant systems are designed to reduce production downtime. Availability can be enhanced, for example, by means of component redundancy. Communication systems are thus extended to automation systems.

Redundant systems in industrial Ethernet are characterized by the multiple (redundant) presence of important automation components. When a redundant component fails, processing of the program is not interrupted.

Redundancy is achieved by duplicating the part components such as CPU, network, CP, etc.

Monitoring and synchronization mechanisms ensure that if the active redundant connection path fails, the previously passive (redundant) connection path takes over the communication automatically. The connection itself remains established.

Redundant network

The following graphic illustrates the principle of the high availability based on the example of a redundant network. The entire cable topology exists twice, in the following graphic represented as "LAN A2 and "LAN B". The connected components must be suitable for redundant operation which is the case with the SIMATIC NET modules with "RNA" in the name (abbreviation for "Redundant Network Access). Every component is connected to both networks and all data is transported at the same time via both networks. If one of the transmission paths is interrupted, the communication via the parallel network is unaffected.

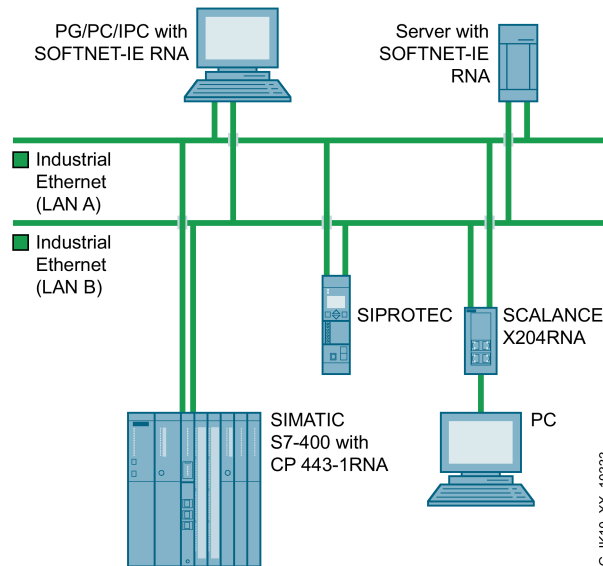


Figure 1-3 Topology example of a redundant network

1.3.7 Access Methods

Switching mechanisms

PROFINET is based on Fast Ethernet with 100 Mbps or Gigabit Ethernet with 1000 Mbps and switch mechanisms and has further developed this technology.

Compared with other methods this has the advantage that each node can send at any time since it always has a free point-to-point connection to the next switch. The connection is bidirectional. The nodes can send and receive in both directions at the same time (full duplex).

Switches in SIMATIC meet the real-time properties in PROFINET with two transmission techniques "Store and Forward" and "Cut through".

"Store and Forward"

With the transmission technique "Store and Forward", the device stores the frames and then enters them in a waiting queue. The frames are now forwarded selectively to the port that has access to the addressed node.

If the device supports the international standard IEEE 802.1Q the frames are sorted into different queues according to their priority. First, the frames with the highest priority are processed.

Advantage

With the transmission technique "Store and Forward", the frames are checked that they are correct and valid. This prevents bad or damaged frames being distributed through the network.

Cut through

With the transmission technique "Cut Through" the entire frame is not stored temporarily in a buffer but forwarded directly to the destination port as soon as the first 6 bytes (destination address) have been read and the destination port identified.

The times that the data packet requires to pass through the switch are minimal and not dependent on the frame length. The data is only stored temporarily using the store and forward mechanism according to its priority when the section between the target part and the port of the next switch is in use.

With PROFINET switches Cut Through is implemented by using ERTEC ASICs, for example in the IRT switches of SCALANCE.

See also

Switches and switched LANs (Page 42)

1.3.8 Layer 3 functions

Introduction

The term layer 3 function effectively means routing. The term routing describes the specification of paths (routes) for communication between different networks. This means: how a data packet travels from subnet A to subnet B.

Devices with layer 3 functionality are also known as layer 3 switches. Layer 3 switches can operate both at OSI layer 2 (MAC address) or at OSI layer 3 (IP address).

A layer 3 switch can assign various subnets to its ports, e.g. subnet A and subnet B. This allows large networks to be divided into smaller subnets with their own address space. Reasons for dividing into subnets include, for example, the separation of the Ethernet network to reduce data traffic, the separation of sensitive areas from the main network and the division of the network into logical workgroups.

The data packets are forwarded either using the Cut Through or the Store and Forward technique.

Static routing

In static routing, the paths that a data packet can take are entered permanently (statically) in the routing table.

Dynamic routing

With dynamic routing, the paths that a data packet can take are identified dynamically between the routers involved, see also "Dynamic routing with OSPF".

Router redundancy with VRRP

With the aid of the Virtual Router Redundancy Protocol the failure of a router in a network can be countered. VRRP, for example, provides the option of setting up device redundancy for the default gateway of the end devices.

Several physical routers in a network segment are grouped together to form a logical group. A virtual MAC and IP address then apply for this area. One router of this group is made master. This master adopts the virtual MAC and IP address of the area. The other routers of this group are then backup routers. If the master fails, another router from the group takes over the virtual MAC and IP address and the tasks of the failed router. This means that the network area affected can continue to communicate with the outside world. The network segment can no longer be reached only after the failure of the last router in the group. Due to the backup router adopting the virtual MAC and IP address, no other actions are necessary for the other routers in the area of the segment. Routing tables or the ARP cache do not need to be updated. This minimizes the consequences of device failure.

Dynamic routing with OSPFv2

Open Short Path First is a routing protocol developed by the Internet Engineering Task Force (IETF). With OSPF, CIDR (Classless Inter-Domain Routing) and VLSM (Variable Length Subnet Mask) are also implemented.

The routers setup a neighborhood database (LSDB = Link State DataBase). The neighborhood database is the heart of OSPF and contains information on the topology of the network.

To set up the neighborhood database, the router needs to learn its direct neighbor routers. To do this, the router sends out Hello packets following initialization. The neighbor routers exchange packets (LSA - Link State Advertisements) that describe the content of their database. When the exchange of information with the neighbor router is completed the neighborhood database of the neighbor routers is the same.

The neighborhood database is used to calculate routes based on the SPF algorithm (Shortest Path First). The algorithm creates a hierarchical tree structure (Shortest Path Tree) in which each destination with the shortest (loop-free) and lowest cost route is entered. The algorithm uses the costs of the path as a metric. What is used to calculate the costs is not defined. The costs can be, for example, the data rate of the connection or the reliability of the connection. The entries from the tree are adopted in the routing table. If several routes with the same costs exist for a destination, the data is transferred via different routes to achieve load distribution.

The routers continuously test the state of the connection between themselves by exchanging Hello packets. If a connection is disrupted, the router sends a message to its neighbor

router. The neighbor router updates its database and sends the message to its neighbor router and so on until the modification has passed through the entire network.

To limit the size of the routing table, OSPF can divide a network (autonomous system) into hierarchical areas. Each area has its own neighborhood database and its own shortest path tree.

By dividing into areas, if there is change in the topology, the entire network is not loaded with messages so that OSPF manages with relatively low overheads.

If several neighbor routers can be reached in an area, the designated router (DR) and the backup designated router (BDR) are identified based on Hello packets. By identifying the designated router, the topology is simplified. The designated router then sends the message.

To send a frame from area 1 to area 2, the frame is first sent to the area border router (ABR) of area 1. The ABR connects its area to the backbone area. The ABR of area 1 sends the frame to the router in the backbone area that forwards the frame to the ABR of area 2. The backbone area (area 0) is used to distribute routing information about the reachability of areas between area border routers. A frame is sent to another AS via an Autonomous System Area Border Router (ASBR). On the ASBR, one interface is connected to another AS, for example an AS that uses the RIP routing protocol.

With OSPF, messages can be authenticated. Only trustworthy routers can take part in the routing with OSPF.

1.3.9 EtherNet/IP

Introduction

EtherNet/IP is an Ethernet protocol that meets real-time requirements within certain limits. EtherNet/IP can be implemented with standard Ethernet hardware, however the restrictions in terms of the cycle time in Ethernet also apply.

Technical basics

Time-critical IO communication is sent in EtherNet/IP as multicast using UDP, which however results in a high network load. This can be eliminated in part by using managed switches with "IGMP snooping". In addition to this, the field devices need to provide a high computing power because the IP stack is used for IO data. Nodes are addressed using the IP address and some standard technologies such as DHCP and BootP are supported by EtherNet/IP. For time synchronization, the Precision Time Protocol according to IEEE 1588 is used.

1.4 Switches and switched LANs

If a network needs to be divided into several (logical and physical) subunits, switches are used at the connection points of the network sections.

Switches are active components that can receive and send at several ports independently. They are equipped with intelligence that allows them to forward received messages only via the port connected to the segment in which the actual addressee is located. This can be connected directly to the port or via a further switch.

Since all direct connections are point-to-point and since the medium used allows full duplex communication, it is no longer possible for collisions to occur.

Switched connection paths: "Shared LANs" and "Switched LANs"

"Shared LANs" are networks on which a message being transmitted blocks the network for all other nodes; in other words, there can only be one sender at any one time. A wireless network is a simple example of such a shared LAN.

"Switched LANs" are set up using switches and are characterized by the connection paths for each data packet being switched based on the target address. Different data packets can be in transit in the network at the same time on different connection paths. The data packets only run through segments that lead to the recipient. All the SCALANCE X products belong to the products that operate according to the switching method and therefore create "switched LANs".

Functions of switches

Essentially, switches have the following functions:

- **Connection of subnetworks**
Switches connect several collision domains. This allows extensive networks to be set up with numerous nodes and simplifies network expansion. The distance covered depends on the FO interfaces or electrical interfaces used in the devices. You will find information on the achievable distances in the system manual Industrial Ethernet/PROFINET Passive Network Components.
- **Separating load**
By filtering the data traffic based on the Ethernet (MAC) addresses, local data traffic remains local. The data is distributed to all ports/network nodes using the direct switching method. Only data intended for nodes in other subnets is switched from the input port to the appropriate output port of the switch. To make this possible, a table assigning Ethernet (MAC) addresses to output ports is created by the switch in a "teach-in" mode.
- **Limiting errors to the affected subnetwork.**
By checking the validity of a data packet on the basis of the checksum which each data packet contains, the switch ensures that bad data packets are not transported further. Collisions in one network segment are not passed on to other segments.

Advantages of switched LANs

The advantages of such switched LANs are:

- Good performance (since the messages only block the sections of cable actually between the sender and receiver),
- Avoidance of data collisions because the sender does not block the entire network
- High availability particularly in topologies that include redundancy,

If a connection path is blocked in a redundant topology (due to a cable break or component failure), switches can still redirect the messages over an alternative path and maintain communication. A network with a ring topology (see below) is a classic example of using switches in this way.

- Option of forming subnets and network segments,
- Simple rules for network configuration,
- Simple, expansion is possible without affecting the existing network.

Application example: Redundant ring

Using an IE Switch X-300 as the redundancy manager in a ring with a redundancy manager (Page 65) provides greater availability. If there is an interruption on the connection between these switches, the IE switch used as redundancy manager acts like a switch and in a very short time creates a line (bus) from the ring. As a result, a functional, end-to-end structure is restored.

1.5 Wireless LAN

1.5.1 What is wireless LAN?

WLAN

A wireless LAN or WLAN is a "Wireless Local Area Network"; in other words a network based on wireless covering a limited area. WLAN is based on the IEEE 802.11 standard.

IWLAN

The Industrial Wireless LAN (IWLAN) technology is a further development of WLAN for industrial applications. In contrast to WLAN, IWLAN provides predictable data traffic (deterministic) and defines response times for high-speed applications. This makes it possible to transfer process-critical data, for example alarms. By implementing a wireless solution, you can replace hard-wired connections that are subject to natural wear and tear, for example contact conductors. Use cases for wireless solutions such as overhead monorails, driverless transport systems or user-specific operator control and maintenance devices.

To protect data traffic, rugged and immune modules are used on the one hand and on the other hand the data is encrypted.

1.5.2 Differences between wireless LAN and wired networks

Cable as opposed to radio waves

The use of cables and wires for communication has certain advantages because this makes an exclusive medium available:

The transmission properties in a hard-wired network are defined and remain the same as long as the cable, routers or similar are not replaced. Since a wired network is limited in locality, it is possible to recognize at any time which nodes are connected to a LAN (Local Area Network) and which are not.

On the other hand, the effort and cost of cabling increases with the number of nodes and, at the same time, the potential for broken cables and other hardware faults. Finally, communication with freely moving nodes using wired methods is practicable only in exceptional situations. Wireless links also allow sections to be covered that would be problematic using cables, for example roads, water.

In these situations, wireless networks are an advantage. The advantage is in the mobility of the individual components and their flexible use.

"Wireless" as such is a limited resource. Due to its nature as a "shared medium" it is not possible to increase the capacity as would be possible, for example, by simply laying more cable. This means that with the increasing number of nodes, the effective data rate that can be reached by the individual nodes sinks.

Complexity of the RF field

Radio waves propagate through space and are deflected by obstacles or weakened when passing through. This means that an RF field with a complex structure is created that changes when the obstacles move. The area illuminated by one or more transmitters is not sharply defined. There is also no clear delineation of the RF field and the transmission characteristics of the individual nodes in the wireless network fluctuate depending on their position. Lastly, it is also practically impossible to detect a "silent listener" in a wireless network.

These properties need to be taken into account in terms of the reliability of the wireless link and the security of a network against eavesdropping and immunity to interference. Wireless networks are, however, just as reliable, secure and resilient as hard-wired networks if trained employees are deployed who are aware of the particular demands of a wireless network.

1.5.3 Preferred areas of application for WLANs

Preferred areas of application

In many environments, their special qualities make wireless networks the preferred, and in some cases only practical medium.

These include:

- Connection of mobile nodes both among themselves and with stationary nodes,
- Connection of mobile nodes with wired networks (Ethernet etc.),
- Contact with rotating nodes (cranes, carousels, ...),
- Connection of nodes with restricted mobility (monorail suspension tracks, high-bay storage racks, ...), as a replacement for slip contacts or trailing cables,
- Establishing wireless bridges between physically separate wired subnets (different buildings, across streets, over water, ...),
- Communication with nodes in inaccessible areas.

1.5.4 The standards of the "IEEE 802.11" series

Standardization of WLANs

IEEE

The acronym "IEEE" stands for the Institute of Electrical and Electronics Engineers, an organization that has taken on the task of developing, publishing and promoting electronic and electrotechnical standards and that can be compared in some ways with DIN.

The IEEE 802.11 group

Under the project number "802", a number of working groups were given the task of developing standards for setting up and operating networks. A known example is the "802.3" working group that is concerned with the standards for Ethernet connections.

The "802.11" working group concentrates on the specification for wireless LAN, the IEEE 802.11 standard. The most important expansions of the standard are "802.11 a/h", "802.11 b/g" and "802.11n".

"802.11" standards

The following table provides an overview of the features of the individual standards.

	802.11 "a"/"h"	802.11 "b"	802.11 "g"	802.11 "n"	802.11 "ac"
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz + 5 GHz	5 GHz
Gross data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1733 Mbps
Modulation	OFDM	DSSS	OFDM	MIMO	4x4 MIMO

Expansions of the 802.11 standard include the following:

- 802.11 "e": Introduces QoS to provide better support for real-time applications (VoIP, streaming),
- 802.11 "i": Replaces the no longer tenable WEP encryption mechanism with WPA or WPA2.
- 802.11 "p": Introduces WLAN technology for motor vehicles with which an interface for applications involving intelligent traffic systems is created.

1.5.5 IEEE 802.11n

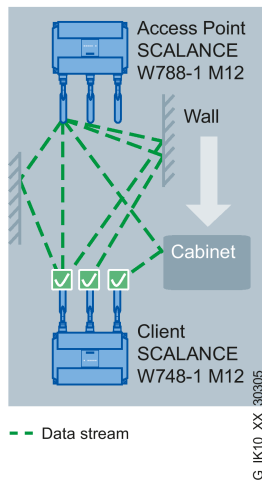
The standard IEEE 802.11n is an expansion of the 802.11 standard and was approved in 2009.

Previous Standards worked either in the 2.4 GHz frequency band (IEEE 802.11g /b) or in the 5 GHz frequency band (IEEE 802.11a). IEEE 802.11n can operate in both frequency band. In the IEEE 802.11n standard, there are mechanisms implemented in PHY and MAC layers that increase the data throughput and improve the wireless coverage.

With SCALANCE W700 devices, a data throughput up to 450 Mbps (gross) is possible due to support of the following mechanisms. This maximum data throughput is possible only if the mechanisms are used at the same time.

MIMO antenna technology

MIMO (Multiple Input - Multiple Output) is based on an intelligent multiple antenna system. The transmitter and the receiver have several spatially separate antennas. The spatially separate antennas transmit the data streams at the same time. Up to four data streams are possible. The data streams are transmitted over spatially separate paths and return over different paths due to diffraction, refraction, fading and reflection (multipath propagation). The multipath propagation means that at the point of reception a complex, space- and time-dependent pattern results as a total signal made up of the individual signals sent. MIMO uses this unique pattern by detecting the spatial position of characteristic signals. Here, each spatial position is different from the neighboring position. By characterizing the individual senders, the recipient is capable of separating several signals from each other.

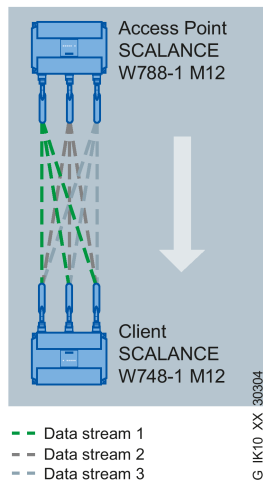


Maximum ratio combining (MRC)

In a multiple antenna system, the wireless signals are received by the individual antennas and combined to form one signal. The MRC method is used to combine the wireless signals. The MRC method weights the wireless signals according to their signal-to-noise ratio and combines the wireless signals to form one signal. The signal-to-noise ratio is improved and the error rate is reduced.

Spatial mutliplexing

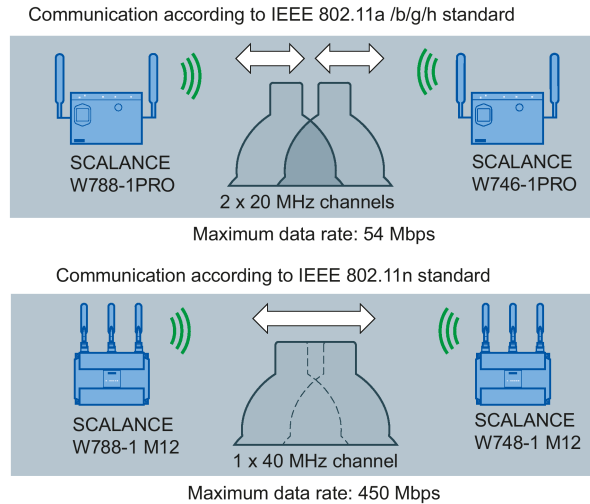
With spatial multiplexing, the data to be transmitted can be distributed over several transmitting antennas according to specified rules. The devices currently use a maximum of three antennas. The data stream is therefore divided among three transmitting antennas. As a result different data streams are transferred at the same time over three transmission paths. This allows the data throughput to be greatly increased. The spatially differing data streams are known as spatial streams. The number of spatial streams specified for an IWLAN (Industrial WLAN) is a measure of the transmission rate. Per data stream, a maximum of 150 Mbps is transferred according to IEEE 802.11n. With four antennas and four data streams this results in a maximum of 600 Mbps and with three antennas and three data streams 450 Mbps. Ideally the net data throughput is then over 200 Mbps which compared with traditional WLAN standards means an almost ten times higher transmission rate.



Channel bonding

With IEEE 802.11n, data can be transferred via two directly neighboring channels. The two 20 MHz channels are put together to form one channel with 40 MHz. This allows the channel bandwidth to be doubled and the data throughput to be increased.

To be able to use channel bonding, the recipient must support 40 MHz transmissions. If the recipient does not support 40 MHz transmissions, the band is automatically reduced to 20 MHz. This means that an IEEE 802.11 access point can communicate with 802.11a/b/g/h and 802.11n products within the network.



Frame aggregation

With IEEE 802.11n, it is possible to group together individual data packets to form a single larger packet; this is known as frame aggregation. There are two types of frame aggregation: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU).

The frame aggregation reduces the packet overheads. Frame aggregation can only be used if the individual data packets are intended for the same receiving station (client).

Accelerated guard interval

The guard interval prevents different transmissions being mixed together. In telecommunications, the guard interval is also as intersymbol interference (ISI).

The guard interval of IEEE 802.11a /b/g is 800 ns. IEEE 802.11n can use the reduced guard interval of 400 ns.

1.5.6 Encryption and data security

WPA2 and AES ("Advanced Encryption Standard")

WPA2 is seen as a standard today and differs from WPA essentially in the encryption method: The weaknesses identified in WPA no longer exist in the AES method used in WPA2.

When a "sensible" password is selected that is adequately long and cannot be guessed at, AES encrypted messages count as being safe from eavesdropping according to today's state of the art.

WPA ("Wi-Fi Protected Access")

WPA is the further development of WEP. Apart from technical modifications in the actual encryption algorithm, the protocol was also adapted:

- Passwords for network access (authentication) are stored on a central server ("RADIUS"),
- The key for frame transmission changes dynamically making statistical attacks more difficult,
- The MAC address is worked into the key (in other words, unique hardware identification) of the sender making it more difficult to falsify the sender of the message.

WEP ("Wired Equivalent Privacy")

WEP is the oldest and at the same time the least secure encryption method with which WLAN transmission is protected against unauthorized intruders according to the 802.11 standard.

With this method, a user password is used as a key from which a series of pseudo random numbers is generated. Each character of the frame to be transmitted is then encoded with next number of this series and decoded at the receiver.

Today, WEP is considered insufficiently secure.

EAP ("Extensible Authentication Protocol")

The acronym EAP covers a wide framework of different authentication mechanisms for network access. In other words, EAP is not an authentication method itself but describes the mechanism according to which the client and server can agree on a method.

1.5.7 Avoiding collisions in wireless networks

CSMA/CA with RTS/CTS

Ethernet uses the bus access method CSMA/CD. This acronym stands for Carrier Sense Multiple Access with Collision Detection. After the node wanting to send has listened to the line and identified it as being free (Carrier Sense CS), the data is sent.

While sending, the sending node can recognize a collision (Collision Detection, CD) with other nodes sending at the same time (Multiple Access, MA) based on a disturbed level and end the transmission.

This mechanism is used in just the same way in a wireless network apart from the fact that collisions are deliberately avoided (Collision Avoidance, CA) to avoid reducing the net data throughput unnecessarily. For this reason wireless LANs do not use the CSMA/CD method with which collisions can occur and be detected, but rather the CSMA/CA method (Carrier Sense Multiple Access with Collision Avoidance).

Instead of physically listening in on the channel, a communications protocol is used that reserves the channel for a specific time. Before sending, a node checks whether or not the medium is free.

In this so-called RTS/CTS method, the node wishing to transmit sends a short test signal ("Ready To Send" - RTS). The actual transmission begins after the recipient has replied to this with "Clear To Send" (CTS). If a collision occurs, the retransmission follows after a pause not selected at random but according to priority. With this strategy, communication remains deterministic.

1.5.8 Structure of an IWLAN

Basic structure of a WLAN

WLANs do not have a physical topology like traditional wired networks. There are no "buses", "rings" or "stars". Instead wireless networks are divided into cells.

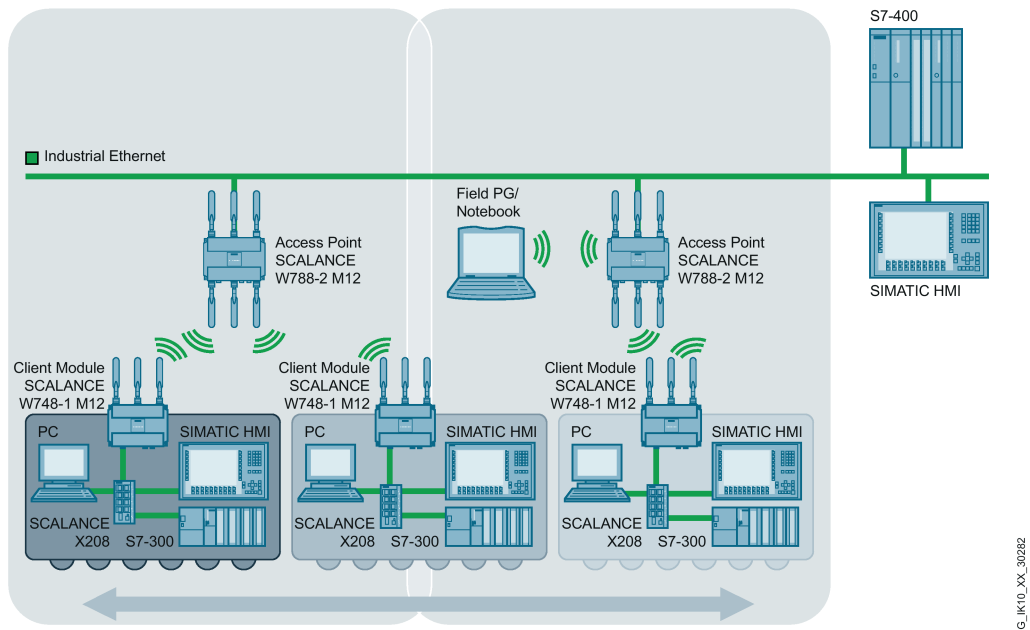


Figure 1-4 Simple WLAN structure with two access points/wireless cells, RCoax cable and IWLAN/PB Link PN IO gateway

Here, access points take over the role of switches. End nodes are connected to the network by turning on so-called "clients". Larger networks can be achieved by setting up several wireless cells each under the control of an access point. The connection between individual cells is also via access points.

The access points function as their own wireless cell, between which the mobile nodes can move. ("roaming")

Shared medium instead of switched medium

Wireless networks operate on the shared medium principle, in other words, only one node can send at any one time. With the increasing number of nodes, the effective data rate that can be reached by the individual nodes sinks.

1.5.9 Network structures

1.5.9.1 Infrastructure mode

In infrastructure mode, communication is handled via an access point. The nodes (clients) need to log on with the access point and transmit on the channel specified by the access point. The access point can manage the access rights of the clients and assign time slices to them for communication so that real-time and deterministic communication is assured.

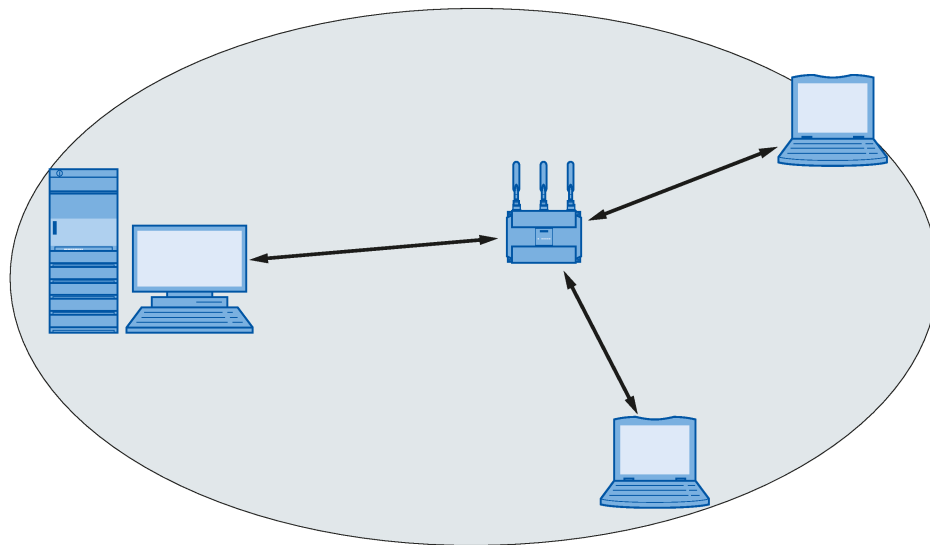
In the simplest case there is a group of clients in the wireless range of the access point. Such a network is also known as a standalone network.

If the wireless range of an access point is inadequate either because the reachable distance is too short or too few clients can be served, the network can be divided into several wireless cells. All clients within the wireless cell are within the range of a central access point (AP). The other clients only ever communicate with their access point and not directly with other clients. By connecting external antennas, the range and coverage can be adapted to the application. This means, for example that omnidirectional antennas in closed rooms can achieve distances between 30 m and 100 m.

Standalone networks

Coordination by an access point:

This configuration does not require a server and the SCALANCE W access point does not have a connection to a wired Ethernet. In this case, a central access point functions like a switch receiving the frames from the individual nodes (clients) and forwarding them.



Multichannel configuration

If neighboring SCALANCE W access points use the same frequency channel, this can lead to longer response times due to collisions that may occur. If the configuration shown in the figure is implemented as a single-channel system, computers A and B cannot communicate at the same time with the SCALANCE W access points in their cells.

If neighboring SCALANCE W access points are set up for different frequencies, this leads to a considerable improvement in performance. As a result, neighboring cells each have their own medium available and the delays resulting from time-offset transmission no longer occur.

The channel spacing should be as large as possible; a practical value is 25 MHz. Even in a multichannel configuration, all SCALANCE W access points can be configured with the same network name.

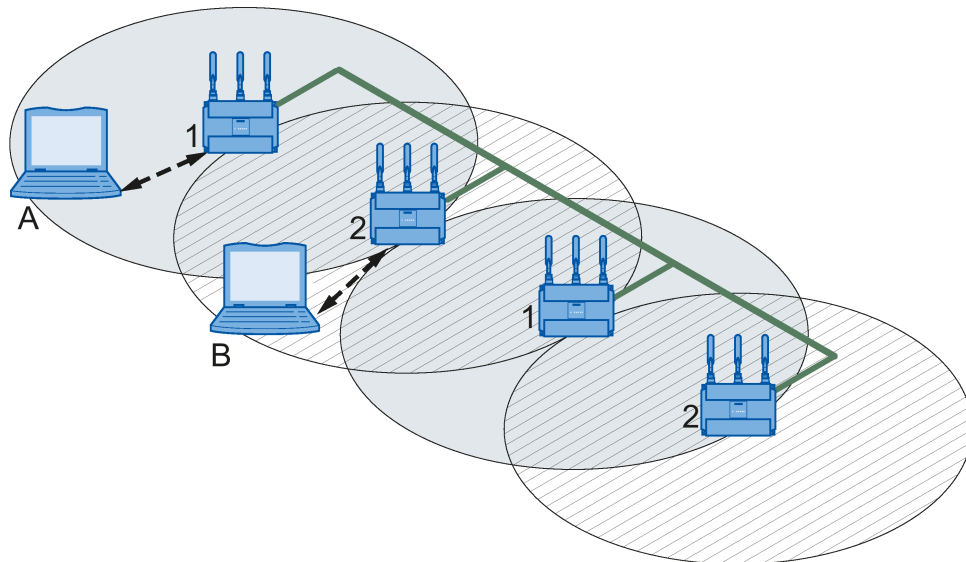


Figure 1-5 Multichannel configuration on channels 1 and 7 with four SCALANCE W access points

Wireless Distribution System (WDS)

WDS allows direct connections between SCALANCE W access points and or between SCALANCE W and other WDS-compliant devices. These are used to create a wireless backbone or to connect an individual SCALANCE W to a network that cannot be connected directly to the cable infrastructure due to its location.

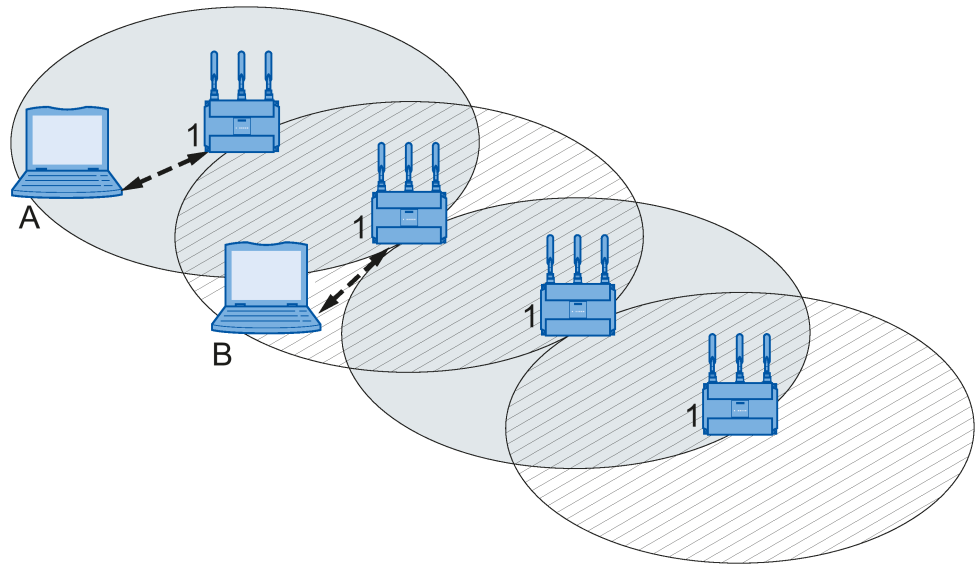
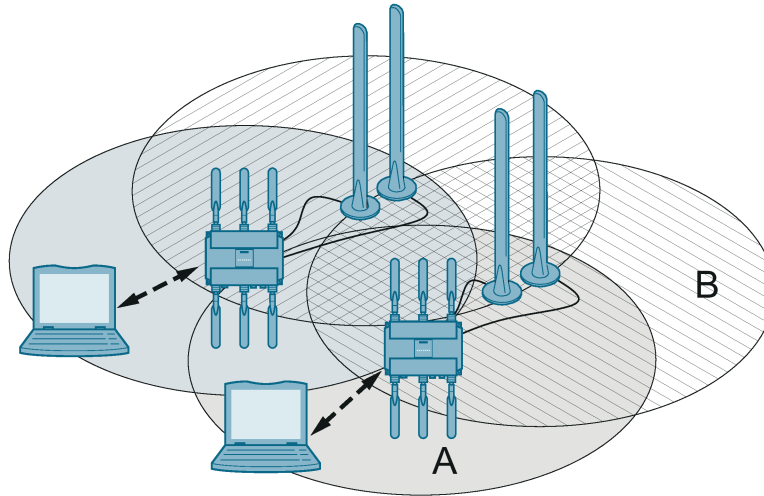


Figure 1-6 Implementation of WDS with four SCALANCE W access points

Redundant Wireless LAN (RWLAN)

RWLAN allows a redundant, wireless connection between two SCALANCE W access points with at least two WLAN interfaces. This is used to set up a redundant wireless backbone that cannot be implemented as a wired network due to its location but nevertheless has high demands in terms of availability.

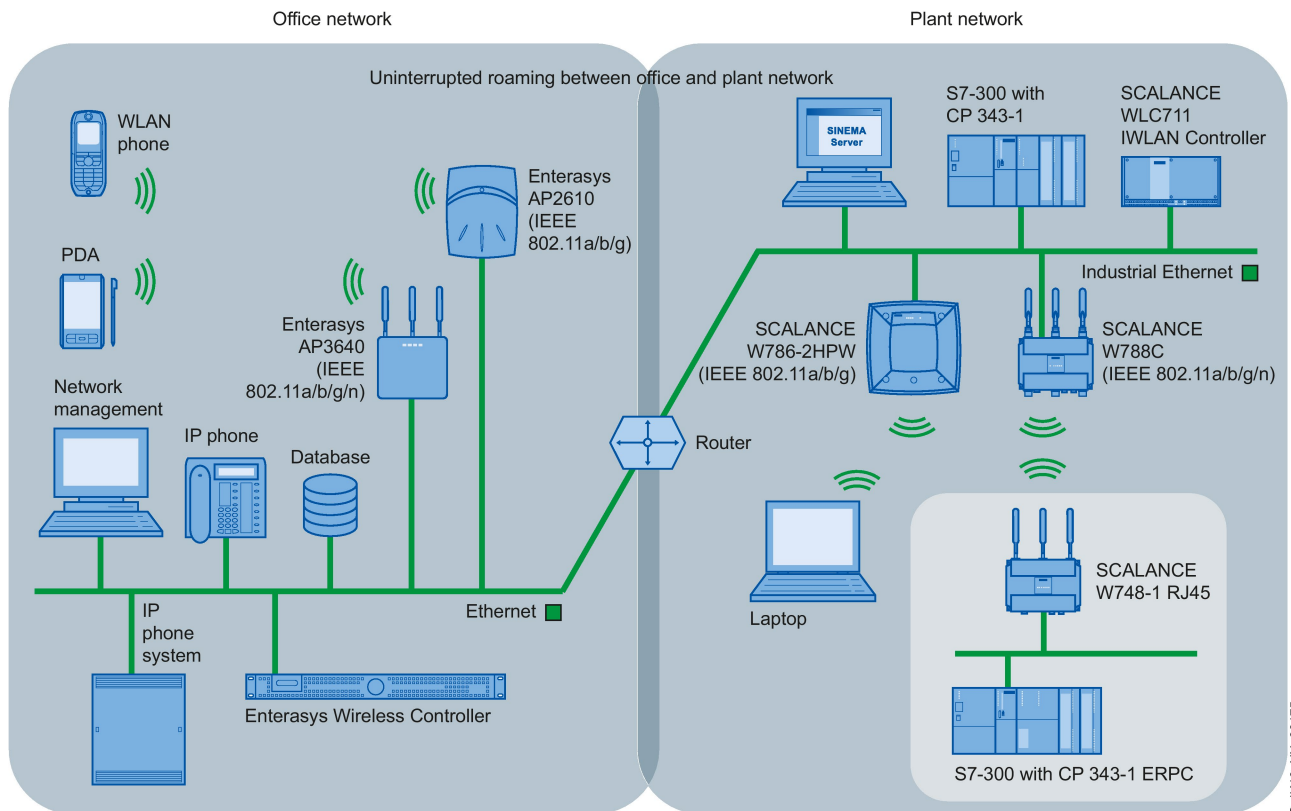


Controller-based network structure

The IWLAN controller SCALANCE WLC711 allows central management of up to 64 controller-based access points. The IWLAN controller automatically recognizes new access points, establishes the connection to them and manages and coordinates both access points and clients. Due to the layer 3 architecture, access points are also managed that are located in various layer 2 subnets. This function allows wireless expansion of an existing Ethernet network without changes being necessary to the existing network structure.

With the IWLAN controller, the IWLAN Wireless infrastructure can be divided into logical, service-based networks (Virtual Network Services). Different services, security requirements and access criteria can be managed reliably and different user groups, for example administrators, commissioning engineers or visitors can use the entire wireless network.

Various applications such as Voice-over-IP (VoIP), video and Internet access can use the same infrastructure.



G_IK10_XX_30175

Figure 1-7 Enterprise-wide WLAN based on Enterasys Wireless Controller and SCALANCE WLC IWLAN controller

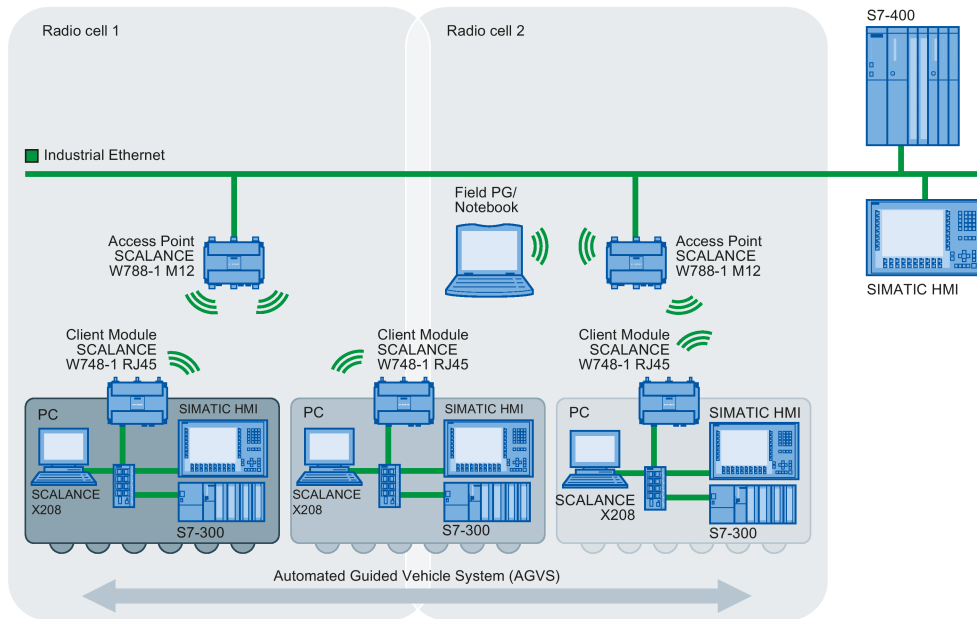
Redundant operation of two SCALANCE WLC711 devices increases the availability of the wireless network. With the IWLAN controller, only the controller-based access points of the SCALANCE W78xC series can be used.

Apart from central management and configuration of the wireless network, the IWLAN controller WLC711 also allows logging of errors, monitoring of the wireless network and documentation of network statistics.

Roaming

Clients moving between wireless cells: "Roaming"

To allow mobile nodes to be able to roam seamlessly from one access point to the next, the individual wireless cells must overlap. This is transparent for the application. The access points need to be interconnected via Industrial Ethernet or a wireless distribution system (WDS).



The figure above shows how a moving node (in this case an automated guided vehicle system) is handed over between two wireless cells: The client module runs regular scans of the wireless signals on all the channels stipulated by the standard being used. The client module then connects to the access point with the channel on which it finds the best reception. If the limit between wireless cell 1 and wireless cell 2 is reached, the connection to the access point of wireless cell 1 is terminated. From this time on, the access point of wireless cell 2 is responsible for the client module.

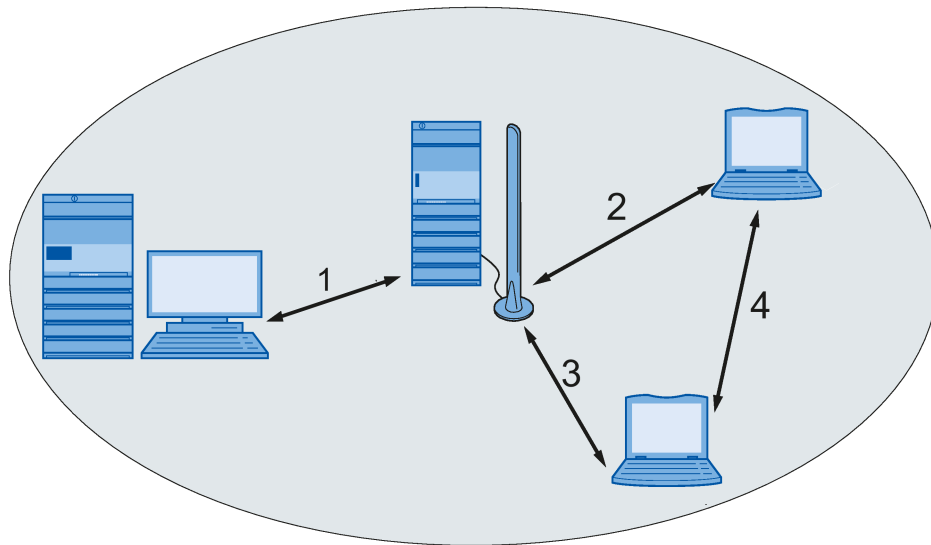
The time required for the change (handover time) is in the order of 100 ms. A significant reduction in handover times can be achieved with Rapid Roaming using the iPCF method ("industrial Point Coordination Function"). Both the access point and client must support rapid roaming.

With some devices, the support of the iPCF method is released by the KEY-PLUG "iFeatures" (example: SCALANCE W788-x), the SCALANCE W722-1 RJ45 supports this method already when shipped.

1.5.9.2 Ad hoc networks

Ad hoc networks

In ad hoc mode, nodes communicate with each other directly (connection 4) without involving an access point. The nodes access common resources (files or even devices, for example printers) of the server (connections 1 to 3 in the figure). This is, of course, only possible when the nodes are within the wireless range of the server or within each other's range. Ad hoc networks can only be operated with the standard 802.11 "b".



As an alternative, wireless networks can be configured in "infrastructure mode".

1.5.10 Other wireless technologies

Industrial Wireless Control

Industrial wireless control is the connection of widely distributed process stations to one or more central control systems. Various wireless methods are used for the communication required for monitoring and control. This makes service possible on installations without fixed telephone lines. An Internet access is also not necessary for the installation.

- GPRS

The General Packet Radio Service (GPRS) is a mobile wireless technology for packet-switched data transmission via GSM networks (Global system for mobile communications). The GSM wireless channels are divided into eight time slots. One time slot represents one transmission channel.

Packet-switched data transmission means that in contrast to line-switched data transmission (as with GSM), no transmission channel is reserved permanently. The sender divides the message into individual packets with additional information (packet sequence, recipient address). With the aid of the GPRS system, the packets are

forwarded through various time slots of the network. This makes it possible to use free capacity. A GPRS session can also use several time slots at the same time. The recipient then puts together the packets in the correct order. GPRS allows data exchange without connection establishment and billing only according to the transferred amount of data. Packet switching is made possible by IP technology. GPRS is used mainly for access in IP-based networks, for example the Internet.

- EGPRS

The Enhanced General Packet Radio Service (EGPRS) is an expansion of GPRS and is also known as Enhanced Data Rates for GSM Evolution (EDGE). EGPRS uses a different modulation technique (8-PSK) from GPRS that is more efficient. This means that a data rate up to four times higher can be achieved with EGPRS.

- UMTS

UMTS is the acronym for Universal Mobile Telecommunications System and is also known as a mobile wireless standard of the third generation (3G). The maximum transmission rate is 384 kbps.

- LTE

LTE stands for Long Term Evolution and is known as the 3.9G standard because it does not completely implement the 4G specification of the ITU-T standard. It supports six different bandwidths between 1.4 and 24 MHz and allows transmission rates up to 300 Mbps. The maximum data rate is only achieved when using 4x4 MIMO (multiple antenna technology). The high transmission rate, for example, allows the transfer of language via TCP/IP ("Voice over IP").

- LTE Advanced

LTE Advanced or also 4G is a protocol extension from LTE. It provides transmission rates up to 1000 Mbps and is downwards compatible to LTE. A further advantage is a higher number of users that can be active at the same time.

WirelessHART

HART (Highway Addressable Remote Transducer) is the wireless connection of field devices in process automation for advanced diagnostics.

Just like WLAN, WirelessHART also uses the ISM frequency band (2.4 GHz and with maximum of 250 kbps) and automatically establishes meshed networks. The span of the network is greater than the nominal wireless range of an individual node. The network organizes itself by having all the connection information evaluated by a network manager. With this information, redundant paths are made available automatically that can bridge the failure of individual nodes. The main focus during the development of WirelessHART was simple commissioning and maintenance of the self-organizing networks so that configuration involved only minimum effort. The main area of application of WirelessHART is in the regular transmission of small, non time critical-amounts of data at long intervals over relatively long distances. Thanks to the low energy consumption, battery working lives of several years are achieved.

Network structures and network configuration

2.1 Network structures

2.1.1 Network topologies

Network topologies are oriented according to the requirements of the equipment to be networked. The most common topologies include bus, star and ring structures. In practice, plants usually consist of mixed structures. These can be implemented both with electrical cables as well as with optical cables (fiber-optic cables).

Glass fiber-optic cables are used for long distances. For short distances, plastic fiber-optic cables such as Polymer Optic Fiber (POF) or plastic covered glass fibers such as Polymer Cladded Fiber (PCF) can be used.

2.1.2 Linear structure

Linear bus



The linear bus is the simplest network structure. It is characterized by a network backbone to which the individual nodes are connected directly or over a branch (only one node is permitted per branch).

- The advantage of the linear bus topology is its simple setup and low hardware investment. It is suitable, for example, for networking of rigidly linked machines over a wide area as found in assembly lines.
- The disadvantages of bus topologies are that the resources are not put to optimum use and that there is no redundancy: A break on the cable at any point cannot be bridged. Connecting the ends of the linear bus, on the other hand, creates a ring with which these disadvantages can be avoided.

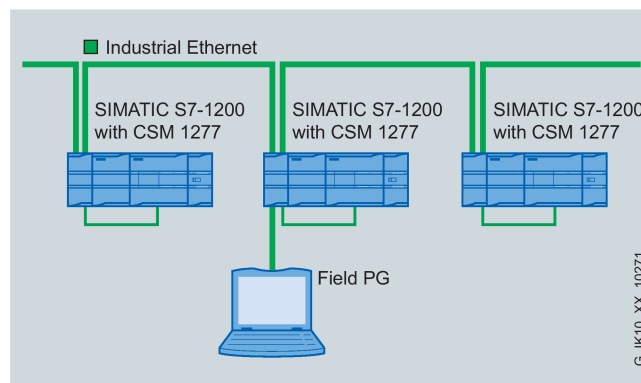


Figure 2-1 Linear bus network topology based on the example of Industrial Ethernet

A further restriction for networks with a linear bus structure is the physical arrangement of the network nodes. Depending on their position, the backbone may need take long detours which may, in turn, lead to problems with frame delay times. In a linear network topology, the network components such as switches typically have only one or few connection points for network nodes. Linear bus structures can also be created with devices with two integrated network interfaces.

Setup

The bus structure can be implemented with SCALANCE X switches. Any TP ports can be used to cascade and form a linear bus. The number of SCALANCE X switches that can be cascaded depends on the response times of the applications operating over this linear bus.

- Electrical cables

There may be a maximum distance of 100 m between two of these devices.

- Optical cables

At 100 Mbps, the maximum distance between 2 devices can be as follows:

- Multimode, glass, up to max. 5 km
- LD: Single mode, glass up to max. 26 km
- LH+: Single mode, glass up to max. 70 km

At 1 Gbps, the maximum distance between 2 devices can be as follows:

- Multimode, glass, up to max. 750 m
- LD: Single mode, glass up to max. 10 km
- LH: Single mode, glass up to max. 40 km
- LH+: Single mode, glass up to max. 70 km
- ELH: Single mode, glass up to max. 120 km

2.1.3 Star structure

"Star"



The difference between the star topology and linear bus topology is that one switch functions as the central node from which the spokes branch off to the individual nodes. The individual nodes of the network therefore have separate point-to-point links with the active network component (i.e. with the switch).

The immediate effect is that the messages only run via the spokes between sender and recipient, in other words network performance improves significantly because several nodes can communicate at the same time.

Depending on the requirements, in practice this may be a mixture of fiber-optic cables and twisted pair cables on the individual transmission links. Typical applications are Ethernet office networking or the networking of production cells in manufacturing with Industrial Ethernet.

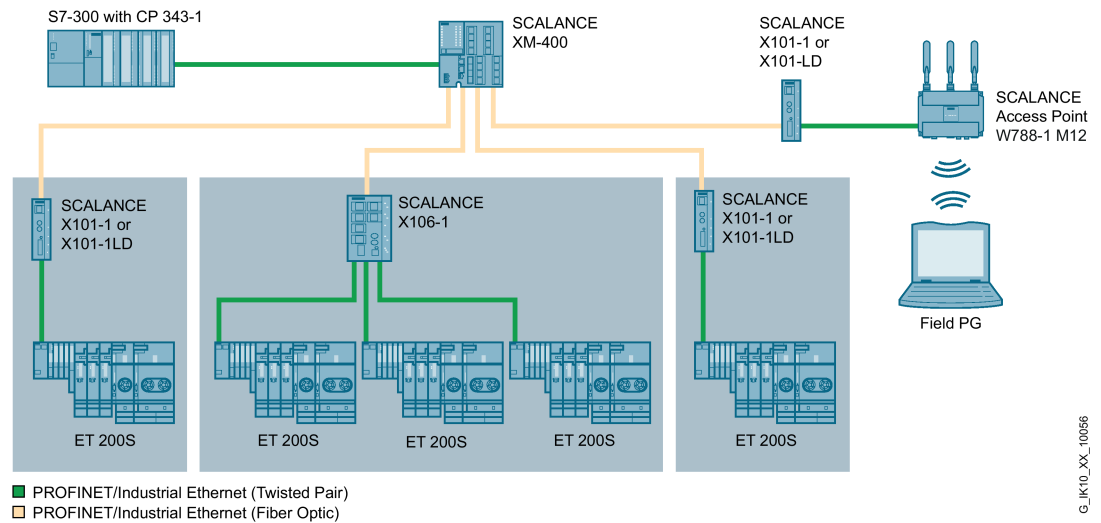


Figure 2-2 Star topology based on the example of Industrial Ethernet with a gateway to Industrial Wireless LAN

- The use of a switch optimizes data throughput in the network. Messages are transferred only on the star segments between sender and recipient and the segments of the other nodes remain unaffected by them. If a node fails, the communication between the other network nodes remains intact.
- Compared with ring or linear bus structures, however, the investment in cabling increases considerably due to the long distances back to the star center.

Typical use cases for star networks are switching cubicles, individual machines or manufacturing cells.

Examples of simple star structures

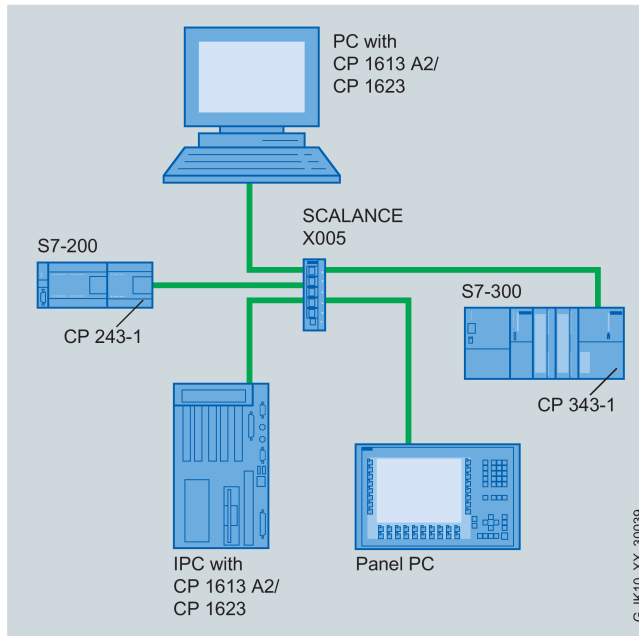


Figure 2-3 Star structure with SCALANCE X005

The number and technology of the connections to the end nodes (electrical/optical) depends on the number of relevant ports on the switch: In the example above, the SCALANCE X005 can support five 10/100 Mbps cables with RJ-45 connectors and no fiber-optic connections.

With an FC TP standard cable, the end nodes can be located up to 100 m from the switch.

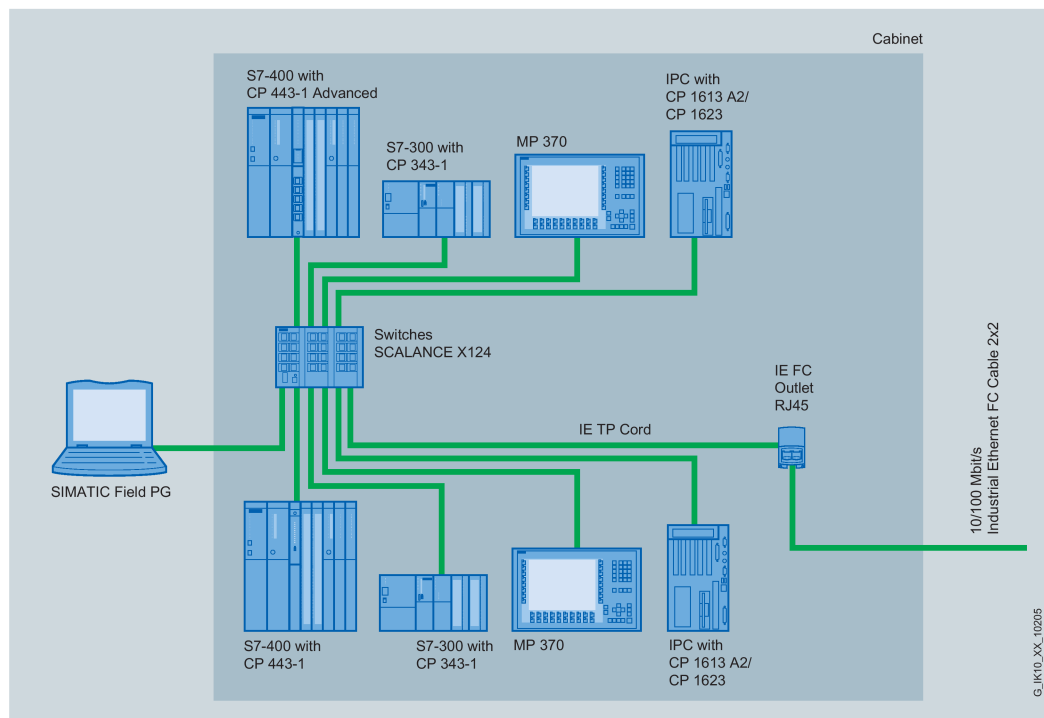


Figure 2-4 Star network structure with SCALANCE X124

More complex network structures can be set up by using switches with a higher number of ports. (In the example above, a SCALANCE X124 with 24 electrical ports.) In terms of the numbers of nodes and the physical span of the network, this is practicable only up to a certain limit.

If extensive networks need to be configured, the use of several switches and the resulting sub-networks makes sense.

See also

SCALANCE X005 (Page 120)

2.1.4 Ring structure

"Ring"



If the ends of a bus are connected via an additional connection, this results in a ring structure. The switches connected together in a ring do not need to be interconnected only with FO cables or only electrical cables. A mixed electrical-optical ring is also permitted.

A special redundancy mechanism ensures that the ring structure remains a logical bus in normal situations and prevents frames from circulating. If a section of the ring fails, the mechanism quickly makes a substitute path available in the ring: The message now travels the long way round via the intact network section instead of over the direct interrupted path and reaches its recipient via this detour. The network does not break down into two segments.

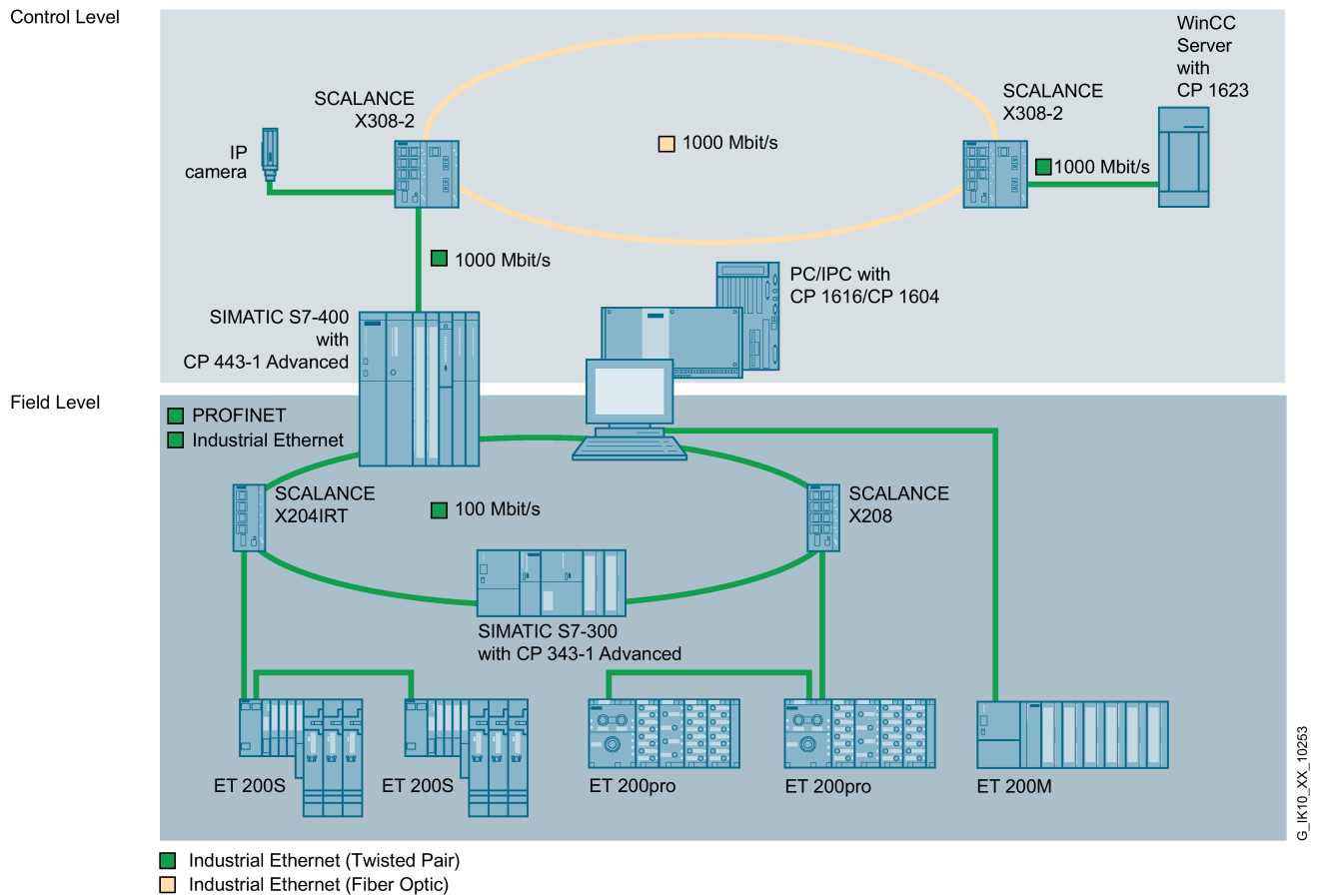


Figure 2-5 Ring topology based on the example of Industrial Ethernet with glass fiber-optic cables and twisted pair cable

- The effects of a network component being disrupted are restricted to the failed component and to the end devices connected to it. If a ring section is interrupted, for example by a cable break, communication continues without any disruption.

The reconfiguration time is faster here than in the office world and meets the requirements of the automation world.

Example: Structure of a redundant network with SCALANCE X switches

With the aid of a redundancy manager (RM), the two ends of a bus can be closed to form a redundant ring. All the media converters SCALANCE X100/200/300/400 and X500 devices can be used in this ring. The role of the RM can be handled by the SCALANCE X200/X300/400 and X500 devices.

The RM monitors the line connected to it, if there is an interruption, it closes the ring and restores a functioning bus configuration. A maximum of 50 of the SCALANCE X devices mentioned above are permitted in an optical ring. Here, a reconfiguration time of less than 0.3 seconds is achieved. The RM mode on the SCALANCE X devices is configured in the software. The maximum length of the fiber-optic cable between two devices is 3000 m for multimode fiber and 200 km for single mode fiber. This means that a maximum of 150 km (multimode) can be achieved for the entire optical ring consisting of 50 switches.

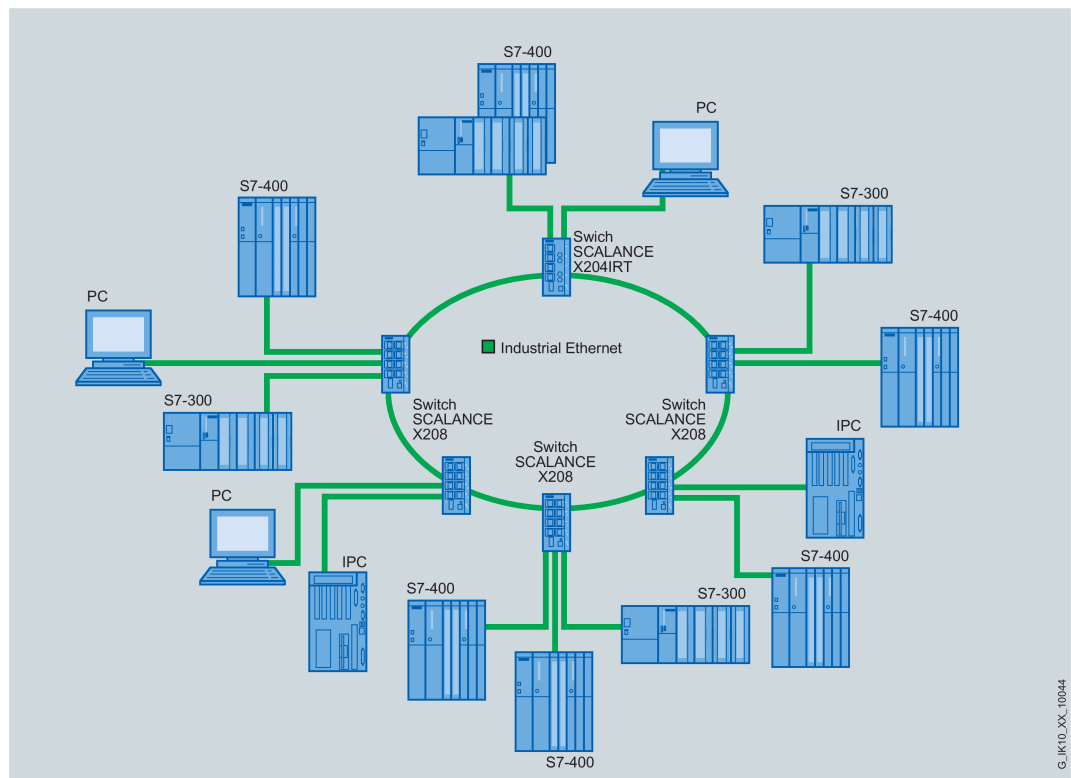


Figure 2-6 SCALANCE X: Configuration with high-speed redundancy in the electrical ring

See also

Network topologies (Page 61)

SCALANCE X500 (Page 149)

2.1.5 Redundant linking of network segments with electrical and FO components

General

SCALANCE X switches support not only ring redundancy within a ring but also redundant linking of several rings or open network segments (linear bus). In the redundant link, two rings are connected together over two Ethernet connections. This is achieved by configuring a master/slave device pair in one ring so that the devices monitor each other and, in the event of a fault, redirect the data traffic from the normally used master Ethernet connection to the substitute (slave) Ethernet connection.

Standby redundancy

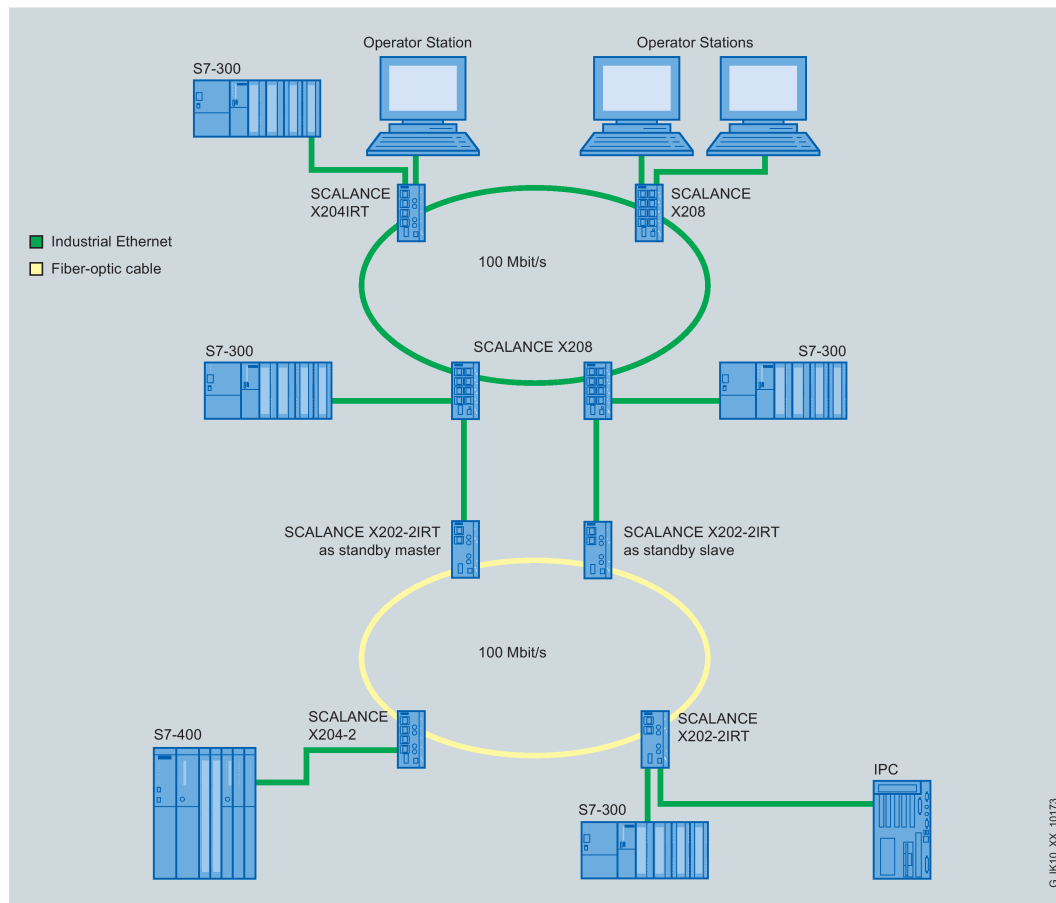


Figure 2-7 Example of redundant linking of two SCALANCE X-200 IRT rings

For a redundant link as shown in the figure, two devices must be configured as standby redundancy switches within a network segment. Here, network segments are rings with a redundancy manager (RM, in the example, the SCALANCE X202-2IRT switches). Instead of rings, network segments might also be linear.

The two X202 devices connected in the configuration exchange data frames with each other to synchronize their operating statuses (one device is master and the other slave). If there are no problems, only the link from the master to the other network segment is active. If this link fails (for example due to a link-down or a device failure), the slave activates its link as long as the problem persists.

See also

SCALANCE X200/X200 IRT (Page 129)

SCALANCE X300 (Page 135)

SCALANCE XM-400 (Page 143)

2.1.6 VLAN

Virtual Local Area Network

VLANs are virtual network segments in a physical network that are assigned to the nodes during configuration. In contrast to the physical network, a VLAN is not spatially restricted. This allows nodes to be put together in logical groups according to their function (VLAN groups). VLANs can be set up without modifying the physical network.

SCALANCE X and SCALANCE W support port-based VLAN. For the parameter assignment of the VLANs, a VLAN ID is assigned to the individual ports of a SCALANCE device. Multicast and broadcast frames are possible only within the boundaries created by the logical network structure; in other words, between ports with the same VLAN ID.

This segmentation not only reduces network load because broadcasts can be limited to a practical number of end systems. VLANs also increase the security of a network since no node can listen in any longer on the data traffic of other nodes unless they are a member of this VLAN.

To identify which packet belongs to which VLAN, the Ethernet frame is expanded by 4 bytes (VLAN tagging). This expansion includes not only the VLAN ID but also priority information.

2.2 Media redundancy

2.2.1 Options of media redundancy

There are various options available to increase the network availability of an Industrial Ethernet network with optical or electrical linear bus topologies:

- Mesh networks
- Parallel connection of transmission paths
- Closing a linear bus topology to form a ring topology

2.2.2 Media redundancy in ring topologies

Structure of a ring topology

Nodes in a ring topology can be external switches and/or the integrated switches of communications modules.

To set up a ring topology with media redundancy, you bring together the two free ends of a linear bus topology in one device. Closing the linear bus topology to form a ring is achieved with two ports (ring ports) of a device in the ring. This device is the redundancy manager. All other devices in the ring are redundancy clients.

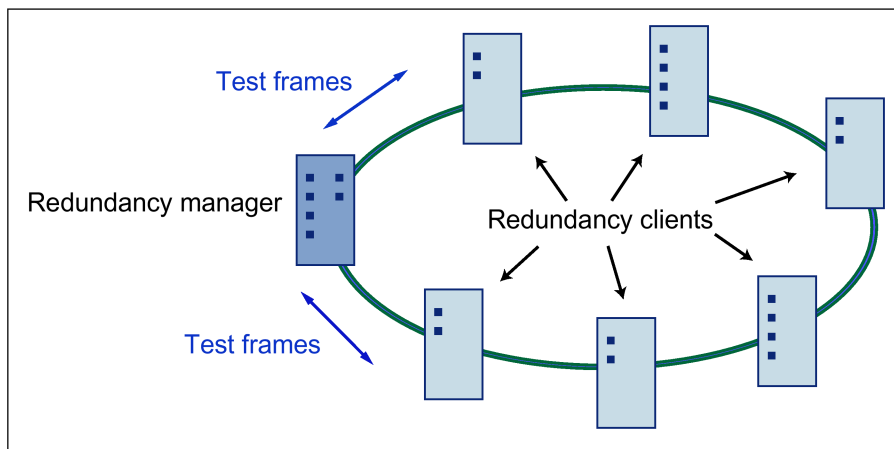


Figure 2-8 Devices in a ring topology with media redundancy

The two ring ports of a device are the ports that establish the connection to the two neighboring devices in the ring topology. The ring ports are selected and set in the configuration of the relevant device. In STEP 7 and on the S7 Ethernet CP modules themselves, the ring ports are indicated by an "R" after the port number.

Note

Before physically closing the ring, download the configuration of your STEP 7 project to the individual devices.

How media redundancy works in a ring topology

When using media redundancy, the data paths between the individual devices are reconfigured if the ring is interrupted at one point. Following reconfiguration of the topology, the devices can once again be reached in the resulting new topology.

In the redundancy manager, the 2 ring ports are disconnected from each other if the network is uninterrupted. This prevents circulating data frames. In terms of data transmission, the ring topology is a linear bus topology. The redundancy manager monitors the ring topology. It does this by sending test frames both from ring port 1 and ring port 2. The test frames run round the ring in both directions until they arrive at the other ring port of the redundancy manager.

An interruption of the ring can be caused by loss of the connection between two devices or by failure of a device in the ring.

If the test frames of the redundancy manager no longer arrive at the other ring port because of an interruption in the ring, the redundancy manager connects its two ring ports. This substitute path once again restores a functioning connection between all remaining devices in the form of a linear bus topology.

As soon as the interruption is eliminated, the original transmission paths are established again, the two ring ports of the redundancy manager are disconnected and the redundancy clients informed of the change. The redundancy clients then use the new paths to the other devices.

The time between the ring interruption and restoration of a functional linear topology is known as the reconfiguration time.

If the redundancy manager fails, the ring becomes a functional linear bus.

Media redundancy methods

The following media redundancy methods are supported by SIMATIC NET products:

- HRP (High Speed Redundancy Protocol)

Reconfiguration time: 0.3 seconds

- MRP (Media Redundancy Protocol)

Reconfiguration time: 0.2 seconds

The mechanisms of these methods are similar. HRP and MRP cannot be used in the ring at the same time.

2.2.3 MRP

The "MRP" method conforms to the Media Redundancy Protocol (MRP) specified in the following standard:

IEC 62439-2 Edition 1.0 (2010-02) Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

The reconfiguration time after an interruption of the ring is a maximum of 0.2 seconds.

Requirements

Requirements for problem-free operation with the MRP media redundancy protocol are as follows:

- MRP is supported in ring topologies with up to 50 devices.
Except in PROFINET IO systems, topologies with up to 100 SCALANCE X-200 and SCALANCE X-300 IE switches were tested successfully.
Exceeding this number of devices can lead to a loss of data traffic.
- The ring in which you want to use MRP may only consist of devices that support this function.
These include, for example, some of the Industrial Ethernet SCALANCE X switches, some of the communications processors (CPs) for SIMATIC S7 and PG/PC or non-Siemens devices that support this function.
- All devices must be interconnected via their ring ports.
Multimode connections up to 3 km and single mode connections up to 26 km between two SCALANCE X IE switches are possible. At greater distances, the specified reconfiguration time may be longer.
- "MRP" must be activated on all devices in the ring (see section "Auto-Hotspot").
- The connection settings (transmission medium / duplex) must be set to full duplex and at least 100 Mbps for all ring ports. Otherwise there may be a loss of data traffic.
 - STEP 7: Set all the ports involved in the ring to "Automatic settings" in the "Options" tab of the properties dialog.
 - WBM: If you configure with Web Based Management, the ring ports are set automatically to autonegotiation.

Topology

The following schematic shows a possible topology for devices in a ring with MRP.

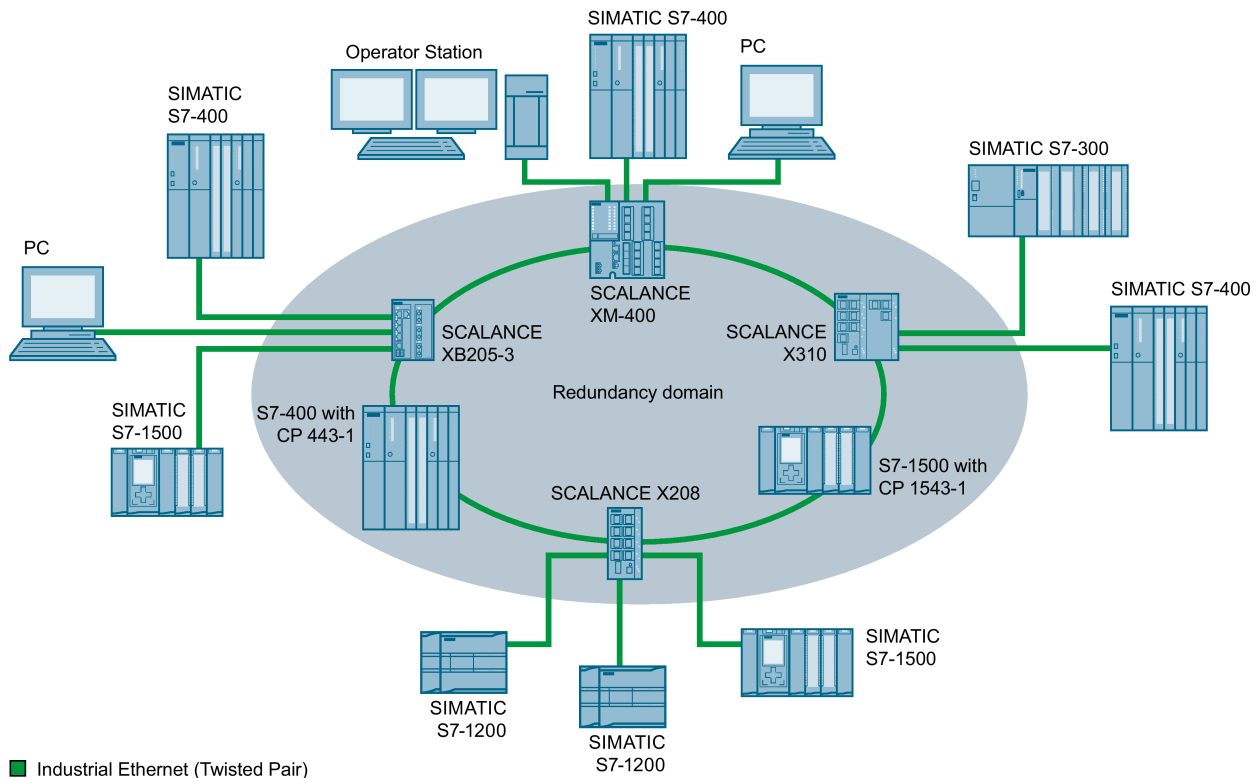


Figure 2-9 Example of a ring topology with the MRP media redundancy protocol

The following rules apply to a ring topology with media redundancy using MRP:

- All the devices connected within the ring topology are members of the same redundancy domain.
- One device in the ring is acting as redundancy manager.
- All other devices in the ring are redundancy clients.

Non MRP-compliant devices can be connected to the ring via a SCALANCE X switch or via a PC with a CP 1616.

2.2.4 MRPD

MRPD - Media Redundancy with Planned Duplication

The MRPD procedure is specified in IEC 61158 Parts 5 and 6 type 10 "PROFINET". It allows bumpless redundant linking of devices.

The cyclic IRT frames are duplicated and the PROFINET devices connected to the ring send their data in both directions. The devices receive this data at both ring ports and this reduces the reconfiguration time of the ring. As with MRP, a redundancy manager prevents circulating data frames.

Requirements

- Devices with ERTEC hardware support.
 - SCALANCE X-200IRT as of firmware version 5.0
- STEP 7 as of version V5.5 SP1

2.2.5 HRP

HRP - High Speed Redundancy Protocol

HRP is the name of a redundancy method for networks with a ring topology. The switches are interconnected via ring ports. One of the switches is configured as the redundancy manager. The other switches are redundancy clients. Using test frames, the redundancy manager checks the ring to make sure it is not interrupted. The redundancy manager sends test frames via both ring ports and checks that they are received at the other ring port. The redundancy clients forward the test frames.

If the test frames of the redundancy manager no longer arrive at the other ring port of the redundancy manager due to an interruption, the redundancy manager switches through its two ring ports and informs the redundancy clients of the change immediately.

Standby redundancy

Standby redundancy is a method with which several rings each of which is protected by HRP can be linked together redundantly. In the ring, a master/slave device pair is configured and these monitor each other via their ring ports. If a fault occurs, the data traffic is redirected from one Ethernet connection (standby port of the master or standby server) to another Ethernet connection (standby port of the slave).

Requirements

- HRP is supported in ring topologies with up to 50 devices. Exceeding this number of devices can lead to a loss of data traffic.
- The following devices support HRP:
 - SCALANCE X500
 - SCALANCE X400
 - SCALANCE X300
 - SCALANCE X200
- All devices must be interconnected via their ring ports.

2.2.6 RNA

Redundant Network Access (RNA)

In Siemens Industry, Redundant Network Access (RNA) stands for devices and software that support the redundancy protocol "Parallel Redundancy Protocol" (PRP). RNA allows the connection of devices to redundant Ethernet network structures.

The product names of the RNA devices end with "RNA".

Some devices of the SCALANCE X-200RNA product line also support the redundancy protocol "High-availability Seamless Redundancy" (HSR).

2.2.7 PRP

Parallel Redundancy Protocol (PRP)

The Parallel Redundancy Protocol (PRP) is a redundancy protocol for Ethernet networks. It is specified in IEC 62439-3.

The areas of application of PRP are distributed applications with high reliability demands that depend on the high availability of the network. Compared with classic fault-tolerant networks, bumpless path redundancy is possible with PRP.

PRP has the advantage that it uses parallel, separate networks made up of standard network components. End devices that use this method are connected to both networks via two ports of an interface of the device or via a SCALANCE X-200RNA or a RUGGEDCOM RS950G. This means that data of the end device can be transferred at the same time via both networks. If a transmission path is interrupted, the data reaches the communications partner via the second parallel path.

If a network is interrupted, communication can be maintained with PRP via the second network without any interruption. Reconfiguration times required with the other redundancy protocols (e.g. MRP) do not therefore apply.

An end device with PRP capability can be connected to redundant networks by using the PRP protocol. An end device that does not have PRP capability can be connected to a redundant network via a SCALANCE X-200RNA or RUGGEDCOM RS950G that does have PRP capability. This means that PRP can also be used by end devices without PRP capability.

Devices with PRP capability are located in two independent networks with the same MAC and IP address.

Communication with PRP

PRP is only possible when two end devices are connected via two independent networks (LAN A and LAN B).

Each end device is represented in both networks LAN A and LAN B with the same MAC and IP address.

PRP communication is handled using the following mechanisms:

- **Send**

An end device with PRP capability duplicates each frame to be sent on the PRP interface. The two duplicates are sent via the 2 ports of the PRP interface via the two separate networks LAN A and LAN B to the communications partner.

If the end device does not have PRP capability, the frame to be sent is duplicated by an X-200RNA to which the end device is connected and sent via LAN A and LAN B to the communications partner.

- **Received**

The two duplicates are received by an end device with PRP capability via LAN A and LAN B on the two ports of the PRP interface.

If the end device does not have PRP capability, the receiving end device must be preceded by an X-200RNA. The X-200RNA forwards the first frame to arrive to the addressee. The second frame is discarded ((N-1) redundancy).

Connecting up and cabling

Each frame duplicate sent using the PRP mechanisms is given in identifier that specifies whether it is sent via LAN A or LAN B.

Note

Cabling

Make sure that all the PRP ports of the nodes and the SCALANCE X204RNA / RUGGEDCOM RS950G on LAN A and LAN B are connected correctly. A frame with the identifier "LAN A" must be received at the corresponding port.

The PRP ports of SIMATIC NET devices have the following identifiers. The CP ports are the ports of the interface with PRP capability.

- Ports for connection to LAN A
 - CPs: X2/P1
 - SCALANCE X204RNA: PRP A
- Ports for connection to LAN B
 - CPs: X2/P2
 - SCALANCE X204RNA: PRP B

2.2.8 STP / RSTP / MSTP

Spanning Tree Protocol (STP)

STP (IEEE 802.1D standard) is the method with which loops are prevented in redundant network structures.

With this method, it is not end devices that know the path from the sender or recipient, but rather the switches. The switches continuously exchange configuration frames with each other known as BPDUs (Bridge Protocol Data Unit). Due to the MAC addresses of the packets passing through, the switches get to know the topology of the network independently. The network is considered to be a tree.

Sequence

After initialization of the switches, a root bridge is selected. Each switch has an ID that it passes on to the group. The switch with the lowest bridge ID becomes the root bridge.

All other paths are decided by this root bridge. The other switches select one of their ports as a root port in the direction of the root bridge. This selection is also made using BPDUs that the root bridge sends to the switches. The port of switch that receives the BPDU of the root bridge first adopts the status of root port.

The designated ports are selected from the remaining ports connected to another switch. This is also done by sending BPDUs. This time the switches send frames to the connected partners. The port via which the frame reaches the recipient quickest becomes the designated port.

The other port is deactivated. If there is a disruption or device failure, the network needs to be reconfigured. The devices start to negotiate new paths only when the interruption occurs. This can take up to 30 seconds.

Rapid Spanning Tree Protocol (RSTP)

RSTP (IEEE 802.1D-2004 standard) is a further development of STP. RSTP differs from STP essentially in that the devices are already collecting information about alternative routes during normal operation and do not need to gather this information after a disruption has occurred. This allows the reconfiguration time for an RSTP-controlled network to be reduced to less than 1 second.

This was achieved by the following functions:

- Edge ports

A port that is defined as an edge port is activated immediately after connection establishment. If a BPDU is received at an edge port, the port loses its role as edge port and takes part in RSTP again. If no further BPDU is received after a certain time has elapsed (3 x hello time), the port returns to the edge port status.

- Point-to-point (direct communication between two neighboring devices)

By directly linking the devices, a status change (reconfiguration of the ports) can be made without any delays.

- Alternative port (substitute for the root port)
A substitute for the root port is configured. If the connection to the root bridge is lost, the device can establish a connection over the alternate port without any delay due to reconfiguration.
- Reaction to events
A Rapid Spanning Tree reacts to events, such as a connection abort, without delay. There is no waiting for timers as in spanning tree.
- Counter for maximum number of bridge hops
The number of bridge hops a package is allowed to make before it automatically becomes invalid.

In principle, therefore with rapid spanning tree, alternatives for many parameters are preconfigured and certain properties of the network structure taken into account to reduce the reconfiguration time.

Multiple Spanning Tree Protocol (MSTP)

MSTP is a further development of RSTP. MSTP is defined in the IEEE 802.1s standard, subsequently IEEE 802.1Q.

Among other things, it provides the option of operating several RSTP instances or VLAN groups within different virtual networks (VLAN - Virtual Local Area Network) so that; for example; paths that would block the simple Rapid Spanning Tree Protocol for data traffic globally can be available within individual VLANs.

2.2.9 Link aggregation

Link aggregation

With link aggregation, several parallel physical connections with the same transmission speed are grouped together to form a logical connection with a higher transmission speed. This method based on IEEE 802.3ad is also known as port trunking or channel bundling.

Link aggregation works only with full duplex connections with the same transmission speed in point-to-point mode. This achieves multiplication of the bandwidth or transmission speed. If part of the connection fails, the data traffic is handled via the remaining parts of the connection.

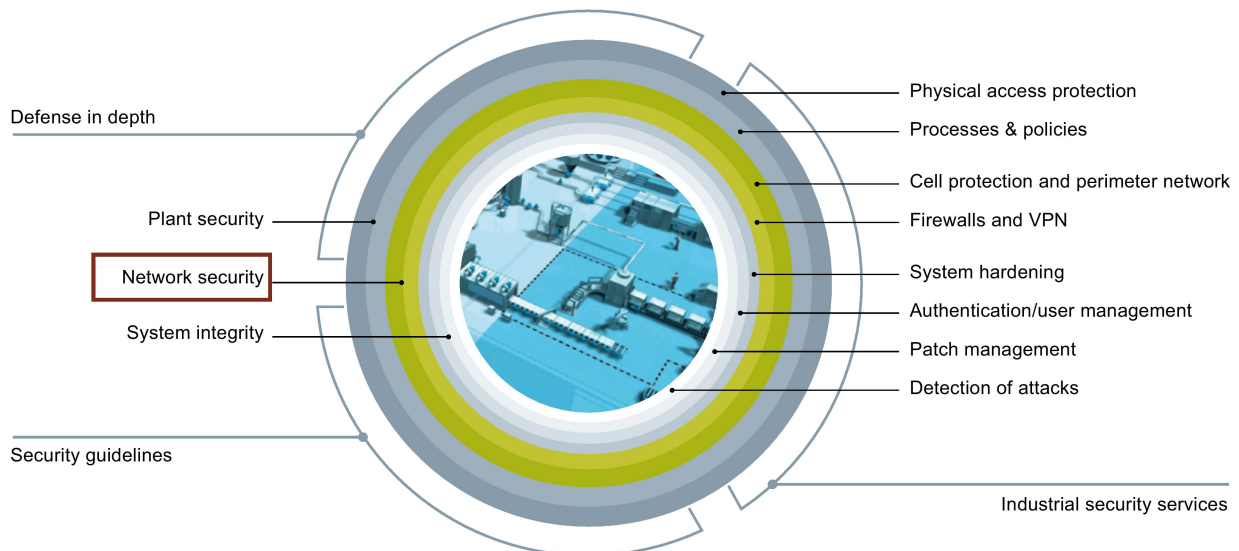
To control and monitor, the Link Aggregation Control Layer (LACL) and the Link Aggregation Control Protocol (LACP) are used.

2.3 Network security

2.3.1 SIMATIC NET products for network security

Achieving information security as a complex task

The use of the Internet is also unavoidable for industrial companies. As a result, however, comprehensive and reliable protection against unauthorized access is necessary because IT systems are implemented on the basis of diverse networking. Information security in an industrial environment is not restricted to technological aspects but also includes administrative measures such as a suitable user management or access restrictions as shown in the following graphic.



Products

SIMATIC NET provides the user with a complete range of high-performance hardware and software components to protect individual networks or an entire network.

- Data manipulation, i.e. violation of the integrity
- Espionage
- Forged addressing (IP spoofing), i.e. violation of the authenticity
- Overload (denial of service) as an accidental or deliberate disturbance of the target system.

2.3 Network security

When remote access using GPRS and UMTS are part of the infrastructure, these can be protected.

The following graphic shows an overview of the available products.

	SCALANCE S family	SCALANCE M family	CP 343-1 Adv CP 443-1 Adv	S7-1200 CPU ¹⁾ S7-1500 CPU	CP 1243-1 ¹⁾ CP 1543-1 CP 1242-7 CP 1243-7 LTE	CP 1628	SOFTNET Security client
							
Configurable copy protection				•			
Access protection (Authentication)				•			
Expanded access protection (firewall)	•	•	•		•	•	
Virtual Private Network with IPsec	•	•	•		•	•	•
Manipulation protection (communication, configuration)	•	•	•	•	•	•	•

• true

1) as of CPU firmware V4.0
as of STEPProfessional V13 (TIA Portal)

G_K10_XX_10347

Security functions

The SIMATIC NET products listed in the table have proven security functions. Which of the security mechanisms are supported by the individual devices and details of the configuration limits can be found in the relevant product documentation.

- IP firewall with stateful packet inspection (layer 3 and 4)
- Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)
- Bandwidth limitation
- Global firewall rules
- Communication made secure by IPsec tunnels (not with SCALANCE S)
- Logging (storage of events in log files)
- NTP (secure) for secure time-of-day synchronization and transmission
- SNMPv3 for secure transmission of network analysis information safe from eavesdropping

SCALANCE S

As a firewall the devices of the SCALANCE S series protect the secured devices against access from the outside. In addition to the security functions described in the previous section, the SCALANCE S devices have a DHCP server and a NAT/NAPT router. The following devices are available:

- SCALANCE S602
- SCALANCE S612
- SCALANCE S623 (DMZ port, router and firewall redundancy as well as a standby link are possible)
- SCALANCE S615 (Up to five variable security zones with a port-based VLAN)
- SCALANCE S627-2M (As S623, two additional slots for media modules)

SCALANCE M

The devices of the SCALANCE M have almost all the security functions of SCALANCE S. The following devices are available:

- SCALANCE M812-1 (ADSL router)
- SCALANCE M816-1 (ADSL router, 4-port switch)
- SCALANCE M826-2 (SHDSL router, 4-port switch)
- SCALANCE M874-3 (HSPA+, 2-port switch)
- SCALANCE M876-3 (HSPA+/EV-DO, 4-port switch)
- SCALANCE M876-4 (LTE, 4-port switch)

Modules for S7 systems

The following modules for SIMATIC S7 systems have security properties:

- CP 1243-1
- CP 1543-1
- CP 343-1 advanced
- CP 443-1 Advanced

Modules for PCs

With the module CP 1628, it is also possible to access networks or automation cells protected by security modules from a PC.

Security Configuration Tool

This program is integrated in STEP 7 but can be called up independent of STEP 7. It allows the configuration of the security mechanisms for a device. In standard mode there are many parameter defaults which simplifies the fast creation of a project. In advanced mode individual settings are possible for many parameters so that complex use scenarios can also be created.

Among other things, with the Security Configuration Tool the firewall of the device is configured that restricts the data traffic according to the specified rules to prevent unauthorized access. The data of the security configuration is stored in an SCT project that can also be used by the Softnet security client.

Softnet security client

The Softnet security client allows secure remote access to security modules and the programmable controllers behind via a public network. The function of the program is based on an IPsec tunnel connection in the VPN (Virtual Private Network). It uses the configuration created by the Security Configuration Tool.

2.3.2 Firewalls

"Gatekeeper" function

Put simply, a firewall is a device or a software application inserted between the network and the outside world as a "gatekeeper" to protect the network. The firewall represents the only access to the local area network from outside and the entire data traffic crossing the boundaries of the network is directed via the firewall. This means that the firewall can block unwanted and potentially dangerous access from the outside. Various techniques are available.

Packet filter

A packet filter inspects data packets entering or leaving the network, their sender and receiver addresses and the "port", or service, to which the data packet will be transferred. Such services might be E-mail, file transfer with FTP, database access, SSH for encrypted transfer etc.

Filter rules stored in the firewall now block the access to certain addresses or certain services. Firewalls can implement complex filter rules in which, for example, service "A" is available only for IP addresses "B" and "C" but is not allowed for other communications partners.

"Stateful Inspection"

"Stateful Inspection" goes a step further than the packet filter and takes into consideration the "context" within the communication in addition to the addresses and ports.

In concrete terms, this means, for example, that Web pages sent by an external server to an internal computer can only pass through the firewall if the internal computer has actually requested this page.

Such techniques are, for example, relevant for preventing "Denial of Service" attacks (DoS) in which an external intruder sends queries to the computer under attack from numerous computers at the same time in the hope of overloading and paralyzing the network. Since, however, the stateful inspection detects these illegitimate queries at the boundary of the local area network, local traffic continues unaffected by the DoS attacks.

"Network Address Translation" (NAT)

"Network Address Translation" ("NAT") is a function with which a router replaces the addresses of the local nodes involved in data traffic with its own IP address whenever the traffic goes beyond the network boundaries. Incoming replies are only assigned to the actual addressees with their IP addresses after passing the firewall.

This mechanism can be used for ergonomic reasons since to the outside only one single IP address is required for any number of local nodes.

It does, however, also provide a certain protection from attacks since only one single address is visible to the outside namely that of the firewall. A "naive" attack would always be aimed at the firewall directly and not at the local computers being protected behind it.

"Network Address Port Translation" (NAPT)

Compared with NAT, NAPT goes one step further. With NAPT, in addition to the IP addresses, the ports of the local nodes are also replaced. Incoming replies are then assigned back to the corresponding IP addresses and ports of the local nodes.

"Personal firewalls"

For professional applications, the firewalls normally used are separate devices. The alternative to these devices are "personal firewalls" in the form of software running on the target computers themselves.

Personal firewalls cannot, however, provide the same security as dedicated devices. Errors in the operating system or badly programmed or configured personal firewalls allow an attacker to avoid the "gatekeeper" filter function and to attack the target computer or target network despite the firewall.

2.3.3 "Virtual Private Networks" (VPNs)

The function of Virtual Private Networks

A VPN means that a public network is used to transfer private data by "embedding" the private communication in the traffic of the public network.

The nodes of the VPN have the impression that they are connected directly to each other. They are not aware of the intermediate steps inserted in the transmission via the public

network. For this reason, the mechanisms are known as "tunneling" through the public network. Using VPNs, for example, two subnets at a considerable physical distance from each other can be connected so that the users can address them as one unit.

Security of VPNs

The term "private" relates primarily to the use of VPNs and not to the confidentiality of the data: VPNs are not automatically secure since the data traffic is not encrypted from the very beginning. If, however, suitable encryption techniques are used, communication via the VPN is practically safe from eavesdropping.

See also

Encryption and data security (Page 50)

2.3.4 Cell protection concept

Basics

With the cell protection concept, a plant network is divided into individual protected automation cells to ensure security for the automation systems; within these cells, all the devices can communicate securely with each other. In the sense of the cell protection concept, production units, for example, are worthy of protecting.

The following graphic illustrates this. A production cell is protected from unauthorized access from the remaining enterprise network by a SCALANCE S firewall.

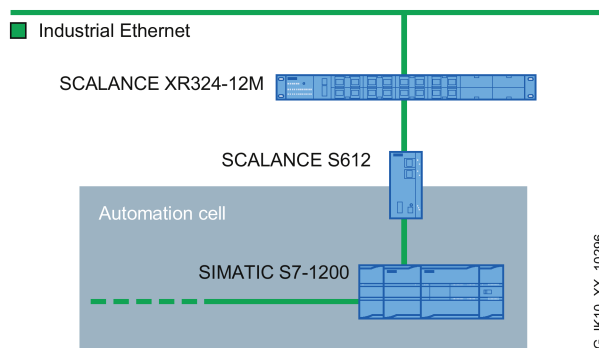


Figure 2-10 Cell protection concept

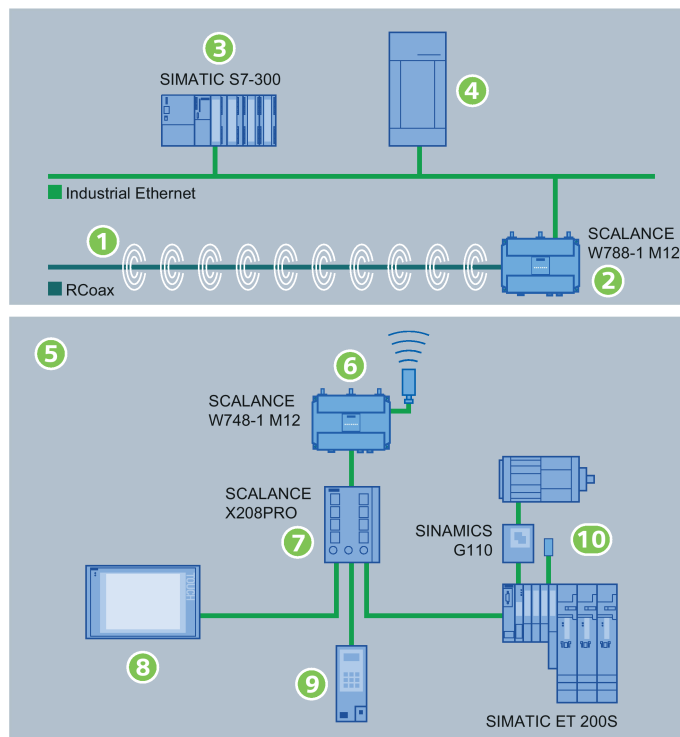
Examples of applications

3.1 Optimization of a power screwdriver control

Task

Handheld compressed air screwdrivers are used in the final assembly of motor vehicles and they can be supplied via mobile stations on overhead monorails. These units need to be replaced by new, motor-driven screwdriver stations and the customer would like to do away with the previously necessary sliding contacts that were always subject to wear and tear.

Solution



The new solution is based on Industrial Wireless LAN. To allow wireless data communication, an RCoax cable ① is laid along the path of the screwdriver stations. The RCoax cable is connected to the antenna output of a SCALANCE W788-1 M12 ② access point. This means that there is a defined RF field available around the RCoax cable. Via the Ethernet interface of the access point, there is a connection to the plant controller ③ and the server of the assembly line ④.

- ⑤ The communications partner on the screwdriver stations is a SCALANCE W748-1 M12 ⑥ client module.

3.1 Optimization of a power screwdriver control

- ⑦ The data exchange with all components of the mobile station is handled by a SCALANCE X208PRO switch. The station is controlled via a panel PC ⑧ and the screwdriver controller ⑨.
- ⑩ The new screwdriver stations are moved by a geared motor connected via the distributed I/O.

Benefits

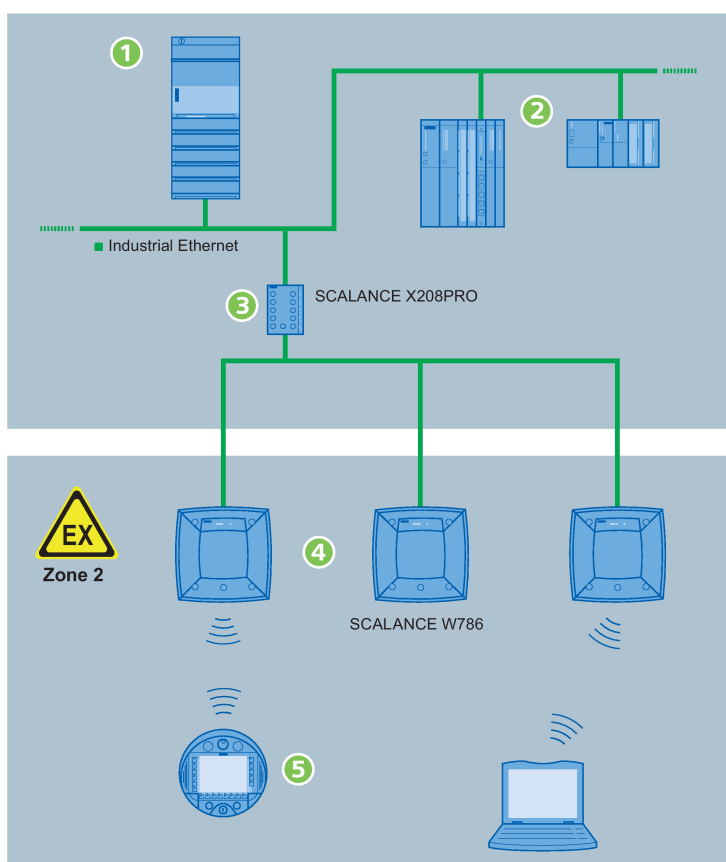
- Low investment costs thanks to fewer screwdriver stations.
- Reduction of maintenance costs and downtimes with reliable wireless and therefore data transmission to mobile communications partners free from wear.
- Shorter downtimes if a fault occurs thanks to the C-PLUG (configuration plug) in the SCALANCE devices. Devices can be replaced without a programming device and without specialist personnel.
- Higher productivity and process reliability because all data of the plant controller (for example workpiece IDs, screwdriver data and assembly information) is also available directly on the screwdriver stations. Other applications for quality assurance are also easy to integrate.
- The SCALANCE wireless devices used W788-1 M12 or W748-1 M12 has a robust metal housing with degree of protection IP65 and are designed specially for industrial use.

3.2 Process automation in hazardous areas

Task

The aim was to allow mobile access to the process data of the entire plant in a hazardous area (production of polyoxymethylene thermoplastic). Extremely complicated constraints had to be taken into account when interfacing to the existing PCS 7 plant. The wireless network had to work in an industrial building made of reinforced concrete with unspecified fittings over seven floors. Added to this, were the chemical load and the high temperature differences resulting from the production process.

Solution



① All the SIMATIC S7-400 and SIMATIC S7-300 controllers ② involved in the production process are connected to the SIMATIC PCS 7 server via Industrial Ethernet.

③ A SCALANCE X208PRO controls data exchange with the access points.

④ In the hazardous area, several SCALANCE W786 access points with integrated antennas ensure stable illumination of the RF field. This device type was selected because it meets all the requirements reliably: The degree of protection IP65 in conjunction with an extended temperature range of -40 to +60 °C and the high mechanical stability providing resistance to vibration and shock ensure high availability of the entire system.

Note the information on the use of modules in hazardous area zone 2. You will find further information on the Internet at:

(<https://support.industry.siemens.com/cs/products?dtp=Certificate&ci=529&pnid=15247&lc=en-VW>)

⑤ With mobile operator stations, all the information relating to the entire plant can be called up anywhere and at any time.

Benefits

- A modular structure and scalability make any necessary expansions simpler.
- Price advantage because industrial components from SIMATIC NET meet users' requirements without them having to take any additional measures.
- Simple integration in the PCS 7 system and simple configuration of the SCALANCE components used thanks to Web-based management.

3.3 Automation of gantry cranes

Task

Two gantry cranes are used in a cold rolling mill to handle the steel coils. Fully automated and fail-safe control of these cranes is required because damage to the steel coils puts up costs considerably. The intention was to minimize maintenance effort and to reduce operating costs. The fail-safe monitoring of the 14 entrances and exits of the 16,000 m² storage area was also required.

Solution

The following graphic shows the components of the crane control ② and the interfacing of the production control system ① and the access monitoring for the open air storage area ③.

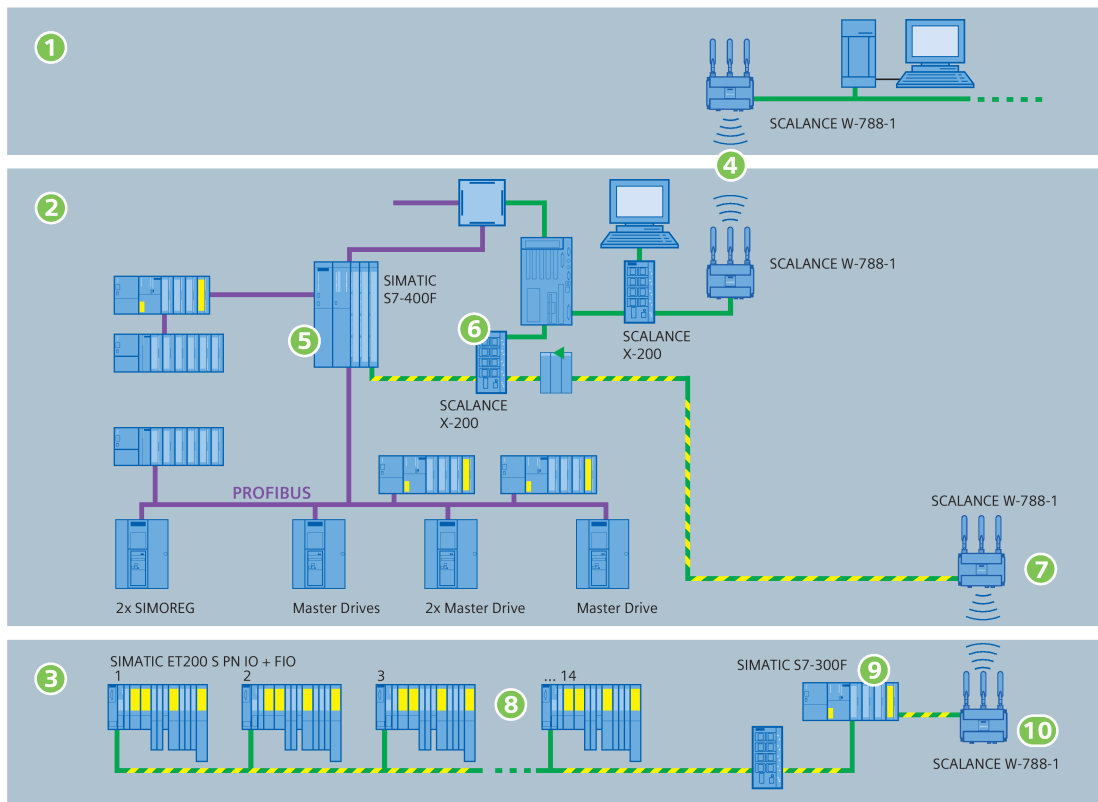


Figure 3-1 Schematic representation of the crane control

④ Data exchange between the production control system and the gantry crane is via two SCALANCE W788-1 access points. The use of wireless communication means that no trailing cables are required between the stationary and mobile station.

⑤ A SIMATIC S7-400F controls all crane movements (lifting, lowering, grasping, travel).

⑥ For the communication between the production control system and an access point ⑦, a SCALANCE X-200 is used. With this switch, security-oriented data for the access monitoring is exchanged via PROFI-safe.

⑧ All access is monitored by an ET 200S PN IO.

⑨ A SIMATIC S7-300F processes all the data of the access monitoring and can, when necessary, stop the movement of the crane via the connected access point ⑩.

Benefits

- By using Industrial Wireless LAN, no cables need to be laid for communication.
- SCALANCE W788-1 access points are designed to be suitable for industry and are therefore capable of withstanding the mechanical load caused by shock and vibration when used on the crane bridges. These devices are also available in degree of protection IP65 and can be used without problems in areas subject to dampness and spray water.
- Lower operating costs thanks to maintenance-free components.
- With PROFINET and the PROFI-safe profile, safety-oriented data can also be transferred with no additional effort.

3.4 Controlling material transportation with SCALANCE components

③ The data from the central controller is forwarded to the access points via Industrial Ethernet switches SCALANCE X414-3E and SCALANCE X204-2.

④ Industrial Wireless LAN is used for the wireless communication with the vehicles. In the production plant, several SCALANCE W774-1 access points ⑤ ensure a full-coverage IWLAN RF field. iPCF can be used with these devices. This minimizes the handover times when the vehicle moves from one wireless cell to another.

⑥ To allow this, each vehicle is equipped with a SCALANCE W734-1 client module. The control information received via wireless is forwarded via the Ethernet interface of the W734-1 client to a SIMATIC S7-300 controller. There, data traffic is handled by a CP 343-1 Lean ⑦.

Benefits

The selected solution has the following advantages for the users:

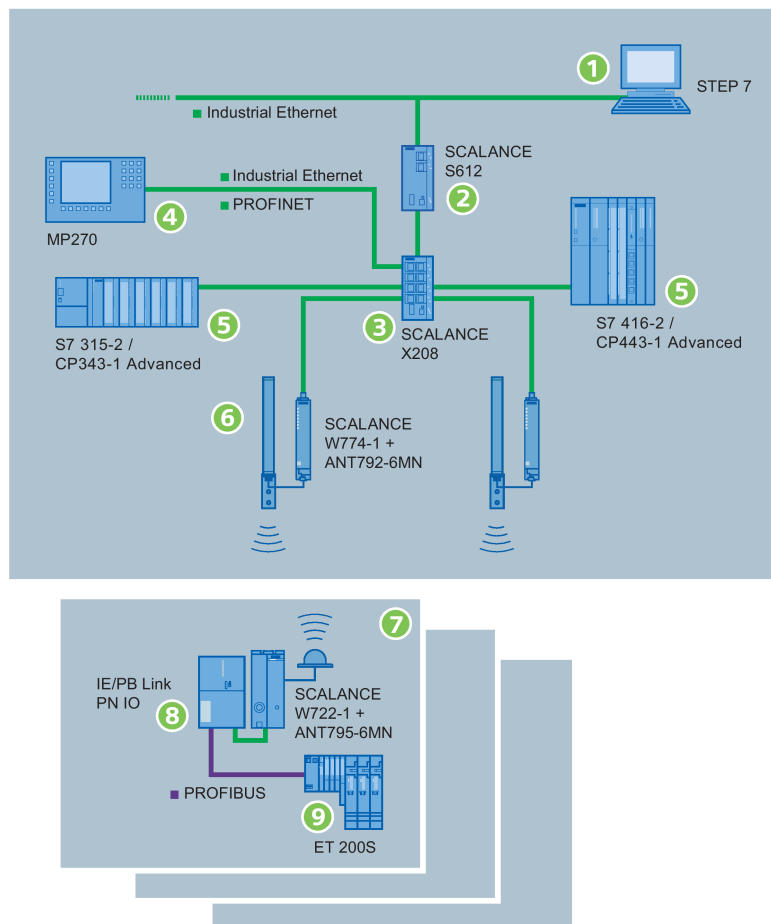
- Wireless LAN suitable for industry that meets all the requirements in terms of reliability and mechanical stability.
- Maximum availability even when changing wireless cells thanks to iPCF.
- Simple integration in a WinCC system.
- Maintenance-free and problem-free scalability.

3.5 Crane carriage control for a high-bay warehouse

Task

An existing SIMATIC S5 controller of a case picking high-bay warehouse system needs to be modernized. The customer also hopes to reduce plant costs by using modern and future-proof components.

Solution



- ① The controller of the high-bay warehouse can be reached via the factory network and it is also be configured via this path.
- ② To protect against unauthorized access, the entire crane system is protected by a SCALANCE S612.
- ③ Starting with a SCALANCE X208, the individual components form a star topology that includes not only four multi-panels MP270 as operator control and monitoring systems ④ but also the controllers for the crane carriage ⑤.

3.5 Crane carriage control for a high-bay warehouse

⑥ IWLAN was selected for the communication between the stationary parts of the system and the mobile crane carriage. This meant that the previously required cable festoons were no longer necessary. Broken cables and the associated maintenance effort would therefore no longer be a problem. Two SCALANCE W774-1 access points ensure reliable wireless coverage in the area in which the crane carriage moves.

⑦ Each crane carriage is equipped with a SCALANCE W722-1 and an IE/PB Link PN IO ⑧ that converts the received wireless control signals for PROFIBUS and forwards them to the ET 200S ⑨ on each crane carriage. In conjunction with absolute value encoders, this achieves precise movement and positioning of the crane carriage.

Benefits

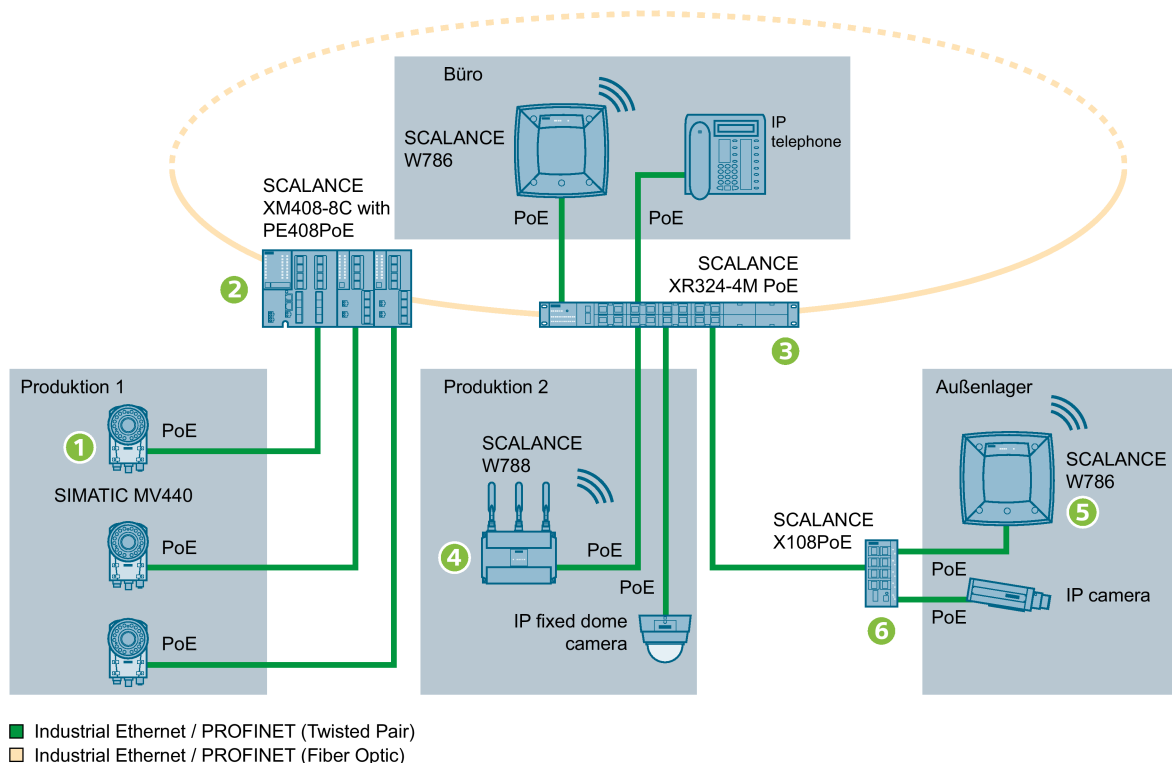
- Reliable and high-speed communication with PROFINET IO and Industrial Wireless LAN with iPCF.
- Protection of investment by using IE/PB Links. The existing PROFIBUS I/O can continue to be used unchanged.
- By integrating the absolute value encoders in the distributed ET 200S, additional cabling is unnecessary.
- Absence of maintenance and operational safety thanks to wireless transmission between the stationary part of the system and the crane carriage.
- Although remote access to the system via the factory network is possible, a SCALANCE S612 protects against unauthorized access.
- If requirements change, the system can be easily expanded or adapted.

3.6 Using Power over Ethernet

Task

In a plant in the food and beverages industry, two new production areas and an additional outside storage area need to be integrated in an existing IT infrastructure. Due to the large distances between the new parts of the company minimization of the cabling effort was sought.

Solution



G_IK10_XX_10378

This aim is to be met by the practically end-to-end use of components capable of PoE. In addition to this, access points allow access to the company network from any location. The starting point for connecting the new production areas and the storage area to the company network are two devices of the SCALANCE X series that provide an adequate number of Ethernet ports with PoE capability. The SIMATIC M440 readers ① of the first production area are connected to the company network via a SCALANCE XM408-8C ②. The basic device XM408-8C can be expanded by port extenders. When necessary, 24 ports are available if additional readers become necessary. With a suitable port module, connection to the existing fiber-optic cables can be achieved without problems.

The second production area with office and the outside storage area are supplied by a SCALANCE XR324-4M PoE ③. Both in production and in the storage area the requirements are the same: An access point will make access to the company network possible, for example to query logistics and job data. In addition to this and IP camera will monitor the entire area. In production, a SCALANCE W788 ④ will be used that is ideal for this use case

due to the high data transmission rate of up to 450 Mbps and its robust design. The SCALANCE W786 ⑤ installed in the outside storage area is resistant to UV radiation, condensation and salt spray and is therefore designed for use outdoors without additional measures. Only an Ethernet cable needs to be laid in the outside storage area, the access point and the camera are connected to the network via a SCALANCE X108PoE ⑥.

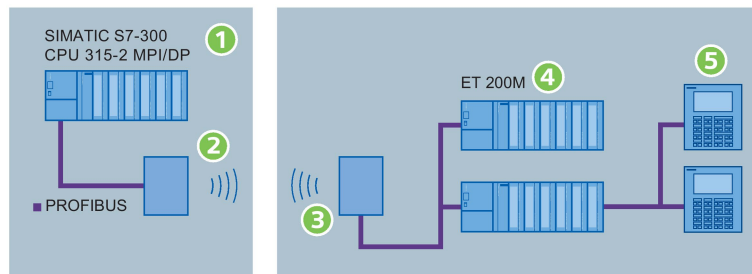
Benefits

- Problem-free integration of the SCALANCE X devices due to the availability of port modules for all common transmission media.
- Minimum cabling effort due to Power over Ethernet. All the devices in production and outside storage are supplied with power via the Ethernet cable.
- Simple expansion of the entire system due to the high port density of the SCALANCE X devices.

3.7 Connecting a PROFIBUS network to a PROFINET installation

Task

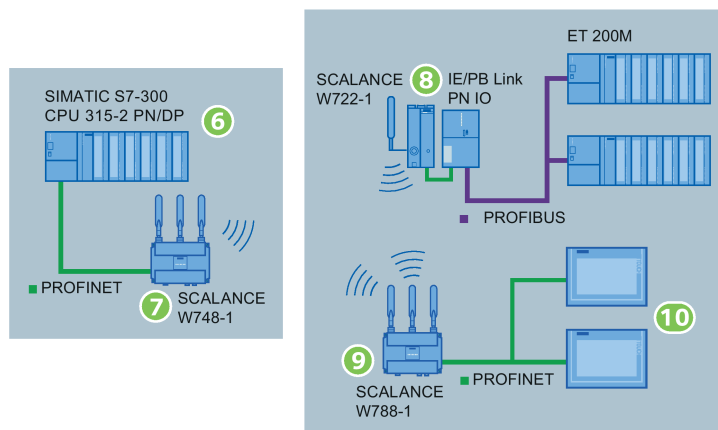
In a brickworks, raw bricks are transported to the drying kiln by a shuttle conveyor ①. The functions of the shuttle conveyor are controlled by an S7-300. The movements of the shuttle conveyor are synchronized with the production process in the stationary parts of the works with which the conveyor communicates via a wireless PROFIBUS modem ②. The doors of the drying kiln open automatically when the conveyor arrives and close again automatically. The original solution had a wireless PROFIBUS modem ③ and the ET 200 I/O ④ and operator control stations ⑤ required for production.



This solution alone eliminates numerous problems that occurred previously with the trailing cables but nevertheless there were occasional short interruptions in communication. The reason was that the transmission speed of the wireless PROFIBUS communication was not fast enough for this situation.

Solution

The new solution consists of Industrial Wireless LAN and PROFINET IO. This combines a high data rate in the wireless communication with a communications concept for modular distributed applications based on Ethernet.



⑥ The CPU 315-2 PN/DP used on the conveyor has a PROFINET interface to connect distributed field devices. For the wireless communication, a SCALANCE W748-1 ⑦ is connected as a client module.

3.7 Connecting a PROFIBUS network to a PROFINET installation

- ⑧ In the stationary part of the works, an IWLAN/PB Link PN IO in conjunction with a SCALANCE W722-1 allows unchanged use of the ET 200M modules.
- ⑨ A SCALANCE W788-1 is used as the access point and the operator control stations ⑩ can access the entire system via its Ethernet interface.

Benefits

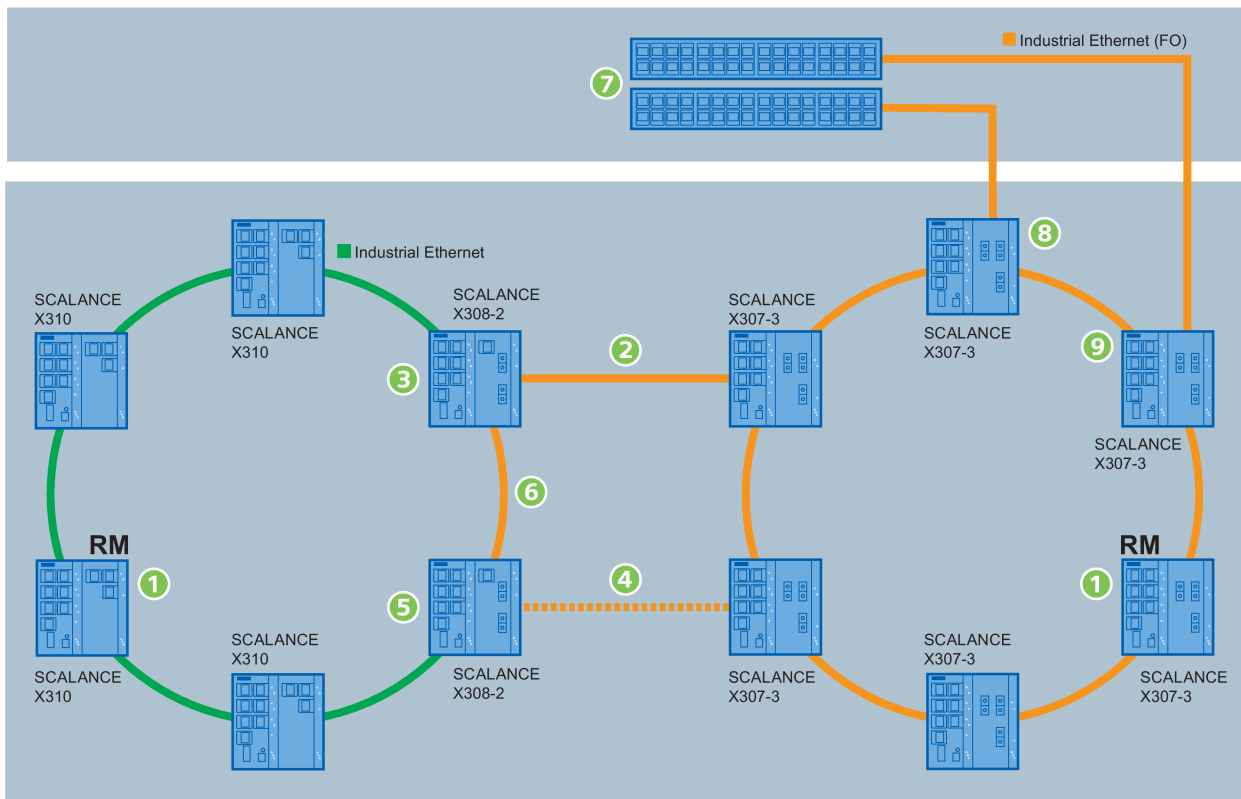
- High data throughput and high reliability in communication with the shuttle conveyor without trailing cables or sliding contacts.
- Transparent network with wireless PROFINET/PROFIBUS gateway.
- When necessary, a PC with a WLAN interface can be used for diagnostics and for process visualization.
- Lower operating costs and reduction of downtimes with maintenance-free IWLAN technology, higher productivity.
- Investment protection due to use of a IE/PB Link PN IO. The existing ET 200 M controllers can continue to be used unchanged.

3.8 Redundant coupled rings with a connection to an office network

Task

In a production plant, two ring topologies need to be interconnected reliably. Faults or the failure of a connecting cable should not have any influence on the data traffic. Data must also be exchanged with the office network of the plant.

Solution



The production network consists of two redundant rings. One switch ① in each of the ring topologies is configured as the redundancy manager (RM) but this does not forward any frames if the transmission path is intact. This means that the ring is interrupted for data traffic at the redundancy manager. If a section of the ring fails, the redundancy manager closes the connection between its ring ports. As a result, all the devices in the ring remain accessible for data traffic.

Due to the high requirements for reliability, the coupling of the two rings is also redundant. In regular operation, the data traffic between the two rings is via cable ②, the device ③ adopts the function of standby master. In this situation, the cable ④ does not transfer any data because the standby slave ⑤ is controlled accordingly by the standby master ③.

If the standby master ③ recognizes that the connection via the cable ② is faulty or interrupted, it activates the cable ④ for data exchange via the standby slave ⑤. Cable ⑥

3.8 Redundant coupled rings with a connection to an office network

serves as the connection between the standby master ③ and the standby slave ⑤. This is a normal network segment that is simply used for the additional function of the standby coupling.

All cables are designed for Gigabit Ethernet because there is an extremely high volume of data to be transferred. Either copper cable or fiber-optic cable can be used without problems because there are SCALANCE X-300 components with gigabit ports for all possible media.

Due to the redundant operation in the two rings of the plant network, Spanning Tree/RSTP cannot be used because an IE switch cannot use both mechanisms at the same time. If Spanning Tree/RSTP is necessary in the office network ⑦, passive listening must be activated for devices ⑧ and ⑨. They then forward (R)STP configuration frames transparently even when (R)STP is disabled for them. This behavior does not conform with the IEEE 802.1d standard but allows the connection of network segments with media redundancy and those that use Spanning Tree/RSTP.

Benefits

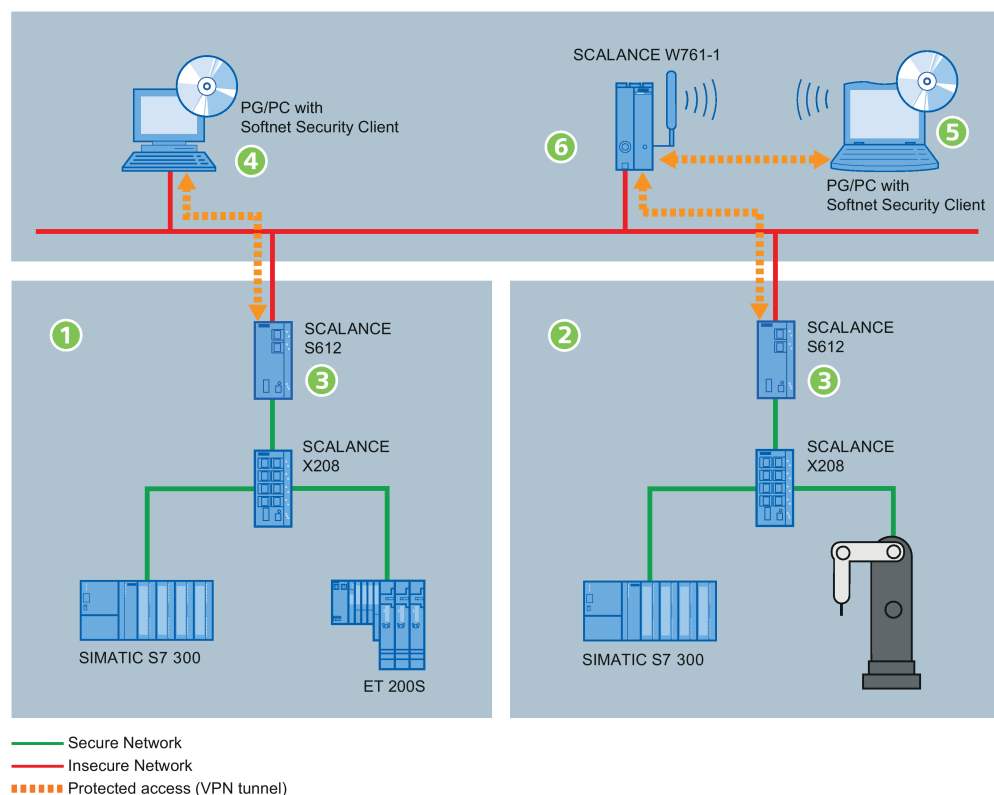
- Extremely high reliability thanks to media redundancy and the redundant coupling of ring topologies.
- High data throughput thanks to gigabit technology.
- Freedom of choice in terms of the transmission medium; depending on specific requirements either twisted-pair cables or fiber-optic cables can be used.
- Connection to networks with activated Spanning Tree/RSTP by using passive listening.

3.9 Data protection during mobile communication

Task

In an assembly plant, access to field devices and the control technology should only be possible for authorized personnel for commissioning, maintenance and service. Due to the size of the plant, network access should also be possible for mobile nodes. In particular, in this case, reliable protection of the automation cells against unauthorized access, manipulation and espionage is necessary.

Solution



Within the automation cells ① and ②, devices can be used without their own security functionality. The entire data exchange with these devices is via a SCALANCE S612 ③ that, among other things, provides the function of a firewall. The protection also extends to layer 2 frames if the SCALANCE S612 is not operating as a router.

④ Devices in public networks can also communicate with the automation cells if they use the SOFTNET Security Client software. This means that the PC/PG is automatically configured so that it can establish a secure IPsec tunnel in the VPN (Virtual Private Network) to one or more SCALANCE S612 modules. As a result, STEP 7 for example can be used to access devices in an automation cell protected by a SCALANCE S612 via a secure tunnel. This cell protection concept allows the use of effective security structures even for access by external devices.

⑤ This protected access is also possible from mobile PCs/PGs that communicate by wireless with an access point ⑥. In the assembly plant, several SCALANCE W761-1 ensure full wireless coverage. Roaming (moving from one wireless cell to another) has no influence on the security mechanisms.

Benefits

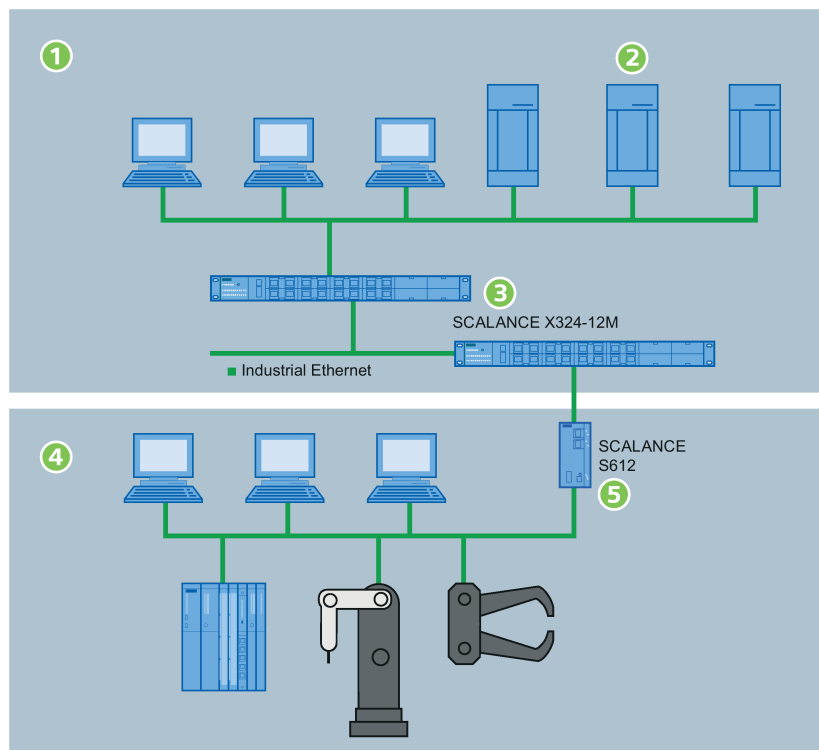
- Reliable protection of the plant against unauthorized access, manipulation and espionage.
- Mobile devices can access the automation cells from any location in the plant which means that the number of stationary nodes for diagnostics and service can be greatly reduced.
- The security mechanisms of the SCALANCE S612 and the SOFTNET Security Client are easy to configure and do not require specialist knowledge.
- No modifications or adaptations of the existing network structure or the applications used are necessary. Internal network nodes are found without configuration.

3.10 Protection of the production network when networking with the office network

Task

In a car bodywork plant, the company network includes both the office network, the data processing center and the automation cells in production. The integration of all company areas allows continuity from the enterprise to the field level. This means that process data such as numbers produced, manufacturing number and type names are available throughout the company. Apart from this, fully integrated diagnostics can be created for field devices and network components. This continuity does, however, involve certain risks. There is a danger of unauthorized access from the office network to the automation cells and the influence of one automation cell on another. The network needs to be structured so that these weak points are eliminated. The configuration should also be simple to create since personnel without special training in security will be involved in commissioning and service.

Solution



① The office network includes a Syslog server ② that also logs unauthorized access attempts and overload situations.

③ Switches of the type SCALANCE X324-12M are responsible for handling the data traffic. With their gigabit ports, these devices are not only suitable for a high data throughput, they also provide wide-ranging configuration options for parameters relevant to security. Using the access control function, for example, individual ports can be blocked for unknown nodes.

3.10 Protection of the production network when networking with the office network

④ Each automation cell includes several components that are connected to the network (controllers, robots, field devices). A SCALANCE S602 ⑤ acting as a firewall filters the data packets and allows communications connections according to the firewall rules. Criteria for the filtering might be the IP address, the MAC address or the communications protocol. There is also an option for limiting overload. The logging functionality allows access monitoring and logs attacks and attempted access to allow preventive measures to be taken. Syslog information such as process data is automatically sent to the Syslog server. To allow effective protection of the automation cells, an IP address conversion is necessary and for this the SCALANCE S602 uses the NAT and NAPT methods.

These measures implement a comprehensive cell protection concept for the individual production areas. The production network is protected effectively and reliably from unauthorized access from the office network and the office network is also protected from any influence from the production network.

Benefits

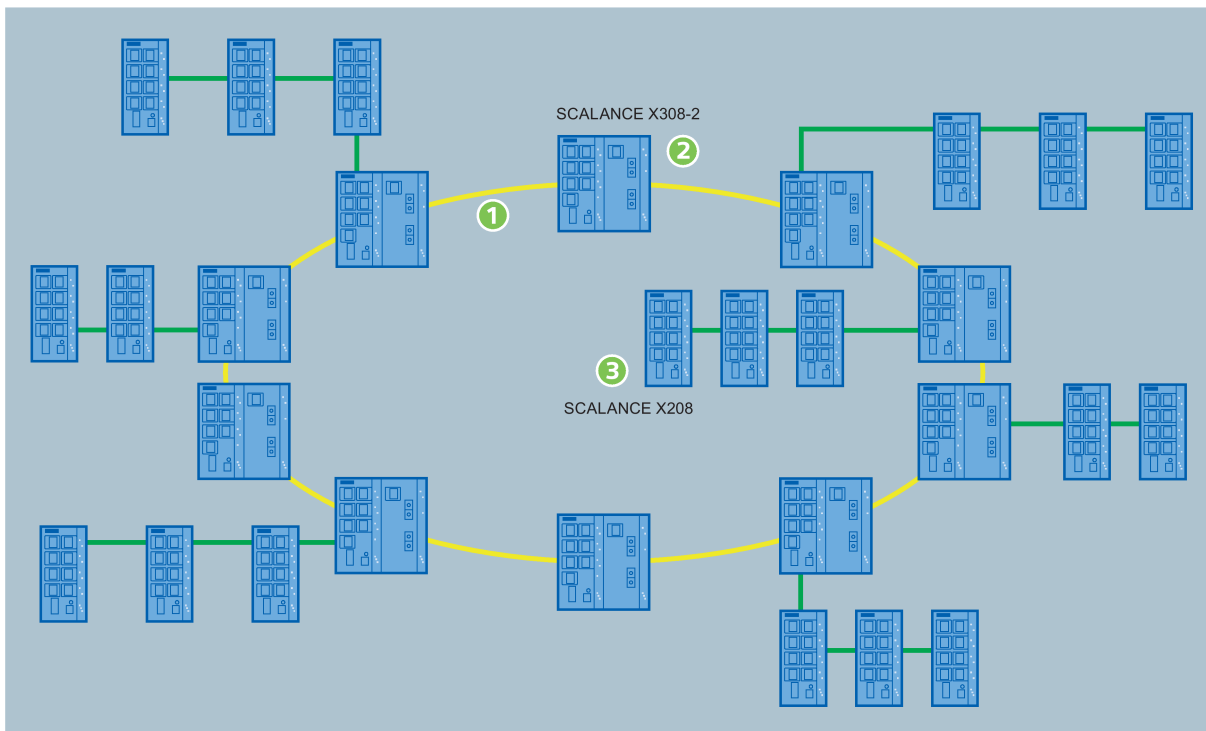
- Effective protection from mutual influence between production and office network.
- Protecting the plant from unauthorized attacks and communication overload by using SCALANCE S602.
- Continuous monitoring of access to the production network.
- Cost savings by saving on public IP addresses.
- Simple maintenance and diagnostics, since all protected cells can be set up identically.

3.11 Gigabit network in the pharmaceuticals industry

Task

An existing network needs to be replaced by a new future-proof network. The aim was not only to increase the bandwidth (gigabit), but to provide ideal conditions for PROFINET. The intention was to use only open communications standards and there was very little time for the implementation.

Solution



① A redundant glass fiber-optic ring was selected as the backbone. The total length of this cable is approximately 2 km.

② The ring topology was set up with SCALANCE X308-2 devices. This device has three gigabit ports (2 x fiber-optic, 1 x RJ-45) as well as comprehensive management functions. The gigabit ports are used for a high-speed connection between the switches. One SCALANCE X308-2 is configured as the redundancy manager and this prevents frames from circulating if the transmission path is intact. If the transmission path is interrupted, this closes the connection between its ring ports and restores a connection between all the components.

③ The second level linear bus structures are made up of SCALANCE X208 devices. These devices also have a compact housing suitable for industry that is, for example, equipped with securing collars for the RJ-45 jacks. In conjunction with the FastConnect connectors used, this achieves a high degree of mechanical stability within the network.

Benefits

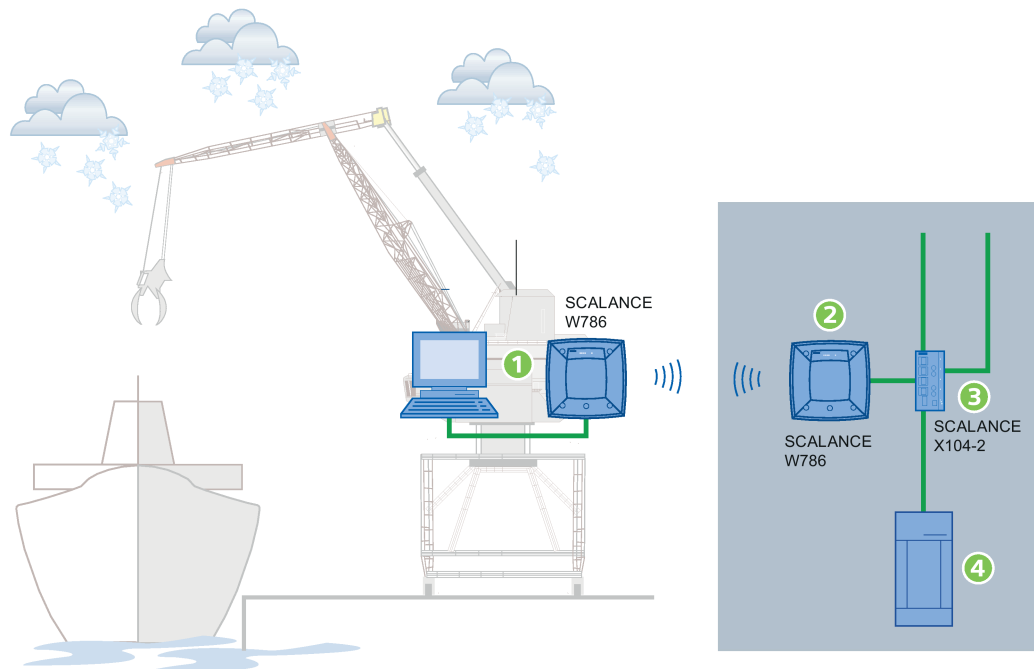
- Ideal configurability and simple diagnostics of the SCALANCE X devices.
- More bandwidth due to the gigabit backbone.
- Future-proof and suitable for straightforward expansion due to the use of PROFINET.

3.12 Communications components for extreme climatic conditions

Task

A mobile loading crane in a harbor needs to be supplied with data from a logistics center. The devices used must be able to stand up to extreme environmental conditions (salt water spray, strong vibration caused by the movement of the crane).

Solution



The communication between the crane and the logistics center is handled via Industrial Wireless LAN. The advantage of wireless data transmission is that neither sliding contacts nor trailing cables are necessary. Taking into account the environmental conditions, this represents a considerable saving in costs.

- ① The loading crane is equipped with a SCALANCE W786 and a PC for displaying and entering data. The SCALANCE W786 fitted to the outside of the crane is particularly suitable for this application due to its resistance to ultraviolet light and salt water. The device is configured as a client. Thanks to the antennas integrated in the housing, external antennas and the associated cabling are unnecessary.
- ② A SCALANCE W786 is also mounted on a building of the logistics center and acts as the access point.
- ③ The integration of the access point in the company network is achieved with a SCALANCE X104-2. Among other things, this switch provides two interfaces for fiber-optic cables that can also be used for networks with a large span. This means that the server of

the logistics center ④ can be accessed although it is several hundred meters away from the loading station.

Benefits

- High availability thanks to maintenance-free components for data transmission.
- Unrestricted suitability of the implemented solution for the difficult environmental conditions.
- Simple integration in the existing company network.
- Access to logistics data regardless of location.

SCALANCE network components

4.1 Product families

The name SCALANCE stands for SIMATIC NET network components for simple setup, management and operation of Industrial Ethernet LANs. The product families are as follows:

- **SCALANCE X** is the product family of Industrial Ethernet switches. Switches are active network components that distribute data to specific addressees, control network traffic and ensure that the load on network connections is optimally distributed. SCALANCE X switches are available in a wide range of variants with electrical and/or optical ports, and in some cases with special functionalities to meet strict real-time requirements.
- **SCALANCE W** is the family of components and accessories for wireless local area networks ("WLANs"). The use of access points, clients and accessories allows the connection of mobile nodes and the establishment of networks in exacting environments. SCALANCE W components are distinguished by their robustness, security and reliability. Wireless transmission can be implemented using omnidirectional antennas, directional antennas or over short distances with leaky feeder cables (RCoax cable).
- **SCALANCE S** security modules protect automation networks from unauthorized access and unnecessary communication load. Both eavesdropping and attacks by outsiders are prevented reliably. Even if there are disturbances in the external network, data traffic in the automation cell remains unaffected. Communication is protected regardless of the application protocol used.
- **SCALANCE M** devices are used as LTE, UMTS, EGPRS (GPRS with Edge) and GPRS routers for wireless IP communication of Industrial Ethernet-based programmable controllers via LTE, UMTS / GSM mobile wireless networks. With LTE and UMTS high transmission speeds are achieved. An integrated firewall provides extensive security functions. Some models can be used both as VPN servers and VPN clients (IPsec).

Note

For further information to support you when selecting Industrial Ethernet switches and when configuring the modular variants, the SIMATIC NET Selection Tool is available.

Online version: <http://www.siemens.de/snst>

Offline version: <http://www.siemens.de/snst-download>

4.2 Common properties of all SCALANCE devices

Properties shared by all SCALANCE devices

All SCALANCE devices have the following properties. If there are exceptions, this will be pointed out in the description of the relevant device.

Autocrossover function

All SCALANCE devices have an integrated MDI/MDIX autocrossover function on their electrical ports making it possible to use straight-through cables. This prevents malfunctions resulting from mismatching send and receive lines. This makes installation much easier for the user.

Autonegotiation

All SCALANCE devices also have the autonegotiation function. Autonegotiation means the automatic detection of the functionality of the interface at the opposite end. Using autonegotiation, repeaters or end devices can detect the functionality available at the interface of a partner device allowing automatic configuration of different types of device. With autonegotiation, two components connected to a link segment can exchange parameters and with these parameters set themselves to the supported communication functionality.

The SCALANCE devices are therefore plug-and-play devices that require no settings when they are put into operation.

Please note the following:

- Devices not supporting autonegotiation must be set to half duplex.
- The port speed and duplex mode must be set identically on the connection partners otherwise frames may be lost.

Fault mask

On all SCALANCE devices with a button on the front panel, it is possible to set a specific configuration as the desired status (good status). Deviations from this setting occurring during operation are treated as errors.

Monitored error statuses include, for example, the status of the power supply or link down to a communications partner, to which the SCALANCE device reacts with a fault LED and by opening the signaling contact.

Avoiding loops

The typical configuration of a network with the SCALANCE products is a tree structure. The direct connection of two ports on the switch or accidental connection over several switches causes an illegal loop. Such a loop can lead to network overload and network failures.

When configuring the network with SCALANCE XB200, X300, X400 and X500, meshing is possible since, in this case, the Rapid Spanning Tree algorithm can eliminate loops. At the same time, RSTP increases the availability of the network. If one connection fails, the redundant connection is activated.

Cable length at the electrical ports

A maximum of two IE-TP cords or IE-TP-XP cords with a total length of max. 10 m can be used between two adjacent SCALANCE devices with IE TP ports.

With the IE FC cables and IE FC RJ-45 plug, an overall cable length of a maximum of 100 m is permitted between two devices depending on the cable type.

Table 4- 1 Maximum section length with twisted-pair cables

Cabling structure	Cable type	Max. length	Max. total of the patch cables (TP cord)
In one piece (without IE TP cords)	IE FC standard cable GP	100 m	-
	IE FC flexible cable GP	85 m	
	IE FC torsion cable GP	55 m	
	IE FC trailing cable GP	85 m	
	IE FC trailing cable	85 m	
	IE FC marine cable	85 m	
	IE FC FRNC cable GP	85 m	
	IE FC food cable	85 m	
	IE FC festoon cable GP	85 m	
Structured (with IE-TP cords and IE FC outlet RJ-45 or IE FC RJ-45 modular outlet)	IE FC standard cable GP	90 m	10 m
	IE FC flexible cable GP	75 m	
	IE FC torsion cable GP	45 m	
	IE FC trailing cable GP	75 m	
	IE FC trailing cable	75 m	
	IE FC marine cable	75 m	
	IE FC FRNC cable GP	75 m	
	IE FC food cable	75 m	
	IE FC festoon cable GP	75 m	

Notes on installation

When installing the devices note the information in the operating instructions of the particular device. Apart from a few exceptions, the devices are suitable for wall mounting, DIN rail mounting and S7 standard rail mounting. In individual cases the required type of mounting can be made possible by using a mounted adapter.

4.3 Web Based Management for configuring networks

Configuration over a Web interface

All SCALANCE devices that have management functions can be configured using "Web Based Management" (WBM).

The devices have an integrated Web server that can be accessed by the configuration engineer with a browser via every Ethernet connection. The server then provides a series of Web pages. On these Web pages, the configuration engineer can make all important settings and can also run diagnostics and report functions.



Figure 4-1 Web Based Management based on the example of configuring a W788 access point

Advantages

- Access is possible from any PC with a Web browser installed on it and with an Ethernet connection to the target device. With SCALANCE W devices, this connection can also be over a wireless network.
- The installation of special software is not necessary and no specialist knowledge is required to navigate through and work with WBM.
- Access is password protected.

For more detailed information on the functions of the WBM, refer to the compact operating instructions of the individual devices and in the configuration manual.

4.4 SCALANCE X switches and media converters

4.4.1 Type designations and properties

Overview of the performance classes of the SCALANCE X devices

The following overview graphic provides you with a summary of the performance classes covered by the various SCALANCE X devices.

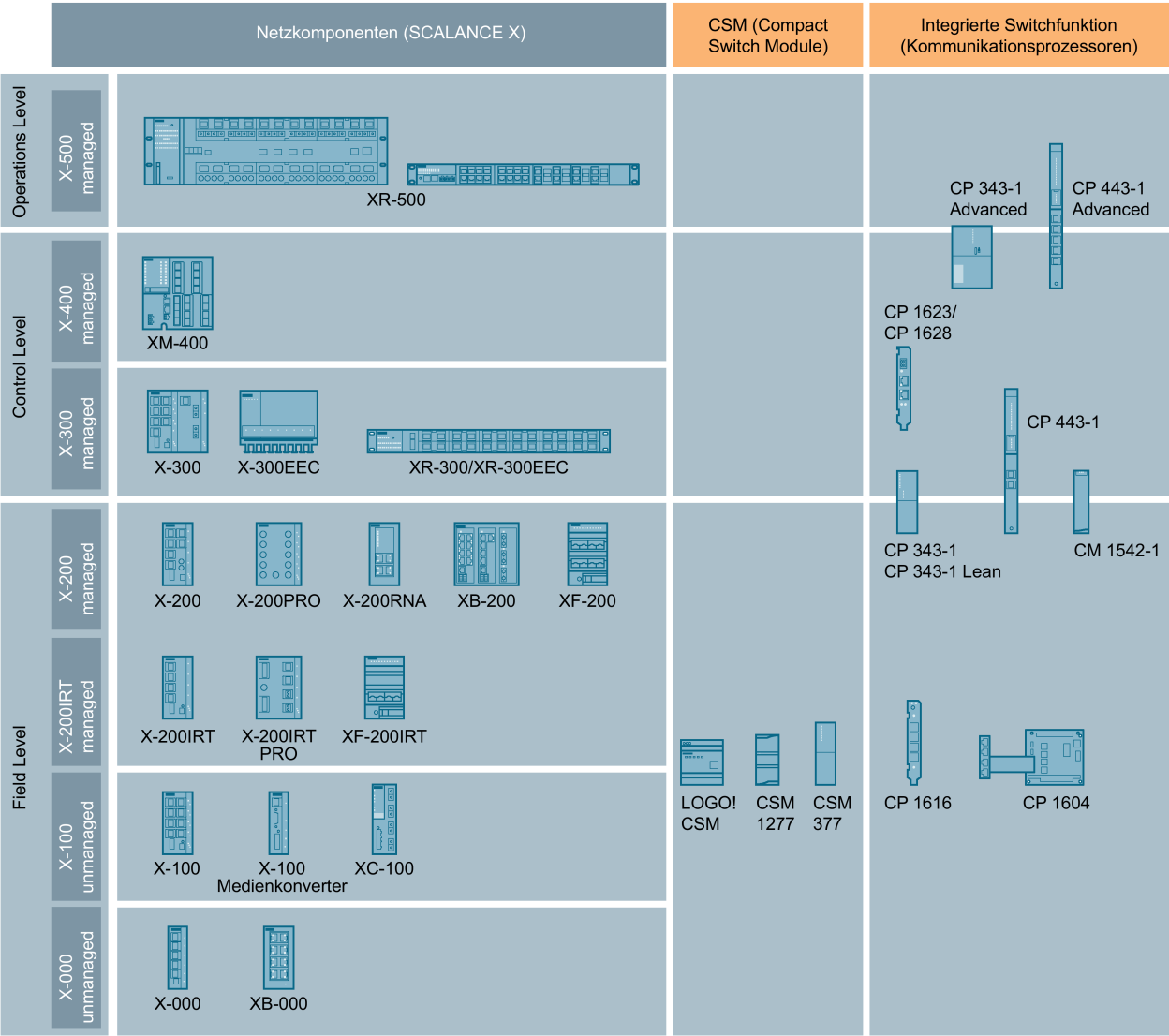


Figure 4-2 Overview of IE switches

Type designations and properties

Identified the SCALANCE X devices based on their type key. The design and basic properties can be identified based on the following type key.

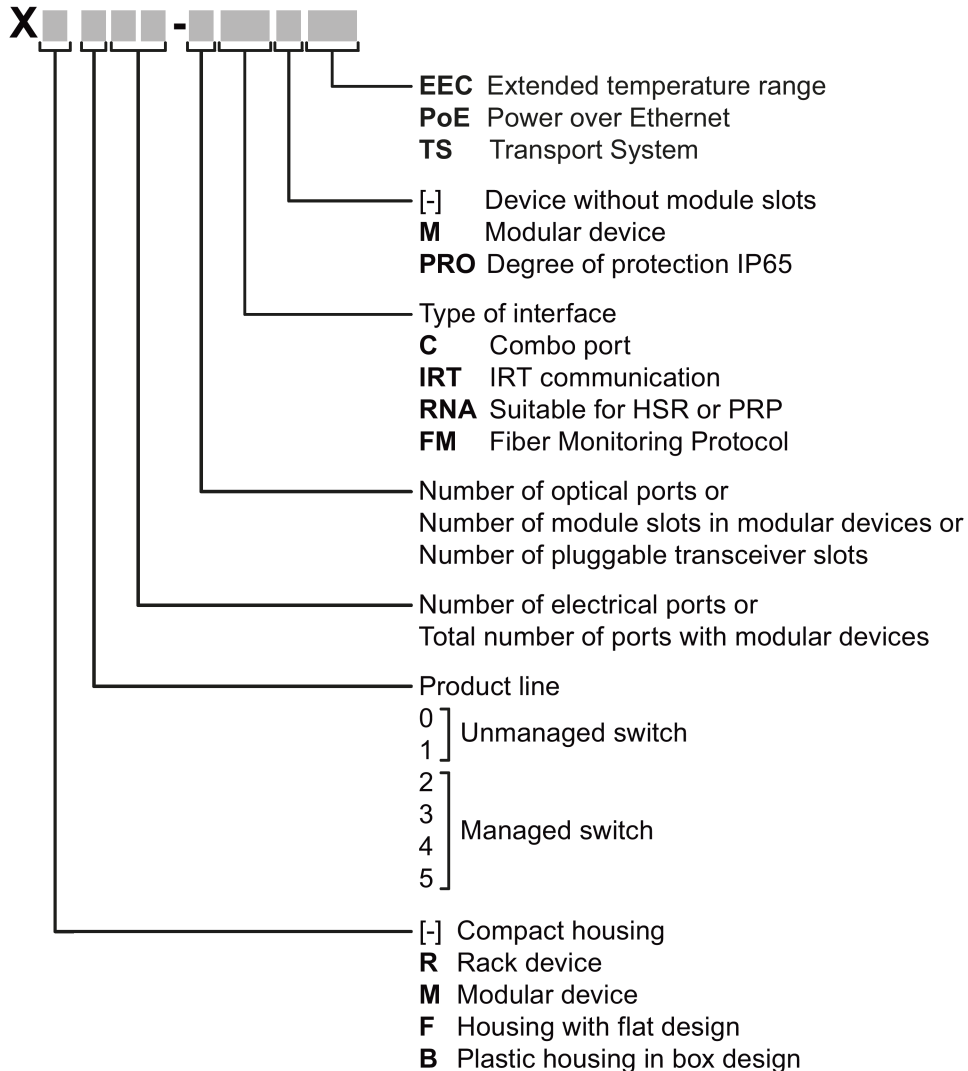


Figure 4-3 Type key SCALANCE X

Interfaces of devices without optical ports:

Interface	Property
LF	Electrical RJ-45 port with 10 Mbps
FE	Electrical RJ-45 port with 10/100 Mbps.
GE	Electrical RJ-45 port with 10/100/1000 Mbps.
RNA	Ethernet interface with RNA capability
[-]	Electrical RJ-45 port for 10/100 Mbps or 10/100/1000 Mbps.

Interfaces of devices with optical ports:

Interface	Property
LF	BFOC port 10 Mbps multimode FO cable (up to max. 5 km)
FE	SC port 100 Mbps multimode FO cable (up to max. 5 km)
LD FE	SC port 100 Mbps single mode FO cable (up to max. 26 km)
POF	SC port with 100 Mbps plastic optical fiber, POF (up to max. 0.05 km)
P	POF/PCF SC RJ ports 100 Mbps
[-]	SC port 1000 Mbps multimode FO cable (up to max. 750 m).
LD	SC port 100 Mbps single mode FO cable (up to max. 10 km).
LH	SC port 100 Mbps single mode FO cable (up to max. 40 km).
LH+	SC port 1000 Mbps single mode FO cable (up to max. 70 km).
ELH	SC port 1000 Mbps single mode FO cable (up to max. 120 km)

Management functions

The SCALANCE X200-, SCALANCE X300-, SCALANCE X400- and SCALANCE X500 devices are equipped with management functions. These devices are also known as "managed switches". The managed devices provide numerous configuration and diagnostics functions that make the operation of an Industrial Ethernet network much more convenient. The SCALANCE X100, SCALANCE XB000 and SCALANCE X005 devices do not have management functions. These "unmanaged switches" are therefore cheaper.

This SCALANCE X modular switches

To achieve the greatest possible flexibility in terms of interfaces, the use of the modular devices such as SCALANCE XR324-12M, SCALANCE X308-2M, and SCALANCE XR-552-12M is recommended. By making use of media modules, these provide the maximum possible variability.

Electrical and optical interfaces

The SCALANCE X devices can be used as switches in both optical and electrical Industrial Ethernet networks. Each performance class therefore includes devices with varying numbers of electrical and optical interfaces. The optical interfaces also include versions specially designed to cover long distances. These are available in devices that have LD, LH, LH+ or ELH in the device designation.

Combo ports

Combo port is the name for two communication ports. A combo port has the two following jacks:

- a fixed RJ-45 port
- an pluggable transceiver slot that can be equipped individually

Of these two ports, only one can ever be active. Using the mode, you can decide how the ports are prioritized. The port name is the same on both jacks of the combo port, for example

"P3C". There is an LED for each combo port. The LEDs for the combo ports can be identified by a vertical line and the word "COMBO". The labeling of the combo port LEDs does not differ from that of the other LEDs, e.g. "P3".

Fault-tolerance due to redundancy

The SCALANCE X200, X300, X400- and X500 switches have functions that allow the setup and management of redundant networks in a ring topology. These networks can handle the failure of individual nodes or cable sections and "divert" the data traffic so that the network remains available.

IRT for strict real-time requirements

Devices with the IRT suffix (Isochronous Real Time) are particularly suitable for applications in which a data transmission must be guaranteed at fixed intervals. To allow this, all devices in an Industrial Ethernet have the same timebase. The messages of the preferred nodes are transmitted together at previously configured times. Frames of other nodes are held back by the IRT switches and sent later.

Media converter SCALANCE X100

The media converters of the SCALANCE X-100 line are particularly suitable for applications in which two Industrial Ethernet networks implemented with different media need to be linked. These have only two interfaces and therefore fit into an extremely narrow casing. They can also be used in a redundant ring.

The media converters have electrical and optical interfaces to link optical networks with electrical networks and to link existing network segments or individual end devices.

Devices for special environmental conditions

Some switches are available in special designs so that they can be used in special environments. This includes the design of the housing in IP65 with M12 plug-in connectors. This version has the supplement PRO in the type designation. Switches with the supplement EEC are approved for expanded environmental conditions.

Notes on installation

When installing the devices note the information in the compact operating instructions of the individual device. Apart from a few exceptions, the devices are suitable for wall mounting, DIN rail mounting and S7 standard rail mounting. In individual cases the required type of mounting can be made possible by using a mounted adapter.

Devices with the supplement R are either suitable as a desktop device or for installation in a 19" rack. To do this, install the mounting aids as described in the compact operating instructions.

4.4.2 Functions of SCALANCE X devices

Introduction

This section describes certain functions of SCALANCE X devices. For further information on all the functions, refer to the compact operating instructions of the devices or the configuration manual.

Signaling contact

The signaling contact is connected to a 2-pin plug-in terminal block. The signaling contact (optical relay contact) is a floating switch with which error/fault states can be signaled by breaking the contact.

The following errors/faults are signaled by the signaling contact:

- The failure of a link on one of the two monitored ports.
- The failure of one of the two redundant power supplies.

The connection or disconnection of a communication node on an unmonitored port does not lead to an error message.

The signaling contact remains activated until the error/fault is eliminated or until the current status is applied as the new desired status using the button or by Web Based Management.

When the device is turned off, the signaling contact is always activated (open).

Support of virtual networks (VLAN)

There is no physical difference between a virtual network (VLAN) and a normal LAN. The particular feature of a VLAN is that devices can be assigned to a device group during configuration. Several of these device groups use a network infrastructure that exists only once physically. Several "virtual networks" result on the one physical network. Data exchange and even the transmission of broadcasts takes place only within a VLAN.

You can configure VLANs on the device or using GVRP frames.

MAC address list

If this function is activated for a port, the device only forwards frames received at this port if their source address exists in the address table.

SCALANCE devices log the information about which MAC address can be reached over which port in a learning table. Entries in this list are deleted automatically when there is no further data transfer for the corresponding MAC addresses. The time after which addresses are deleted if there is no data traffic is set in the 'Aging Time' parameter.

The learning table indicates the Ethernet interface on which a MAC address can be reached.

The MAC address list can be based on the port or MAC addresses.

Network access protection complying with the standard IEEE 802.1X

Ports can be configured for end devices that support authentication according to IEEE 802.1X. The authentication is via a RADIUS server.

IGMP snooping and IGMP querier

IGMP (Internet Group Message Protocol, RFC 2236) is a protocol used for the group management of IP multicasts.

The group management is on a central device, for example a switch. With IGM snooping, the switch (IGM querier) queries the multicast group membership of its connected devices. The switch notes the outgoing interfaces on which devices are located that want to receive certain multicast IP packets. The switch enters the devices in a list (MAC filter table). When a switch receives a multicast, the message is forwarded only to the members of the multicast group. The multicast data traffic is therefore filtered and the load on the network limited.

Bundling network links for redundancy and higher bandwidth

Link aggregation according to IEEE 802.3ad allows several links between neighboring devices to be bundled to achieve higher bandwidths, see section Link aggregation (Page 78).

Topology support (LLDP)

The topology is identified using LLDP (Link Layer Discovery Protocol). The devices exchange LLDP frames with each other. The information is stored and can be represented graphically by network management software. In the default setting, LLDP is enabled for all ports; in other words, LLDP frames are sent and received on all ports.

Using the GARP VLAN Registration Protocol (GVRP)

Whether or not a port belongs to a VLAN is set dynamically using GVRP frames.

Forwarding of multicast frames with GMRP (Generic Multicast Protocol)

GMRP is a mechanism for efficient forwarding of multicast frames. With a GARP Information Declaration (GID), a node registers with the IE switch as recipient for a multicast address. The IE switch sends this registration to its ports. As a result, this address is also known to other IE switches and they send multicast frames for this address only to ports that have received a registration for this address.

Fast redundancy in the ring

The following redundancy methods are possible:

- MRP in the ring with a maximum reconfiguration time of 200 ms, see section MRP (Page 72)
- HSR with a maximum reconfiguration time of 300 ms, see section HRP (Page 74)

- MRPD (IE switches with IRT) with 250 μ s reconfiguration time, see section MRPD (Page 73)
- Standby redundancy, see section HRP (Page 74)

Limiting the transfer rate of incoming and outgoing data

To limit the transfer load, the maximum number of data packets per second can be specified for the individual ports.

The limit values can apply to the following category of frames:

- Broadcast: Special form of multicast.
- Multicast: A device sends a single data packet to several recipients
- Unicast: A device sends the data packets to one recipient

4.4.3 SCALANCE X005

4.4.3.1 Description



Figure 4-4 SCALANCE X005

The SCALANCE X005 switch allows the cost-effective installation of small Industrial Ethernet linear bus or star structures with switching functionality.

The SCALANCE X005 has five RJ-45 jacks for connection of end devices or other network segments.

To keep the size of the switch as small as possible while including a large number of TP interfaces, a redundant power supply and signaling contact were not implemented.

4.4.3.2 Functions

The switch does not support any redundancy functions and cannot be used in redundant networks. An exception is between two devices capable of RNA. If the connecting network line is not subject to other redundancy methods, the device does not need to be capable of redundancy or RNA.

The SCALANCE X005TS (transportation systems) is suitable for railway and road traffic due to its specification according to EN 50155 and e1/E1.

4.4.3.3 Interfaces

Core statement

Table 4- 2

Name	SCALANCE X005	SCALANCE X005TS
Transmission rate	10/100 Mbps	10/100 Mbps
Interfaces	2 x RJ-45 ports	5 x RJ-45 ports
Power supply	1	1
Signaling contact	--	--

Article numbers

X005	Industrial Ethernet Switch for 10/100 Mbps; with five 10/100 Mbps RJ45 ports for setting up small star and bus structures	6GK5005-0BA00-1AA3
X005TS	Industrial Ethernet Switch with expanded temperature range and approvals for use in rail and road traffic	6GK5005-0BA00-1CA3

4.4.4 SCALANCE XB000

4.4.4.1 Description



Figure 4-5 SCALANCE XB000

The unmanaged Industrial Ethernet switches of the SCALANCE XB000 line allow small electrical and optical star or bus structures to be set up with switching functionality in machines or plant sections. Depending on the version, the switches have 5 to 8 RJ-45 jacks for connection of end devices or other network segments. Here, a connection can be implemented by an optical interface.

With SCALANCE XB000, there are variants that support gigabit Ethernet. These devices have the suffix G in the device designation.

4.4.4.2 Characteristics

- Data rates of 10/100 and, depending on the specific device, 1000 Mbps (half/full duplex) are supported.
- Diagnostics LED

4.4.4.3 Interfaces

Table 4- 3

IE switch	Twisted pair		Fiber-optic cables				
	RJ-45 connectors 10 / 100 Mbps	RJ-45 connectors 10 / 100 / 1000 Mbps	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Max. segment length / km	Multi- mode	Single mode
XB004-1	4	-	1	-	4* / 5**	•	-
XB004-1LD	4	-	1	-	26	-	•
XB005	5	-	-	-	-	-	-
XB008	8	-	-	-	-	-	-
XB004-1G	-	4	-	1	0.75	•	-
XB004-1LDG	-	4	-	1	10	-	•

IE switch	Twisted pair		Fiber-optic cables				
	RJ-45 connectors 10 / 100 Mbps	RJ-45 connectors 10 / 100 / 1000 Mbps	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Max. segment length / km	Multi- mode	Single mode
XB005G	-	5	-	-	-	-	-
XB008G	-	8	-	-	-	-	-

• Suitable / available or according to the specified standard.

* at 50 µm core diameter of the FO cable

** at 62.5 µm core diameter of the FO cable

Article numbers

XB004-1	4 x 10/100 Mbps RJ-45 ports electrical, 1x 100 Mbps SC port optical (multimode, glass), up to max. 5 km	6GK5004-1BD00-1AB2
XB004-1LD	4 x 10/100 Mbps RJ-45 ports electrical, 1x 100 Mbps SC port optical (single mode, glass), up to max. 26 km	6GK5004-1BF00-1AB2
XB005	5 x 10/100 Mbps RJ-45 ports electrical	6GK5005-0BA00-1AB2
XB008	8 x 10/100 Mbps RJ-45 ports electrical	6GK5008-0BA00-1AB2
XB004-1G	4 x 10/100/1000 Mbps RJ-45 ports electrical, 1x 1000 Mbps SC port optical (multimode, glass), up to 0.75 km	6GK5004-1GL00-1AB2
XB004-1LDG	4 x 10/100/1000 Mbps RJ-45 ports electrical, 1x 1000 Mbps SC port optical (single mode, glass), up to max. 10 km	6GK5004-1GM00-1AB2
XB005G	5 x 10/100/1000 Mbps, RJ-45 ports electrical	6GK5005-0GA00-1AB2
XB008G	8 x 10/100/1000 Mbps, RJ-45 ports electrical	6GK5008-0GA00-1AB2

4.4.5 SCALANCE XC100-4OBR

4.4.5.1 Description



Figure 4-6 SCALANCE XC100-4OBR

The optical bypass relay SCALANCE XB100-4OBR is used to turn end devices in a network topology on or off without impairing the communication between the other network devices. If the end device is not part of the network, the bypass relay bridges its two network interfaces as if the end device did not exist. With devices with the TAP function, however, data is sent to the end device. In addition to this, the end device can establish a link to the neighboring network components.

4.4.5.2 Features and functions

Features

	SCALANCE XC100-4OBR (single mode, with TAP function) SCALANCE XC100-4OBR (single mode, without TAP function)	SCALANCE XC100-4OBR (multimode with TAP function)
Diagnostics LED	•	•
Gigabit Ethernet	•	-
Redundant power supply	•	•
Signaling contact	•	•
On site display (Set button)	•	•
C-PLUG slot	-	-

- Suitable / available or according to the specified standard.

Functions

The SCALANCE XC100-4OBR do not have configurable functions like other SCALANCE X devices. The startup time and the monitoring voltage can be configured with a button directly on the device.

4.4.5.3 Interfaces

Table 4- 4

IE switch	Twisted pair			Fiber-optic cables				
	RJ-45 connect-ors 10/100 Mbps	RJ-45 connect-ors 10/100/1000 Mbps	RJ-45 connect-ors 10/100/1000 Mbps with PoE	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Max. segment length / km	Multimode	Single mode
XC100-4OBR single mode, with TAP function	-	-	-	-	4 (SC)	10	-	•
XC100-4OBR single mode, without TAP function	-	-	-	-	4 (SC)	10	-	•
XC100-4OBR multimode with TAP function	-	-	-	4 (SC)	-	4* / 5*	•	-

• Suitable / available or according to the specified standard.

* at 50 µm core diameter of the FO cable

** at 62.5 µm core diameter of the FO cable

Article numbers

XC100-4OBR	4 x 100/1000 Mbps SC ports single mode, with TAP function	6GK5100-4AV00-2FA2
	4 x 100/1000 Mbps SC ports single mode, without TAP function	6GK5100-4AV00-2DA2
	4 x 10/100 Mbps SC ports multimode, with TAP function	6GK5100-4AW00-2FA2

4.4.6 SCALANCE XB-200

4.4.6.1 Description

Overview



Figure 4-7 SCALANCE XB208



Figure 4-8 SCALANCE XB213-3LD

The SCALANCE XB-200 series provides devices suitable for industry at aa favorable price. They can be used anywhere where there are no high requirements regarding mechanical load, degree of protection and equipment. The devices have a plastic housing in degree of protection IP20 and are intended for installation in the cabinet. They can be installed on a DIN rail without tools. They also have a separate console connector and a redundant power supply. There are various port configurations for copper and fibre-optic cables. All the designs are available in two variants that differ in the factory settings (Ethernet/IP or PROFINET variant). This minimizes configuration effort and the devices are quickly ready for use.

4.4.6.2 Features and functions

Features

	XB208 XB205-3 (SC) XB205-3LD (SC) XB205-3 XB216 XB213-3 (SC) XB213-3LD (SC) XB213-3
Diagnostics LED	•
Redundant power supply	•
Signaling contact	-
On site display (Set button)	-
C-PLUG slot	-

- Suitable / available or according to the specified standard.

Functions

All devices have the following functions:

- Configuration with the Primary Setup Tool (PST) V3 or higher;
To be able to use the Primary Setup Tool to assign the IP address, the SCALANCE XB-200 must be accessible over Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7 V 5.3 plus SP 1
- Web-based management
- Command Line Interface
- Configuration with STEP 7
- SNMP
- Sntp
- Ring redundancy including RM functionality or RSTP
- Passive listening
- PROFINET diagnostics
- Topology support (LLDP)
- Standby redundancy

- All models are available in two variants: PROFINET and EtherNet/IP. The mode can, however, be switched over as required with both device variants.
- In the EtherNet/IP mode, the devices also have EtherNet/IP diagnostics.

4.4.6.3 Interfaces

Table 4- 5

IE switch	Twisted pair		Fiber-optic cables					
	RJ-45 connectors 10 / 100 Mbps	M12 10 / 100 Mbps	Optical connectors 100 Mbps	Optical connectors 1000 Mbps	Max. segment length / km	FO multi-mode	FO single mode	POF PCF
XB208	8	-	-	-	-	-	-	-
XB205-3 (SC)	5	-	3 (SC)	-	4* / 5**	•	-	-
XB205-3LD (SC)	5	-	3 (SC)	-	10	-	•	-
XB205-3	5	-	3 (ST)	-	4* / 5**	•	-	-
XB216	16	-	-	-	-	-	-	-
XB213-3 (SC)	13	-	3 (SC)	-	4* / 5**	•	-	-
XB213-3LD (SC)	13	-	3 (SC)	-	10	-	•	-
XB213-3	13	-	3 (ST)	-	4* / 5**	•	-	-

- Suitable / available or according to the specified standard.

* with a core diameter of 50 µm

** with a core diameter of 62.5 µm

Article numbers

Device	Description	Article number (Ethernet/IP)	Article number (PROFINET)
SCALANCE XB208	8 x 10/100 Mbps RJ-45 ports	6GK5208-0BA00-2TB2	6GK5208-0BA00-2AB2
SCALANCE XB205-3 (SC)	5 x 10/100 Mbps RJ-45 ports, 3 x 10/100 Mbps SC ports, multimode fiber-optic cable	6GK5205-3BD00-2TB2	6GK5205-3BD00-2AB2
SCALANCE XB205-3LD (SC)	5 x 10/100 Mbps RJ-45 ports, 3 x 10/100 Mbps SC ports, single mode fiber-optic cable	6GK5205-3BF00-2TB2	6GK5205-3BF00-2AB2
SCALANCE XB205-3	5 x 10/100 Mbps RJ-45 ports, 3 x 10/100 Mbps ST ports, multimode fiber-optic cable	6GK5205-3BB00-2TB2	6GK5205-3BB00-2AB2
SCALANCE XB216	16 x 10/100 Mbps RJ-45 ports	6GK5216-0BA00-2TB2	6GK5216-0BA00-2AB2
SCALANCE XB213-3 (SC)	13 x 10/100 Mbps RJ-45 ports, 3 x 10/100 Mbps SC ports, multimode fiber-optic cable	6GK5213-3BD00-2TB2	6GK5213-3BD00-2AB2

Device	Description	Article number (Ethernet/IP)	Article number (PROFINET)
SCALANCE XB213-3LD (SC)	13 x 10/100 Mbps RJ-45 ports, 3 x 10/100 Mbps SC ports, single mode fiber-optic cable	6GK5213-3BF00-2TB2	6GK5213-3BF00-2AB2
SCALANCE XB213-3	13 x 10/100 Mbps RJ-45 ports, 3 x 10/100 Mbps ST ports, multimode fiber- optic cable	6GK5213-3BB00-2TB2	6GK5213-3BB00-2AB2

4.4.7 SCALANCE X200/X200 IRT

4.4.7.1 Description

Overview



Figure 4-9 SCALANCE X200 managed switches



Figure 4-10 SCALANCE XF200



Figure 4-11 SCALANCE X 20x IRT PRO



Figure 4-12 SCALANCE X204 RNA

SCALANCE X200 Industrial Ethernet switches allow the cost-effective installation of 10/100 Mbps Industrial Ethernet linear (bus), star and ring structures with switching functionality, where availability of the network or remote diagnostics options are required. The devices have IP30 protection and are designed for installation in a cabinet. With IP65, the SCALANCE X208PRO is intended for installation outside a cabinet. The SCALANCE X202-2P IRT PRO and SCALANCE X204 IRT PRO devices have IP67 protection.

SCALANCE X200 switches vary in terms of the functions they provide and the number and type of electrical and optical IE interfaces.

The SCALANCE X200IRT switches form a special class by using the "cut through" switching mechanism, the optimum solution to meet the real-time requirements of PROFINET. SCALANCE X200IRT switches allow the installation of isochronous mode real-time Industrial Ethernet linear bus and star structures with switching functionality. The special requirements for automation solutions in terms of linear topology, hard real time and unrestricted IT openness are incorporated in one technology.

The only difference between the devices of the SCALANCE XF200 product line and the SCALANCE X200 product is the flatter construction.

4.4.7.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	X204-2 X204-2LD X206-1 X206-1LD X208 X208PRO X212-2 X212-2LD X216 X224 XF204 XF204-2 XF206-1 XF208	X204-2TS X204-2LD TS	X204-2FM	X200-4P IRT X201-3P IRT X202-2IRT X202-2P IRT X204IRT XF204IRT	X201-3P IRT PRO X202-2P IRT PRO X204IRT PRO	X204RNA X204RNA EEC
Diagnostics LED	•	•	•	•	•	•
Redundant power supply	•	•	•	•	-	•
Signaling contact	•	•	•	•	•	•
On site display (Set button)	•	•	•	•	•	•
Railway approval	-	•	-	-	-	-
Fiber Monitoring Protocol	-	-	•	-	-	-
IRT communication	-	-	-	•	•	-
Suitable for HSR or PRP	-	-	-	-	-	•
C-PLUG slot	•	•	•	•	•	•

- Suitable / available or according to the specified standard.

Functions

All devices have the following functions:

- Configuration with the Primary Setup Tool (PST) V3 or higher;
To be able to use the Primary Setup Tool to assign the IP address, the SCALANCE X-200 must be accessible over Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7 V 5.3 plus SP 1
- Web-based management
- Command Line Interface

- Configuration with STEP 7
- SNMP
- SNTp

Apart from X208PRO, the devices have the following functions:

- PROFINET diagnostics
- Topology support (LLDP)
- Ring redundancy including RM functionality
- Passive listening

The devices with the supplement IRT have the following further functions:

- Standby redundancy
- IRT capability
- Fast learning
- RNA (PRP)

4.4.7.3 Interfaces

Table 4- 6

IE switch	Twisted pair		Fiber-optic cables					
	RJ-45 connectors 10 / 100 Mbps	M12 10 / 100 Mbps	Optical connectors 100 Mbps	Optical connectors 1000 Mbps	Max. segment length / km	FO multi-mode	FO single mode	POF PCF
X204-2	4	-	2 (BFOC)	-	4* / 5**	•	-	-
X204-2TS	4	-	2 (BFOC)	-	4* / 5**	•	-	-
X204-2LD	4	-	2 (BFOC)	-	26	-	•	-
X206-1	6	-	1 (BFOC)	-	4* / 5**	•	-	-
X206-1LD	6	-	1 (BFOC)	-	26	-	•	-
X208	8	-	-	-	-	-	-	-
X208PRO	-	8	-	-	-	-	-	-
X212-2	12	-	2 (BFOC)	-	4* / 5**	•	-	-
X212-2LD	12	-	2 (BFOC)	-	26	-	•	-
X216	16	-	-	-	-	-	-	-
X224	16	-	-	-	-	-	-	-
XF204	4	-	-	-	-	-	-	-

IE switch	Twisted pair		Fiber-optic cables					
	RJ-45 connectors 10 / 100 Mbps	M12 10 / 100 Mbps	Optical connectors 100 Mbps	Optical connectors 1000 Mbps	Max. segment length / km	FO multi-mode	FO single mode	POF PCF
XF204-2	7	-	2 (BFOC)	-	4* / 5**	•	-	-
XF206-1	6	-	1 (BFOC)	-	4* / 5**	•	-	-
XF208	8	-	-	-	-	-	-	-
X200-4P IRT	-	-	4 (SC RJ)	-	0.05 / 0.100 ****	-	-	•
X201-3P IRT	1	-	3 (SC RJ)	-	0.05 / 0.100 ****	-	-	•
X201-3P IRT PRO	1	-	3 (SC-RJ / push-pull plug PRO)	-	0.05 / 0.100 ****	-	-	•
X202-2IRT	2	-	2 (BFOC)	-	4* / 5**	•	-	-
X202-2P IRT	-	2	2 (SC RJ)	-	0.05 / 0.100 ****	-	-	•
X202-2P IRT PRO	2 (IE RJ-45 plug PRO)	-	2 (SC-RJ / push-pull plug PRO)	-	0.05 / 0.100 ****	-	-	•
X204IRT	4	-	-	-	-	-	-	-
X204IRT PRO	4 (IE RJ-45 plug PRO)	-	-	-	-	-	-	-
X204RNA	2 x 2 2 x ports and 2 x PRP ports	-	-	-	-	-	-	-
X204RNA EEC	2x2 2 RJ-45 (ports) and 2 x RJ-45 or 2 x SFP modules (PRP ports)	-	2 (Duplex LC)	-	3 (SFP991-1)	•	-	-
		-	2 (Duplex LC)	-	26 (SFP991-1LD) 70 (SFP991-1LH+)	-	•	-

• Suitable / available or according to the specified standard.

* at 50 µm core diameter of the FO cable

** at 62.5 µm core diameter of the FO cable

*** with POF fiber-optic cables 1 - 50 m and PCF fiber-optic cables 1 - 100 m

Note

TP connectors of SCALANCE X204RNA EEC

2 x RJ-45 for connecting two end devices / network structures without PRP-1 capability and optionally 2 x RJ-45 or 2 x SFP modules for connecting network structures capable of PRP. If an SFP module is inserted, the corresponding RJ-45 jack is disabled.

Example: If an SFP module "PRP A" is inserted, the TP Interface "PRP A" has no function

Note

SCALANCE X200RNA

The networks LAN A and/or LAN B can have PROFINET or IRT functionality. These cannot, however, be transferred via the SCALANCE X200RNA because PRP does not support this. PRP functionality is not impaired by using PROFINET or IRT components in the LAN A and LAN B networks.

Article numbers

X204-2	with four 10/100 Mbps RJ-45 ports and two FO ports 6GK5 204-2BB10-2AA3	6GK5204-2BB10-2AA3
X204-2TS	with four 10/100 Mbps RJ-45 ports and two FO ports with extended temperature range and approval EN 50155 for rolling stock applications	6GK5204-2BB10-2CA2
X204-2LD	with four 10/100 Mbps RJ-45 ports and two FO ports long distance	6GK5204-2BC10-2AA3
X206-1	with six 10/100 Mbps RJ-45 ports and one FO port	6GK5206-1BB10-2AA3
X206-1LD	with six 10/100 Mbps RJ-45 ports and one FO port long distance	6GK5206-1BC10-2AA3
X208	with eight 10/100 Mbps RJ-45 ports	6GK5208-0BA10-2AA3
X208PRO	with eight 10/100 Mbps M12 ports, incl. eleven M12 dust caps, degree of protection IP65,	6GK5208-0HA00-2AA6
X212-2	with 12 10/100 Mbps RJ-45 ports and two FO ports	6GK5212-2BB00-2AA3
X212-2LD	with 12 10/100 Mbps RJ-45 ports and two FO ports with six 10/100 Mbps RJ-45 ports and one FO port long distance	6GK5212-2BC00-2AA3
X216	with 16 10/100 Mbps RJ-45 ports	6GK5216-0BA00-2AA3
X224	with 24 10/100 Mbps RJ-45 ports	6GK5224-0BA00-2AA3
XF204	4 x 10/100 Mbps RJ-45 ports electrical	6GK5204-0BA00-2AF2
XF204-2	4 x 10/100 Mbps RJ-45 ports electrical; 2 x 100 Mbps BFOC ports; optical (multimode, glass), up to max. 5 km	6GK5204-2BC00-2AF2
XF206-1	6 x 10/100 Mbps RJ-45 ports electrical, 1x 100 Mbps BFOC port optical (multimode, glass), up to max. 5 km	6GK5206-1BC00-2AF2
XF208	8 x 10/100 Mbps RJ-45 ports electrical	6GK5208-0BA00-2AF2

X200-4P IRT	4 x 100 Mbps POF/PCF SC RJ ports	6GK5200-4AH00-2BA3
X201-3P IRT	4 x 10/100 Mbps RJ-45 port, 3 x 100 Mbps POF/PCF SC RJ ports	6GK5201-3BH00-2BA3
X201-3P IRT PRO	4 x 10/100 Mbps RJ-45 port, 3 x 100 Mbps POF/PCF SC RJ ports	6GK5201-3BH00-2BA3
X202-2IRT	2 x 10/100 Mbps RJ-45 ports, 2 x 100 Mbps multimode BFOC ports	6GK5202-2BB00-2BA3
X202-2P IRT	4 x 10/100 Mbps RJ-45 ports, 2 x 100 Mbps POF/PCF SC RJ ports	6GK5202-2BH00-2BA3
X202-2P IRT PRO	1 x 10/100 Mbps RJ-45 push-pull ports, 2 x 100 Mbps POF/PCF SC RJ push-pull ports	6GK5202-2JR00-2BA6
X204IRT	4 x 10/100 Mbps RJ-45 ports	6GK5204-0BA00-2BA3
X204IRT PRO	4 x 10/100 Mbps RJ-45 push-pull ports	6GK5204-0JA00-2BA6
X204RNA	with four 10/100 Mbps RJ-45 ports	6GK5204-0BA00-2MB2
X204RNA EEC	with four 10/100 Mbps RJ-45 ports, of which 2 combo ports	6GK5204-0BS00-2NA3

4.4.8 SCALANCE X300

4.4.8.1 Description



Figure 4-13 SCALANCE X300



Figure 4-14 SCALANCE XR324-12M

The managed switches SCALANCE X300 from SIMATIC NET are for use in high-performance plant networks.

With the HSR redundancy function and standby coupling of rings, high network availability can be achieved. If the connection between these switches is interrupted, the IE switch SCALANCE X-300 used as the redundancy manager acts like a switch and in a very short time forms a linear bus from the ring with redundancy manager. As a result, a functional, end-to-end structure is restored.

Support of IT standards such as VLAN, RSTP, IGMP, and GARP makes seamless integration of automation networks in existing office networks possible.

The IE Sswitches SCALANCE X-300 and XR300 are designed for use in switching cubicles and cabinets. The X300 models have a robust metal housing with IP30 protection for installation on a DIN rail, an S7-300 standard rail or for wall mounting. The XR300 models are intended for installation in the 19" rack.

All devices have C-PLUG to back up the configuration data and a signaling contact. They are suitable for the use of a redundant power supply.

4.4.8.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	X310FE X306-1LD FE X320-1FE X320-3LD FE	X310X X307-3 X307-3LD X308-2 X308-2LD X308-2LH X308-2LH+ X308-2 X302-7EEC X307-2EEC	X308-2M XR324-12M XR324-4M EEC	X308-2M PoE
Modular design			•	•

Gigabit Ethernet		•	•	•
PoE Power over Ethernet				•
Diagnostics LED	•	•	•	•
Redundant power supply	•	•	•	•
On site display (Set button)	•	•	•	•
C-PLUG slot	•	•	•	•

- Suitable / available or according to the specified standard.

Functions

All devices have the following functions:

- PROFINET diagnostics
- SNMP / SNMP-supported diagnostics
- Topology support (LLDP)
- Command Line Interface
- Web-based management
- Configuration with STEP 7
- Ring redundancy including RM functionality
- Standby redundancy
- VLAN (Virtual Local Area Network)
- GVRP (Generic VLAN Registration Protocol)
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol)
- Passive listening
- IGMP snooping/querier (Internet Group Management Protocol)
- GMRP (Generic Multicast Protocol)
- Broadcast, Multicast, Unicast limiter
- Broadcast blocking
- Access Control List (ACL)
- IEEE 802.1x (Radius)
- Link aggregation

4.4.8.3 Interfaces

Table 4- 7

IE switch	Twisted pair			Fiber-optic cables				
	RJ-45 connectors 10 / 100 Mbps	RJ-45 connectors 10 / 100 / 1000 Mbps	RJ-45 connectors 10 / 100 / 1000 Mbps with PoE	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Max. seg- ment length / km	Multi- mode	Single mode
X304-2FE	4	-	-	2 (SC)	-	5	●	-
X306-1LD FE	6	-	-	1 (SC)	-	26	-	●
X307-3	7	-	-	-	3 (SC)	0.75	●	-
X307-3LD	7	-	-	-	3 (SC)	10	-	●
X308-2	7	1	-	-	2 (SC)	0.75	●	-
X308-2LD	7	1	-	-	2 (SC)	10	-	●
X308-2LH	7	1	-	-	2 (SC)	40	-	●
X308-2LH+	7	1	-	-	2 (SC)	70	-	●
X310	7	3	-	-	-	-	-	●
X310FE	10	-	-	-	-	-	-	-
X320-1FE	20	-	-	1	-	4** / 5***	●	-
X320-3LD FE	20	-	-	1	2 (SC)	5 / 26	●	●
X308-2M	-	4 and *	-	*	*	*	*	*
X308-2M TS	-	4 and *	-	*	*	*	*	*
XR324-12M	-	*	-	-	*	*	*	*
X308-2M PoE	-	-	4	*	*	*	*	*
XR324-4M PoE	-	8 and *	8	*	*	*	*	*
X302-7 EEC	-	2	-	7	-	4** / 5***	●	-
X307-2 EEC	5	2	-	2	-	4** / 5***	●	-

● Suitable / available or according to the specified standard.

* 2 x 100/1000 Mbps slots for 2-port media modules, electrical or optical.

** with a core diameter of 50 µm

*** with a core diameter of 62.5 µm

Article numbers

X304-2FE	2 x 100 Mbps, SC ports, optical (single mode glass), up to max. 26 km 4 x 10/100 Mbps RJ-45 ports, electrical	6GK5304-2BD00-2AA3
X306-1LD FE	1 x 100 Mbps SC port, optical (single mode glass), up to max. 26 km 6 x 10/100 Mbps RJ-45 ports, electrical	6GK5306-1BF00-2AA3
X307-3	3 x 1000 Mbps SC ports optical (multimode glass), up to max. 750 m 7 x 10/100 Mbps RJ-45 ports, electrical	6GK5307-3BL00-2AA3
X307-3LD	3 x 1000 Mbps, SC ports, optical (single mode glass), up to max. 10 km 7 x 10/100 Mbps RJ-45 ports, electrical	6GK5307-3BM00-2AA3
X308-2	2 x 1000 Mbps SC ports, optical (multimode glass), up to max. 750 m 1 x 10/100/1000 Mbps RJ-45 port, electrical, 7 x 10/100 Mbps RJ-45 ports, electrical	6GK5308-2FL00-2AA3
X308-2LD	2 x 1000 Mbps, SC ports, optical (single mode glass), up to max. 10 km 1 x 10/100/1000 Mbps RJ-45 port, electrical, 7 x 10/100 Mbps RJ-45 ports, electrical	6GK5308-2FM00-2AA3
X308-2LH	2 x 1000 Mbps, SC ports, optical (single mode glass), up to max. 40 km 1 x 10/100/1000 Mbps RJ-45 port, electrical, 7 x 10/100 Mbps RJ-45 ports, electrical	6GK5308-2FN00-2AA3
X308-2LH+	2 x 1000 Mbps, SC ports, optical (single mode glass), up to max. 70 km 1 x 10/100/1000 Mbps RJ-45 port, electrical, 7 x 10/100 Mbps RJ-45 ports, electrical	6GK5308-2FP00-2AA3
X310	3 x 10/100/1000 Mbps RJ-45 ports, electrical, 7 x 10/100 Mbps RJ-45 ports, electrical	6GK5310-0FA00-2AA3
X310FE	10 x 10/100 Mbps RJ-45 ports, electrical	6GK5310-0BA00-2AA3
X320-1FE	1 x 100 Mbps SC port optical (multimode, glass), up to max. 5 km 20 x 10/100 Mbps RJ-45 ports, electrical	6GK5320-1BD00-2AA3
X320-3LD FE	1 x 100 Mbps SC port optical (multimode, glass), up to max. 5 km 2 x 100 Mbps SC ports, optical (single mode glass) up to max. 26 km 20 x 10/100 Mbps RJ-45 ports, electrical	6GK5320-3BF00-2AA3
X308-2M	4 x 10/100/1000 Mbps RJ-45 ports, electrical 2 x 10/100/1000 Mbps slots for 2-port media modules, electrical or optical	6GK5308-2GG00-2AA2
X308-2M TS	4 x 10/100/1000 Mbps RJ-45 ports, electrical 2 x 10/100/1000 Mbps slots for 2-port media modules, electrical or optical, with extended temperature range and approval EN50155 for railway applications	6GK5308-2GG00-2CA2
X308-2M PoE	4 x 10/100/1000 Mbps RJ-45 ports with PoE, electrical, 2 x 10/100/1000 Mbps slots for 2-port media modules, electrical or optical	6GK5308-2QG00-2AA2

XR324-12M	Fully modular 19" Industrial Ethernet switches for setting up electrical and/or optical Industrial Ethernet networks, all can be fitted either with optical or electrical 2-port media modules) 12 x 10/100/1000 Mbps slots for 2-port media modules, electrical or optical	
	24 VDC power supply	
	Data cable outlet front	6GK5324-0GG00-1AR2
	Data cable outlet back	6GK5324-0GG00-1HR2
	110 to 230 VAC power supply	
	Data cable outlet front	6GK5324-0GG00-3AR2
	Data cable outlet back	6GK5324-0GG00-3HR2
XR324-4M PoE	Partially modular 19" Industrial Ethernet switches for setting up electrical and optical Industrial Ethernet networks, eight ports with Poe capability. can be fitted optionally with optical or electrical 2-port media modules 16 x 10/100/1000 Mbps RJ-45 ports of which eight support PoE, 4 x 10/100/1000 Mbps slots for 2-port media modules, electrical or optical	
	24 VDC power supply	
	Data cable outlet front	6GK5324-4QG00-1AR2
	Data cable outlet back	6GK5324-4QG00-1HR2
	110 to 230 VAC power supply	
	Data cable outlet front	6GK5324-4QG00-3AR2
	Data cable outlet back	6GK5324-4QG00-3HR2
X302-7 EEC	2 x 10/100/1000 Mbps RJ-45 ports, electrical; 7 x 100 Mbps LC ports, optical (multimode, glass) up to max.5 km Approval EN 50155 for railway applications	
	110 to 230 VAC power supply	
	1 power supply unit	6GK5302-7GD00-1EA3
	2 power supply units	6GK5302-7GD00-2EA3
	1 power supply unit with conformal coating	6GK5302-7GD00-1GA3
	2 power supply units with conformal coating	6GK5302-7GD00-2GA3
	110 to 230 VAC power supply	
	1 power supply unit	6GK5302-7GD00-3EA3
	2 power supply units	6GK5302-7GD00-4EA3
	1 power supply unit with conformal coating	6GK5302-7GD00-3GA3
	2 power supply units with conformal coating	6GK5302-7GD00-4GA3
X307-2 EEC	2 x 10/100/1000 Mbps RJ-45 ports, electrical; 7 x 100 Mbps LC ports, optical (multimode, glass) up to max.5 km Approval EN 50155 for railway applications	
	110 to 230 VAC power supply	
	1 power supply unit	6GK5307-2FD00-1EA3
	2 power supply units	6GK5307-2FD00-2EA3
	1 power supply unit with conformal coating	6GK5307-2FD00-1GA3
	2 power supply units with conformal coating	6GK5307-2FD00-2GA3

110 to 230 VAC power supply		
1 power supply unit		6GK5307-2FD00-3EA3
2 power supply units		6GK5307-2FD00-4EA3
1 power supply unit with conformal coating		6GK5307-2FD00-3GA3
2 power supply units with conformal coating		6GK5307-2FD00-4GA3

4.4.8.4 Media modules and SFP transceivers

Media modules

The use of media modules in partially and fully modular variants of the SCALANCE X-300 switches allows the expansion of networks by subsequently plugging in additional media modules in unused media module slots and allows a changeover of the cabling technology (the example change from copper to fiber-optic or from multimode to single mode fiber-optic cable).

Media module	Twisted pair		Fiber-optic cables				
	RJ-45 connectors 10 / 100 Mbps	RJ-45 connectors 10 / 100 / 1000 Mbps	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Max. segment length / km	Multi-mode	Single mode
MM991-2	-	-	2 (ST)	-	4* / 5**	•	-
MM991-2LD	-	-	2 (ST)	-	26	-	•
MM991-2	-	-	2 (SC)	-	4* / 5**	•	-
MM991-2LD	-	-	2 (SC)	-	26	-	•
MM991-2LH+	-	-	2 (SC)	-	70	-	•
MM992-2CUC	-	2	-	-	-	-	-
MM992-2CU	-	2	-	-	-	-	-
MM992-2SFP	-	2	-	-	-	-	-
MM992-2	-	-	-	2 (SC)	0.75	•	-
MM992-2LD	-	-	-	2 (SC)	10	-	•
MM992-2LH	-	-	-	2 (SC)	40	-	•
MM992-2LH+	-	-	-	2 (SC)	70	-	•
MM992-2ELH	-	-	-	2 (SC)	120	-	•

- Suitable / available or according to the specified standard.

* with a core diameter of 50 µm

** with a core diameter of 62.5 µm

SFP transceiver

The SFP transceiver (Small Form-factor Pluggable) can be used only in conjunction with the SFP media module MM992-2SFP.

SFP transceiver	Twisted pair		Fiber-optic cables				
	RJ-45 connectors 10 / 100 Mbps	RJ-45 connectors 10 / 100 / 1000 Mbps	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Max. segment length / km	Multi-mode	Single mode
SFP991-1	-	-	1 (LC)	-	4* / 5**	•	-
SFP991-1LD	-	-	1 (LC)	-	26	-	•
SFP991-1LH+	-	-	1 (LC)	-	70	-	•
SFP992-1	-	-	-	1 (LC)	0.75	•	-
SFP992-1LD	-	-	-	1 (LC)	10	-	•
SFP992-1LH	-	-	-	1 (LC)	40	-	•
SFP992-1LH+	-	-	-	1 (LC)	70	-	•
SFP992-1ELH	-	-	-	1 (LC)	120	-	•

- Suitable / available or according to the specified standard.

* with a core diameter of 50 µm

** with a core diameter of 62.5 µm

4.4.9 SCALANCE XM-400

4.4.9.1 Description



Figure 4-15 SCALANCE XM408-4C



Figure 4-16 SCALANCE XM408-8C



Figure 4-17 SCALANCE XM416-4C

The devices of the product group SCALANCE XM-400 provide both RJ-45 ports (1000 Mbps) as well as individual receptacles for pluggable transceivers. Each device can be expanded by port extenders, the maximum number of ports is 24. The main area of

application for these devices is in high-performance plant networks in which high port numbers and a high transmission rate are required. Normally, these devices are installed in a cabinet. There are device variants with and without layer 3 functionality. Devices without integrated layer 3 functionality can be retrofitted with a KEY-PLUG.

4.4.9.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	XM408-4C	XM408-8C	XM416-4C
Modular design	•	•	•
Gigabit Ethernet	•	•	•
PoE Power over Ethernet	-	-	-
Redundant power supply	•	•	•
Signaling contact	•	•	•
On site display (Set button)	•	•	•
Console port (1 x RS232)	•	•	•
Out-band port for on-site parameter assignment	•	•	•
C-PLUG slot	•	•	•

Functions

All devices have the following functions

- PROFINET diagnostics
- Topology support (LLDP)
- Command Line Interface / Telnet
- Web-based management
- Configuration with STEP 7
- SNMP
- Ring redundancy including RM functionality
- Standby redundancy
- VLAN (Virtual Local Area Network)
- GVRP (Generic VLAN Registration Protocol)
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol)
- Passive listening
- IGMP snooping/querier (Internet Group Management Protocol)

- GMRP (Generic Multicast Protocol)
- Broadcast, Multicast, Unicast limiter
- Broadcast blocking
- DHCP option 82 (Dynamic Host Configuration Protocol)
- Access control list (MAC)
- IEEE 802.1x (Radius)
- Link aggregation

Devices with layer 3 support and devices without integrated layer 3 support that are equipped with a KEY-PLUG also provide the following extra functions:

- Static IP routing
- RIPv2 (dynamic routing)
- OSPFv2 (dynamic routing)
- VRRP, router redundancy (Virtual Router Redundancy Protocol)

4.4.9.3 Interfaces

	XM408-4C	XM408-8C	XM416-4C
24 VDC supply	2 (redundant)	2 (redundant)	2 (redundant)
Signaling contact	1	1	1
Transmission speeds	10/100/1000 Mbps via RJ-45	10/100/1000 Mbps via RJ-45	10/100/1000 Mbps via RJ-45
Console port	1 x RS232	1 x RS232	1 x RS232
Out-band port for on-site parameter assignment	1 x RJ-45	1 x RJ-45	1 x RJ-45
RJ-45 ports	8	8	16
STP/SCP ports	4	-	-
SFP ports	-	8	4
Maximum number of port extenders	2	2	1
Maximum number of network interfaces	24	24	24

Article numbers

XM408-4C	8 RJ-45 ports, 4 pluggable transceiver slots, up to 2 port extenders, layer 3 with KEY-PLUG	6GK5408-4GP00-2AM2
	8 RJ-45 ports, 4 pluggable transceiver slots, up to 2 port extenders, layer 3 integrated	6GK5408-4GQ00-2AM2
XM408-8C	8 RJ-45 ports, 8 pluggable transceiver slots, up to 2 port extenders, layer 3 with KEY-PLUG	6GK5408-8GS00-2AM2
	8 RJ-45 ports, 8 pluggable transceiver slots, up to 2 port extenders, layer 3 integrated	6GK5408-8GR00-2AM2

XM416-4C	16 RJ-45 ports, 4 pluggable transceiver slots, max. 1 port extender, layer 3 with KEY-PLUG	6GK5416-4GS00-2AM2
	16 RJ-45 ports, 4 pluggable transceiver slots, max. 1 port extender, layer 3 integrated	6GK5416-4GR00-2AM2

4.4.9.4 Extender modules

Devices of the SCALANCE XM-400 series have an extension interface on the right side of the housing for optional extender modules. The following variants exist:



Figure 4-18 Extender module PE408



Figure 4-19 Extender module PE408PoE



Figure 4-20 Extender module PE400-8SFP

SCALANCE XM-400 basic devices are not capable of PoE. With the extender module PE408PoE, however, the XM-400 devices can be expanded with ports that allow a power supply via Ethernet.

Interfaces

	PE408	PE408PoE	PE400-8SFP
RJ-45 connectors 10 / 100 Mbps	8	-	-
RJ-45 connectors 10/100/1000 Mbps capable of PoE	-	8	-
SFP slots	-	-	8
Separate feed-in for PoE voltage	-	2	-

Article numbers

PE408	1 x 10/100/1000 Mbps RJ-45 ports	6GK5 408-0GA00-8AP2
PE408PoE	4 x 10/100/1000 Mbps, RJ-45 ports with PoE	6GK5 408-0PA00-8AP2
PE400-8SFP	8 x 10/100 Mbps, SFP ports	6GK5 400-8AS00-8AP2

4.4.9.5 SCALANCE PS-900



Figure 4-21 SCALANCE PS9230 PoE and SCALANCE PS924 PoE

Description

The power supply units of the SCALANCE PS-900 PoE series, were specially developed to supply the extender module PE408PoE with power. There are two product variants available:

- SCALANCE PS9230 PoE for 120/230 VAC input voltage
- SCALANCE PS924 PoE for 24 VDC input voltage

The devices with degree of protection IP20 can be used in ambient temperatures between - 40 °C und +70 °C. A SCALANCE PS-900 PoE supplies a maximum power of 86 W. To supply all eight ports of a PE408PoE with power two SCALANCE PS-900 PoE must therefore be connected.

Overview

	SCALANCE PS9230 PoE	SCALANCE PS924 PoE
Interfaces	Screw terminals PE/N/L for input voltage	Screw terminals FE/+/- for input voltage
	2 x 2 screw terminals +/- for output voltage	
	2 screw terminals for the signaling contact	
Electrical data		
Input voltage	85 ... 264 VAC at 47 ... 63 Hz	19.2 ... 28.8 VDC
Output voltage	48 ... 54 VDC, can be set	

	SCALANCE PS9230 PoE	SCALANCE PS924 PoE
Output effective power		86 W
Effective power loss		14 W
Permitted ambient conditions		
Operating temperature		-40 ... +70 °C
Transportation/storage temperature		-40 ... +85 °C
Relative humidity at 25 °C		95%
Degree of protection		IP20
Standards and approvals		
Approvals	cULus listed (UL508, CSA C22.2 No. 107.1) EN 61000-6-4: 2007 EN 61000-6-2 EN 61000-6-4: 2007 CE mark C-Tick	

Article numbers

SCALANCE PS9230 PoE	PoE power supply for SCALANCE XM-400 with input voltage 230 VAC	6GK5923-0PS00-3AA2
SCALANCE PS924 PoE	PoE power supply for SCALANCE XM-400 with input voltage 24 VDC	6GK5924-0PS00-1AA2

4.4.10 SCALANCE X500

4.4.10.1 Description



Figure 4-22 SCALANCE XR500

SCALANCE XR500 switches are ideal for use in industrial networks and for integrating the industrial network in an existing enterprise network. From the control level to the management level, the switch handles the networking of both plant sections and distributed

field devices and ensures high plant availability with wide-ranging diagnostics options and high transmission speeds. Due to the scalability of the basic device and optionally available layer 3 functions, the network can be set up specially for relevant application or adapted and expanded at any time. SCALANCE XR500 switches are suitable for setting up electrical and optical Industrial Ethernet linear bus, star or ring structures. With transmission rates up to 10 Gbps, the switches can be used as Industrial Ethernet backbone switches and as hubs in the plant bus (redundant connection possible).

Apart from four integrated SFP+ slots (for SFP+ transceivers) (10 Gbps) or SFP transceivers (1000 Mbps) the device variants XR528-6M and XR552-12M provide six or 12 media module slots. These can be fitted with electrical and/or optical 4-port media modules. Using media modules or SFP+/SFP allows:

- Expansion of networks by adding additional media modules in unused media module slots
- Replacement of the cabling technology, for example converting from copper to FO cable or from multimode to single mode FO cable
- The transmission rate to be changed, e.g. from 1000 Mbps to 10 Gbps

With their low height of one height unit, the device variants XR524-8C and XR526-8C require little space in the cabinet. Both devices are suitable for fanless operation and redundant power supply. Eight of the twenty four ports are designed as combo ports, they can have pluggable transceivers fitted therefore providing electrical or optical interfaces as required.

4.4.10.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	XR552-12M XR528-5M	XR524-8C XR526-8C
Modular design	•	-
Combo ports	-	•
Gigabit Ethernet	•	•
10 Gigabit Ethernet	•	•
PoE Power over Ethernet	•	-
Diagnostics LED	•	•
Redundant power supply	•	•
On site display (Set button)	•	•
C-PLUG slot	•	•

- Suitable / available or according to the specified standard.

Functions

All devices have the following functions:

- PROFINET diagnostics
- SNMP / SNMP-supported diagnostics
- Topology support (LLDP)
- Command Line Interface
- Web-based management
- Configuration with STEP 7
- Ring redundancy including RM functionality
- Standby redundancy
- IRT capability
- VLAN (Virtual Local Area Network)
- GVRP (Generic VLAN Registration Protocol)
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol)
- Passive listening
- IGMP snooping/querier (Internet Group Management Protocol)
- GMRP (Generic Multicast Protocol)
- Broadcast, Multicast, Unicast limiter
- Broadcast blocking
- Access Control List (ACL)
- IEEE 802.1x (Radius)
- Link aggregation
- Static IP routing
- RIPv2 (dynamic routing)
- OSPFv2 (dynamic routing)
- VRRP, router redundancy (Virtual Router Redundancy Protocol)

4.4.10.3 Interfaces

Table 4- 8

IE switch	Number of ports	Pluggable transceiver slots		Number of combo ports	Number of slots for media modules
		SFP	SFP+		
XR524-8C	24	8	-	8	-
XR526-8C	26	8	2	8	-
XR528-6M	28	-	4	-	6
XR552-12M	52	-	4	-	12

Article numbers

Device	Properties	Layer 3	Power supply	Article number
XR524-8C	1 height unit. 8 integrated 1/10 Gbps SFP slots as combo ports, 24 RJ-45 ports.	KEY-PLUG	2 x 24 VDC Connectors on front	6GK5524-8GS00-2AR2
			1 x 100 to 240 VAC Connector on rear	6GK5524-8GS00-3AR2
			2 x 100 to 240 VAC Connectors on rear	6GK5524-8GS00-4AR2
		Integrated	2 x 24 VDC Connectors on front	6GK5524-8GR00-2AR2
			1 x 100 to 240 VAC Connector on rear	6GK5524-8GR00-3AR2
			2 x 100 to 240 VAC Connectors on rear	6GK5524-8GR00-4AR2
XR526-8C	1 height unit. 8 integrated 1/10 Gbps SFP slots as combo ports, 2 SFP+ slots, 24 RJ-45 ports.	KEY-PLUG	2 x 24 VDC Connectors on front	6GK5526-8GS00-2AR2
			1 x 100 to 240 VAC Connector on rear	6GK5526-8GS00-3AR2
			2 x 100 to 240 VAC Connectors on rear	6GK5526-8GS00-4AR2
		Integrated	2 x 24 VDC Connectors on front	6GK5526-8GR00-2AR2
			1 x 100 to 240 VAC Connector on rear	6GK5526-8GR00-3AR2
			2 x 100 to 240 VAC Connectors on rear	6GK5526-8GR00-4AR2

Device	Properties	Layer 3	Cable outlet	Article number
XR528-6M	2 height units. 4 integrated 1/10 Gbps SFP+ slots for SFP or SFP+ transceivers; 6 x 10/100/1000 Mbps slots for 4-port media modules, electrical or optical.	KEY-PLUG	Front	6GK5528-0AA00-2AR2
			Back	6GK5528-0AA00-2HR2
		Integrated	Front	6GK5528-0AR00-2AR2
			Back	6GK5528-0AR00-2HR2
XR552-12M	3 height units. 4 integrated 1/10 Gbps SFP+ slots for SFP or SFP+ transceivers; 12 x 10/100/1000 Mbps slots for 4-port media modules, electrical or optical.	KEY-PLUG	Front	6GK5552-0AA00-2AR2
			Back	6GK5552-0AA00-2HR2
		Integrated	Front	6GK5552-0AR00-2AR2
			Back	6GK5552-0AR00-2HR2

Media modules

The use of media modules with the IE switches SCALANCE X-500 allows the expansion of networks by subsequently plugging in additional media modules in unused media module slots and allows a changeover of the cabling technology (for example changing from copper to fiber-optic or from multimode to single mode fiber-optic cable).

Media module	Twisted pair	Fiber-optic cables					
	RJ-45 connectors 10 / 100 / 1000 Mbps	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Fiber-optic ports 10 000 Mbps	Max. segment length / km	Multi-mode	Single mode
MM992-4	-	-	4 (SC)	-	4* / 5**	•	-
MM992-4CU	4	-	-	-	-	-	-
MM992-4CUC	4 ¹⁾	-	-	-	-	-	-
MM992-4LD	-	-	4 (SC)	-	10	-	•
MM992-4PoEC	4 ¹⁾	-	-	-	-	-	-
MM992-4PoE	4	-	-	-	-	-	-
MM992-4SFP	-	4 (LC) ²⁾	4 (LC) ²⁾	4 (LC) ²⁾		•	•
MM991-4	-	-	4 (SC)	-	4* / 5**	•	-
MM991-4LD	-	-	4 (SC)		10	-	•

• Suitable / available or according to the specified standard.

* with a core diameter of 50 µm

** with a core diameter of 62.5 µm

¹⁾ Securing collar

²⁾ the SFP slot module can hold a total of maximum 4 x 1-port SFP modules

SFP transceiver

The SFP transceiver (Small Form-factor Pluggable) can be used only in conjunction with the SFP media module MM992-2SFP.

Media modules	Fiber-optic cables					
	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Fiber-optic ports 10 000 Mbps	Max. segment length / km	Multi-mode	Single mode
SFP991-1 ¹⁾	1 (LC)	-	-	4* / 5**	•	-
SFP991-1LD ¹⁾	1 (LC)	-	-	26	-	•
SFP991-1LH ¹⁾	1 (LC)	-	-	26	-	•
SFP992-1 ^{1) 2)}	-	1 (LC)	-	0.75	•	-

Media modules	Fiber-optic cables					
	Fiber-optic ports, 100 Mbps	Fiber-optic ports, 1000 Mbps	Fiber-optic ports 10 000 Mbps	Max. segment length / km	Multi-mode	Single mode
SFP992-1LD ^{1) 2)}	-	1 (LC)	-	10	-	•
SFP992-1LH ^{1) 2)}	-	1 (LC)	-	40	-	•
SFP992-1LH+ ^{1) 2)}	-	1 (LC)	-	70	-	•
SFP992-1ELH ^{1) 2)}	-	1 (LC)	-	120	-	•
SFP993-1 ²⁾	-	-	1 (LC)	0.3	•	-
SFP993-1LD ²⁾	-	-	1 (LC)	10	-	•
SFP993-1L ²⁾	-	-	1 (LC)	40	-	•

• Suitable / available or according to the specified standard.

* with a core diameter of 50 µm

** with a core diameter of 62.5 µm

¹⁾ can only be plugged in combined with the slot module MM992-4SFP

²⁾ can only be plugged into XR-500 SFPplus slots

Optional external power supply units

Optional external power supply units are available to supply power to the switches of the SCALANCE X-500 series. You can create a redundant power supply by installing two power supply units for one switch in the rack.



Figure 4-23 SCALANCE X-500 power supply unit

Connectors

Type	Power	Input voltage	Output voltage
PS598-1	300 W	100 to 240 VAC	24 VDC

Note**Two connectors for the 24 VDC output voltage**

The PS598-1 has two connectors with the output voltage 24 VDC. Note that you can only use one connector on the front or the connector on the rear of the PS598-1. You cannot operate the device with the connectors on the front and rear at the same time.

Note**Requirement for connecting at the rear**

Note that the connector on the rear of the PS598-1 can only be used if the power supply is mounted on the SCALANCE XR-500M.

Note**Replacing the filter mat**

To replace the filter mat, use the material Viledon P 15/150 G2 EN 779. The dimensions of the filter mat are 38 x 135 x 8 mm (H x W x D).

4.5 SCALANCE W components for Industrial Wireless LAN

4.5.1 SCALANCE W devices

Introduction

All SCALANCE W products were developed specially for industrial use. Thanks to the robust housing and high reliability in data transmission, the devices are suitable for all sectors and applications. With most of the devices, the power supply can also be via Power over Ethernet. This allows these devices to be integrated in an existing infrastructure without additional cabling. The accessories such as antennas, power supply units and cabling are also part of this concept and produced to be suitable for industry. The exchangeable media C-PLUG (configuration plug) and KEY-PLUG store project engineering and configuration data which makes device replacement possible in a short time without specially trained personnel. This minimizes downtimes and saves training costs. Over and above this, the KEY-PLUG releases further device properties (known as "iFeatures").

To protect against unauthorized access, the products provide modern standard mechanisms for user identification (authentication) and encryption of data, and can be easily integrated into existing security concepts at the same time.

With the international standard IEEE 802.11n wireless communication becomes even more robust. The greatest advantage results from the use of multipath propagation (Multiple Input, Multiple Output (MIMO)). This makes it possible for the devices to use multiple antennas at the same time. This achieves a higher data rate and at the same time reduces the susceptibility to disturbances in environments with a lot of reflections.

- Access points

Access points are the central base stations for infrastructure networks. They coordinate and control the wireless traffic within a wireless cell. If there are two or more access points in a wireless network, i.e. same wireless network name (SSID), the client module can move between the wireless cells formed by the individual access points (roaming). The wireless connection is retained during roaming. This technique is used when the required wireless coverage is greater than the distance that can be covered by a single access point. All access points can also be configured so that they are restricted to client functionality.

- Client modules

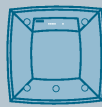
Client modules of the SCALANCE W product line are used as gateways between wireless and wired network segments (bridge function). Normally, they communicate with an access point (infrastructure network). All access points - except the controller access points - can also be configured as client modules.

- WLAN controller

The IWLAN controller SCALANCE W product line manages and coordinates controller-based access points.

Overview of the performance classes of the SCALANCE W devices

The following overview graphic provides you with a summary of the performance classes covered by the various SCALANCE W devices.

	Access Points	Client Modules
For outdoors	W786-1 RJ45 W786-2 RJ45 W786-2IA RJ45 W786-2 SFP W786C-2 RJ45 W786C-2IA RJ45 W786C-2 SFP 	
For indoors	W788-1 M12 W788-2 M12 W788-2 M12 EEC W788C-2 M12 W788C-2 M12 EEC  	W748-1 M12  
For the control cabinet	W788-1 RJ45 W788-2 RJ45 W788C-2 RJ45  	W748-1 RJ45  
	W774-1 RJ45 W774-1 M12 EEC  	W734-1 RJ45  
	W761-1 RJ45 	W722-1 RJ45 W721-1 RJ45 

 The KEY-PLUG symbol identifies devices which have the "iFeatures" functionality available when the optional KEY-PLUG is inserted. The device variants W786 and W722 have the "iFeatures" as default.

Figure 4-24 Overview of the SCALANCE W network components

Example of a topology

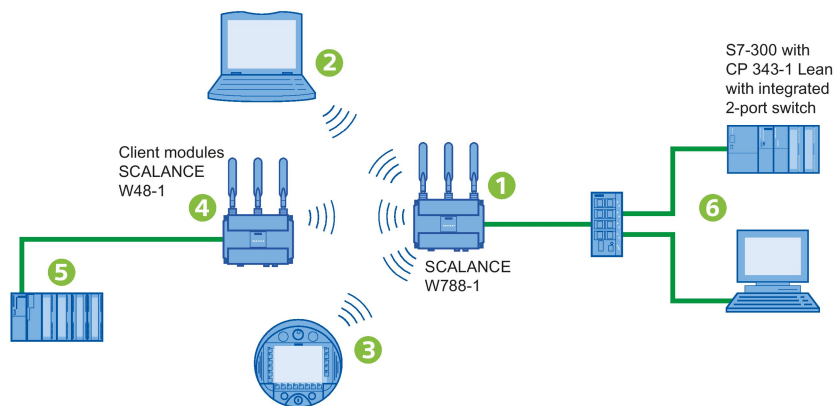


Figure 4-25 Example of an infrastructure network:
A SCALANCE W788 ① adopts the function of the access point. Mobile nodes such as PC/PG with IWLAN card ②, IWLAN control panels ③ or WLAN clients ④ and their nodes ⑤ can communicate with each other or exchange data with stationary nodes ⑥.

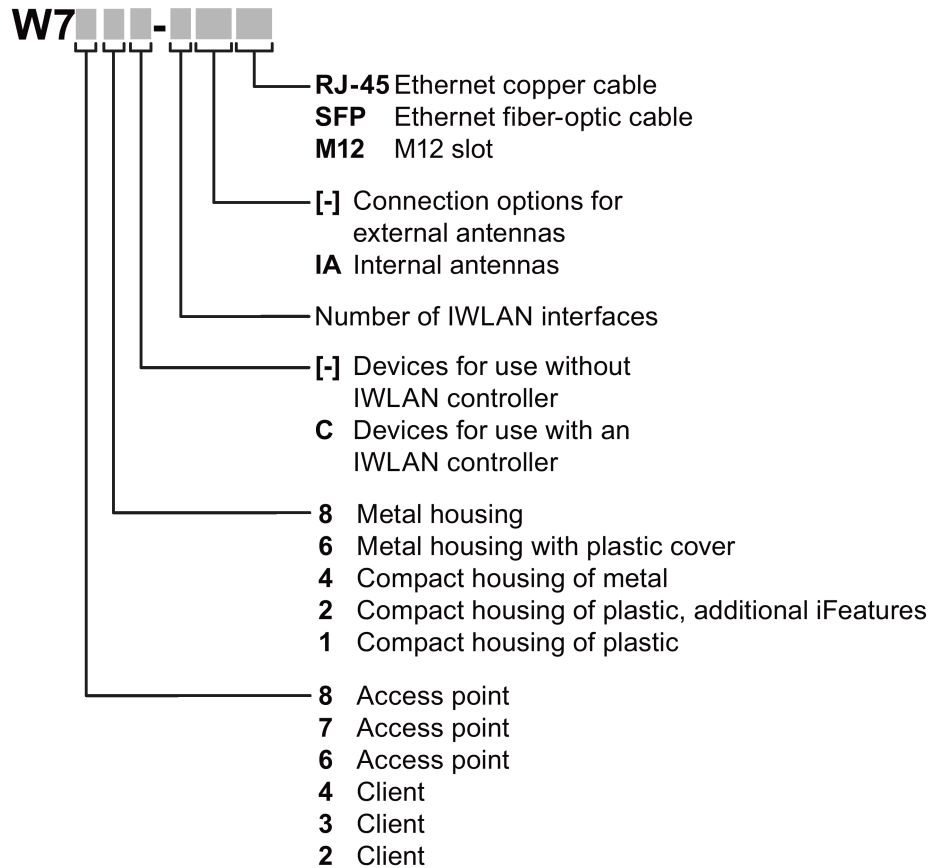
Note

In the online help of the Web-Based Management, you will find further information on the configuration parameters of the particular SCALANCE W devices.

4.5.2 Type designations

Identify the SCALANCE W devices based on their type key. The design and basic properties can be identified based on the following type key.

Type designations for SCALANCE W devices complying with IEEE 802.11a/b/g/n



4.5.3 Functions of WLAN devices

Introduction

This section describes certain functions of SCALANCE W devices. For further information on all the functions, refer to the operating instructions of the individual devices or the configuration manual.

Authentication and encryption

Authentication and encryption protect a network from unauthorized access. This is achieved by an exchange of keys or certificates between client and server. There are various methods that are explained in detail in the SCALANCE W700 configuration manual and in the section "Encryption and data security (Page 50)".

Support of IEEE 802.11n

With SCALANCE W700 devices that support IEEE 802.11n, a data throughput up to 450 Mbps (gross) is possible depending on the version. You will find detailed information in the section "IEEE 802.11n (Page 46)". These devices also support the following functions:

- Frame aggregation
- Shortened guard interval
- Channel bonding

SCALANCE W devices as bridges

A bridge is a network component that connects two networks. A bridge is not dependent on the protocol; management of the data packages is based on the physical address of the network nodes, the MAC address. The SCALANCE W provides bridge functionality for handling data exchange between wired and wireless Ethernet.

- **Learning Table**

SCALANCE W devices log the information about which MAC address can be reached over which port in a learning table.

- **NAPT: Network Address Port Translation**

With Network Address Port Translation (NAPT) or Port Address Translation (PAT), several internal source IP addresses are translated into the same external source IP address. This function is only available on clients in client mode.

Special functions for industrial applications

The following functions are used especially in an industrial environment:

- **IPCF: Industrial Point Coordination Function**

iPCF is the functional expansion of the IEEE 802.11 standard for applications requiring real time and a deterministic response (predictable reply times). This allows Rapid Roaming of mobile nodes from one RF field to the next. Wireless and secure PROFINET IO communication is also supported with the SIMATIC Mobile Panel 277F IWLAN.

- **IPCF-MC: IPCF Management Channel**

The iPCF Management Channel, iPCF MC, is a further development of iPCF. This mode should be used when IWLAN nodes that also support iPCF MC are moving freely in the RF field. This method is particularly suitable when using omnidirectional antennas, when deterministic data needs to be exchanged.

4.5.4 SCALANCE W760/W720

4.5.4.1 Description



Figure 4-26 SCALANCE W761-1 RJ-45 access point

The devices of the SCALANCE W760/W720 product line have a plastic housing in SIMATIC ET200 design, and are intended for installation in a cabinet. Due to their compact space-saving design, they are particularly suitable for applications in which IWLAN needs to be integrated cost-effectively in a device. The client module SCALANCE W722-1 RJ-45 provides support of the iFeatures and is therefore suitable for real-time applications such as PROFINET IO. The access point SCALANCE W761-1 RJ45 can also be operated as a client module.

The following variants exist:

- SCALANCE W761-1 RJ-45 access point
- SCALANCE W721-1 RJ-45 Ethernet Client Module
- SCALANCE W722-1 RJ-45 Ethernet Client Module with support of the iFeatures

4.5.4.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

Table 4- 9

Functionality	W761-1 RJ-45 W722-1 RJ-45 W721-1 RJ-45
PoE Power over Ethernet (IEEE 802.3at Type 1, previously IEEE 802.3af)	-

Redundant power supply	-
Digital input / digital output	-
C-PLUG slot	-
IP degree of protection	IP20
Operating temperature minimum [°C]	0
Operating temperature maximum [°C]	+55
Resistant to condensation	-
Resistant to salt water spray	-
Use in EX Zone 2 ¹⁾	•
IEEE 802.11 a/b/g/n	•
Number of supported IP nodes	4
Number of supported MAC nodes	4

- Suitable / available or according to the specified standard.

Functions

All devices have the following functions:

- Support of forced roaming
- SSH / HTTPS / admin password
- WEP / WPA / WPA2
- IEEE 802.11i, Hidden SSID
- IEEE 802.1X (RADIUS)
- EAP-TLS, EAP-TTLS, PEAP
- NAT / NAPT
- iQoS: industrial Quality of Service
- IEEE 802.11e (QoS/WMM)
- STP / RSTP (IEEE 802.1d/w)
- WDS (Wireless Distribution System)
- VLANs (Multi-SSID)
- PROFINET IO diagnostics
- SNMP
- Syslog

The SCALANCE W722-1 also has the following functions:

- iPCF
- iPCF-MC

4.5.4.3 Interfaces

Table 4- 10

Functionality	W761-1 RJ-45 W721-1 RJ-45 W722-1 RJ-45
Number of wireless interfaces	1
Connectors for external antennas	1 (R-SMA connector female)
Number and type of the Ethernet interfaces	1 x RJ-45

Article numbers

Table 4- 11

W761-1 RJ-45	Ethernet interface RJ-45, 1 external antenna	6GK5761-1FC00-0AA0 6GK5761-1FC00-0AB0 ¹⁾
W721-1 RJ-45	Ethernet interface RJ-45, 1 external antenna	6GK5721-1FC00-0AA0 6GK5721-1FC00-0AB0 ¹⁾
W722-1 RJ-45	Ethernet interface RJ-45, 1 external antenna	6GK5722-1FC00-0AA0 6GK5722-1FC00-0AB0 ¹⁾

¹⁾ US variant

4.5.5 SCALANCE W770/W730

4.5.5.1 Description



Figure 4-27 SCALANCE W774-1 RJ-45 access point

The devices of the SCALANCE W770/W730 product line have a metal housing in SIMATIC S7-1500 and ET 200MP design and are intended for installation in a cabinet. Since the devices support MIMO 2x2 antenna technology, they are also suitable for applications with

high requirements for reliability. A redundant power supply is also possible as is Power over Ethernet. With the optionally available KEY-PLUG, real-time data transfer is also possible.

The following variants exist:

- SCALANCE W774-1 RJ-45 access point
- SCALANCE W774-1 M12 EEC access point with M12 connector sockets
- SCALANCE W734-1 RJ-45 client module

4.5.5.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

Table 4- 12

Functionality	W774-1 RJ-45 W734-1 RJ-45	W774-1 M12 EEC
PoE Power over Ethernet (IEEE 802.3at Type 1, previously IEEE 802.3af)	•	•
Redundant power supply	•	•
Digital input / digital output	-	-
PLUG slot	•	•
IP degree of protection	IP30	IP30
Operating temperature minimum	-20 °C	-20 °C
Operating temperature maximum	+60 °C	+65 °C
Conformal coating	-	•
Resistant to condensation	-	•
Resistant to salt water spray	-	-
Use in EX Zone 2 ¹⁾	•	•
IEEE 802.11 a/b/g/n	•	•
Number of supported IP nodes	8	8
Number of supported MAC nodes	8	8

- Suitable / available or according to the specified standard.

Functions

All devices have the following functions:

- Support of forced roaming
- SSH / HTTPS / admin password
- WEP / WPA / WPA2

- IEEE 802.11i, Hidden SSID
- IEEE 802.1X (RADIUS)
- EAP-TLS, EAP-TTLS, PEAP
- NAT / NAPT
- iQoS: industrial Quality of Service
- IEEE 802.11e (QoS/WMM)
- STP / RSTP (IEEE 802.1d/w)
- WDS (Wireless Distribution System)
- VLANs (Multi-SSID)
- PROFINET IO diagnostics
- SNMP
- Syslog

With the optionally available KEY-PLUG, the following functions can be used:

- iPCF
- iPCF-MC

4.5.5.3 Interfaces

Table 4- 13

Functionality	W774-1 RJ-45 W734-1 RJ-45	W774-1 M12 EEC
Number of wireless interfaces	1	1
Connectors for external antennas	2 (R-SMA connector female)	2 (R-SMA connector female)
Number and type of Ethernet interface	2 x RJ-45	2 x M12

Article numbers

Table 4- 14

W774-1 RJ-45	Ethernet interface RJ-45, 2 external antennas	6GK5774-1FX00-0AA0 6GK5774-1FX00-0AB0 ¹⁾
W774-1 M12 EEC	Ethernet interface M12, 2 external antennas	6GK5774-1FY00-0TA0 6GK5774-1FY00-0TB0
W734-1 RJ-45	Ethernet interface RJ-45, 2 external antennas	6GK5734-1FX00-0AA0 6GK5734-1FX00-0AB0

¹⁾ US variant

4.5.6 SCALANCE W788/W748

4.5.6.1 Description

Description



Figure 4-28 SCALANCE W788 M12 access point

The access points W788-x RJ45/W788-x M12 and the client modules W748-1 RJ45/W748-1 M12 support the standard IEEE 802.11a/b/g/n. These devices are intended to set up Industrial Wireless LAN (IWLAN) wireless networks for 2.4 GHz or 5 GHz.

The devices SCALANCE W788/W748 use three data streams and therefore achieve data rates up to 450 Mbps. The high data rate is achieved among other things by channel bonding and by 3 x 3 MIMO technology (Multiple Input, Multiple Output), see section IEEE 802.11n (Page 46) The devices each use three data streams for the simultaneous send and receiving of wireless signals.

The access points SCALANCE W788-x RJ-45 and the client module SCALANCE W748-1 RJ-45 are particularly suitable for applications in which the access point is to be installed in the cabinet. The robust aluminum housing of the SCALANCE W788 RJ-45 devices in degree of protection IP30 provides protection from mechanisms and electromagnetic loads and is a cost-effective alternative for use in indoors.

The access points SCALANCE W788-x M12 and the client module SCALANCE W748-1 M12 can be installed at locations with suitable wireless properties indoors also outside the cabinet. The housing with degree of protection IP65 and the connectors withstand high loads caused by shock and vibration since all connections are screwed or lock in place.

The access point SCALANCE W788-2 M12 EEC also has an extended temperature range and conformal coating. The maximum ambient temperature for operation of this device is 70 °C.

4.5.6.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

Table 4- 15

	<i>Access point</i> W788-1 RJ-45 W788-2 RJ-45 <i>Client modules</i> W748-1 RJ-45	<i>Access point</i> W788-1 M12 W788-2 M12 <i>Client modules</i> W748-1 M12	<i>Access point</i> W788-2 M12 EEC
PoE (Power-over-Ethernet) IEEE 802.3at Type 1, previously IEEE 802.3af.	•	•	•
Redundant power supply	•	•	•
Digital input / digital output	•	-	-
C-PLUG/KEY-PLUG slot	•	•	•
IP degree of protection	IP30	IP65	IP65
Operating temperature minimum	-20 °C	-20 °C	-40 °C
Operating temperature maximum	+60 °C	+60 °C	+70 °C
Conformal coating	-	-	•
Resistant to condensation	-	-	•
Resistant to salt water spray	-	-	-
UV resistant	-	-	-
Use in EX Zone 2 ¹⁾	•	•	•
IEEE 802.11a/b/g/n	•	•	•
IEEE 802.11n MIMO (input x output streams)	3 x 3	3 x 3	3 x 3

• Suitable / available or according to the specified standard.

¹⁾ Note installation instructions

Functions

All devices have the following functions:

- SSH / HTTPS / admin password
- WEP / WPA / WPA2
- IEEE 802.11i, Hidden SSID
- IEEE 802.1x (RADIUS)
- EAP-TLS, EAP-TTLS, PEAP
- PROFINET IO diagnostics
- SNMP
- Syslog

The access points also have the following functions:

- Support of forced roaming
- IEEE 802.11e (QoS/WMM)
- STP / RSTP (IEEE 802.1d/w)
- WDS (Wireless Distribution System)
- Operation possible as IWLAN client
- VLANs (Multi-SSID)

With the optionally available KEY-PLUG, the following functions can be used:

- iPCF
- iPCF-MC

4.5.6.3 Interfaces

Table 4- 16

Functionality	W788-1 RJ-45 W748-1 RJ-45	W788-2 RJ-45	W788-1 M12 W748-1 M12	W788-2 M12 W788-2 M12 EEC
WLAN interface	1	2	1	2
Internal antennas	-	-	-	-
Connectors for external antennas	3 R-SMA female	6 R-SMA female	3 N-Connect female	6 N-Connect female
Number and type of Ethernet interface	1 x RJ-45, incl. PoE	1 x RJ-45, incl. PoE	1 x M12 (X-coded), incl. PoE	1 x M12 (X-coded), incl. PoE

Article numbers

Table 4- 17 Access points

W788-1 RJ-45 ²⁾	Ethernet interface RJ-45, 3 external antennas	6GK5788-1FC00-0AA0 6GK5788-1FC00-0AB0 ¹⁾
W788-2 RJ-45 ³⁾	Ethernet interface RJ-45, 6 external antennas	6GK5788-2FC00-0AA0 6GK5788-2FC00-0AB0 ¹⁾
W788-1 M12 ²⁾	Ethernet interface M12, 3 external antennas	6GK5788-1GD00-0AA0 6GK5788-1GD00-0AB0 ¹⁾
W788-2 M12 ³⁾	Ethernet interface M12, 6 external antennas	6GK5788-2GD00-0AA0 6GK5788-2GD00-0AB0 ¹⁾
W788-2 M12 EEC ³⁾	Ethernet interface M12, 6 external antennas	6GK5788-2GD00-0TA0 6GK5788-2GD00-0TB0 ¹⁾

¹⁾ US variant ²⁾ One integrated wireless card ³⁾ Two integrated wireless cards

Table 4- 18 Client modules

W748-1 RJ-45	Ethernet interface RJ-45, 3 external antennas	6GK5748-1FC00-0AA0 6GK5748-1FC00-0AB0 ¹⁾
W748-1 M12	Ethernet interface M12	6GK5748-1GD00-0AA0 6GK5748-1GD00-0AB0 ¹⁾

¹⁾ US variant

4.5.7 SCALANCE W786

4.5.7.1 Description



Figure 4-29 SCALANCE W788 access point

SCALANCE W786 access points according to IEEE 802.11n

SCALANCE W786 products are intended for applications with high mechanical loads, for example outdoors or when the installation location is open to the public. The functions correspond to the IEEE 802.11a/b/g/n standards.

The access points are designed for ruggedness. No parts that can be damaged are led out of the devices. The SCALANCE W786 devices have a housing that is resistant to impact and shock and tensile compression.

The SCALANCE W786-1 RJ-45 device type is equipped with a wireless card, SCALANCE W786-2 RJ-45 with two wireless cards. The access point SCALANCE W786-2 RJ-45 also exists with six internal antennas.

The SCALANCE W786-2 SFP access point is very variable due to the use of pluggable transceivers, and can be used for various transmission media. Two wireless cards are integrated in the device.

4.5.7.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	W786-1 RJ-45 W786-2 RJ-45 W786-2IA RJ-45	W786-2 SFP
PoE (Power-over-Ethernet) IEEE 802.3at Type 1, previously IEEE 802.3af.	•	-
Redundant power supply	•	•
Digital input / digital output	-	-
C-PLUG slot	•	•
IP degree of protection	IP65	IP65
Operating temperature minimum	-40 °C	-40 °C
Operating temperature maximum	+60 °C	+60 °C
Resistant to condensation	•	•
Resistant to salt water spray	•	•
UV resistant	•	•
Use in EX Zone 2 ¹⁾	•	•
IEEE 802.11a/b/g/n	•	•

- Suitable / available or according to the specified standard.

¹⁾ Note installation instructions

Functions

All devices have the following functions:

- SSH / HTTPS / admin password
- WEP / WPA / WPA2
- IEEE 802.11i, Hidden SSID
- IEEE 802.1x (RADIUS)
- EAP-TLS, EAP-TTLS, PEAP
- IEEE 802.11e (QoS/WMM)
- STP / RSTP (IEEE 802.1d/w)
- WDS (Wireless Distribution System)
- Operation possible as IWLAN client
- VLANs (Multi-SSID)
- PROFINET IO diagnostics
- SNMPv1/v2/v3
- Syslog

- Support of forced roaming
- Wireless redundancy between access points
- Operation as IWLAN client
- NAT / NAPT

With the optionally available KEY-PLUG, the following functions can be used:

- iPCF
- iPCF-MC

4.5.7.3 Interfaces

	W786-1 RJ-45 W786-2 RJ-45	W786-2 SFP	W786-2IA RJ-45
Number of wireless interfaces	1 – 2	2	2
Connectors for external antennas	3 – 6	6	-
Internal antennas	-	-	6
Type and number of Ethernet interfaces	1 x RJ-45	2 x SFP	1 x RJ-45

Article numbers

W786-1 RJ-45	Ethernet interface RJ-45, 3 external antennas	6GK5786-1FC00-0AA0 6GK5786-1FC00-0AB0 ¹⁾
W786-2 RJ-45	Ethernet interface RJ-45, 6 external antennas	6GK5786-2FC00-0AA0 6GK5786-2FC00-0AB0 ¹⁾
W786-2IA RJ-45	Ethernet interface RJ-45, 6 internal antennas	6GK5786-2HC00-0AA0 6GK5786-2HC00-0AB0 ¹⁾
W786-2 SFP	SFP slot, 6 external antennas	6GK5786-2FE00-0AA0 6GK5786-2FE00-0AB0 ¹⁾

¹⁾ US variant

4.5.8 SCALANCE WLC711, W788C and W786C

4.5.8.1 Description

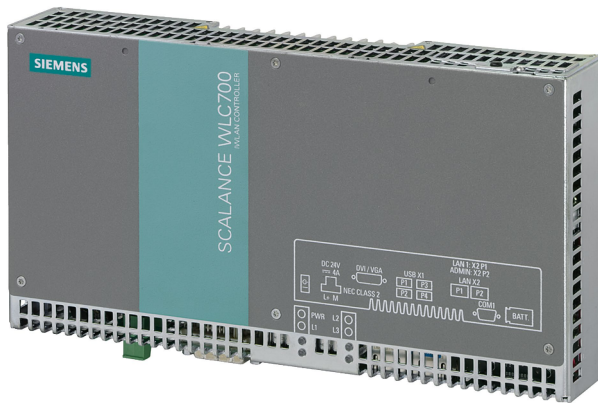


Figure 4-30 SCALANCE WLC711

The IWLAN controller SCALANCE WLC711 as the central station handles the management of wireless networks. The controller provide support when commissioning, during diagnostics, access checks and the security settings of the wireless network and when the firmware of the access points is updated. This reduces effort and costs during commissioning and operation of larger IWLAN installations. Only controller-based access points can be used with the controller.

The redundant operation of two IWLAN controllers increases the availability of the communications network.

The device with degree of protection IP20 is licensed for the connection of up to 16 controller-based access points of the SCALANCE W78xC product line, of the SCALANCE W786-2HPW according to IEEE 802.11n and IEEE 802.11a/ b/ g.

By licensing, this function can be extended to 48 or 96 (redundancy) access points in standard operation. New access points are detected automatically.

Der SCALANCE IWLAN controller WLC711 also supports:

- Up to 64 access points in redundant operation with two IWLAN controllers.
- Up to 512 WLAN clients
- Up to 8 logical service-based networks (Virtual Network Services)

Controller-based access points SCALANCE W788C and W786C

The device SCALANCE W788C-2 RJ-45 with degree of protection IP30 just like all other controller access points is intended for setting up Industrial Wireless LAN (IWLAN) wireless networks in the 2.4 GHz and 5 GHz frequency band. The robust aluminum housing is resistant to shock and vibration and provides protection from mechanisms and electromagnetic loads in industry. It is installed in a cabinet, on the wall, an S7 standard rail or on a 35 mm DIN rail.

SCALANCE W788C-2 RJ-45 is a cost-effective alternative for use indoors with less hard environmental influences.

The controller access point SCALANCE W788C-2 M12 with degree of protection IP65 is intended for indoors and has similar characteristics to the SCALANCE W788C-2 RJ-45 but has a more robust design.

The controller access points SCALANCE W786C-2IA RJ-45, SCALANCE W786C-2 RJ-45 and SCALANCE W786C-2 SFP are equipped with an impact resistant plastic housing. The devices with degree of protection IP65 are shock and vibration resistant, designed for high mechanical and climatic requirements. This makes them particularly well suited for applications for mounting outdoors and / or in areas accessible to the public.

All controller access points must only be operated with the IWLAN controller WLC711.

4.5.8.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

Table 4- 19

Functionality	W788C-2 RJ-45	W788C-2 M12	W788C-2 M12 EEC	W786C-2 RJ-45 W786C-2IA RJ-45	W786C-2 SFP
PoE (Power-over-Ethernet) IEEE 802.3at Type 1, previously IEEE 802.3af.	•	•	•	•	-
Redundant power supply	•	•	•	•	•
Digital input / digital output	-	-	-	-	-
C-PLUG slot	-	-	-	-	-
IP degree of protection	IP30	IP65	IP65	IP65	IP65
Operating temperature minimum	-20 °C	-20 °C	-40 °C	-40 °C	-40 °C
Operating temperature maximum	+60 °C	+60 °C	+70 °C	+60 °C	+60 °C
Resistant to condensation	-	-	-	•	•
Resistant to salt water spray	-	-	-	•	•
UV resistant	-	-	-	•	•
Use in EX Zone 2 (EN60079-15:2005, EN60079-0:2006) ¹⁾	-	-	-	•	•
Use in EX Zone 2 in external housing (EN50021 min. IP54 according to EN60529) ¹⁾	•	•	•	-	-
IEEE 802.11 a/b/g/n	•	•	•	•	•
IEEE 802.11n MIMO	•	•	•	•	•

Operation with IWLAN controller	•	•	•	•	•
Operation with Enterasys WLAN controller	•	•	•	•	•

- Suitable / available or according to the specified standard.

¹⁾ Note installation instructions

Functions

All devices have the following functions:

- SSH / HTTPS / admin password
- WEP / WPA / WPA2
- IEEE 802.11i, Hidden SSID
- IEEE 802.1x (RADIUS)
- EAP-TLS, EAP-TTLS, PEAP
- WDS (Wireless Distribution System)
- SNMP
- Syslog

The controller-based access points of the SCALANCE W78xC have the following additional functions:

- IEEE 802.11e (QoS/WMM)
- PROFINET IO diagnostics
- STP / RSTP (IEEE 802.1d/w)
- VLANs (Multi-SSID)

The WLC controller also has the following functions:

- Integrated VLAN-VNS
- Auto detection of new access points
- Dynamic Radio Management
- VoIP QoS mapping (DSCP/TCP to WMM)
- VoIP roaming between IP subnets
- VoIP roaming between several IWLAN controllers

4.5.8.3 Interfaces

Interfaces

Table 4- 20

	WLAN inter- face	Antenna connector		Ethernet interface 10 / 100/ 1000 Mbps	Power supply connector
		external	internal		
WLC711	-	-	-	2 (RJ-45)	2-pin screw terminal
W788C-2 M12	2	6 (N-Connect fe- male)	-	1 (M12)	4-pin screw terminal incl. PoE or 4 to 8-pin, PoE
W788C-2 RJ-45	2	6 (R-SMA connector female)	-	1 (RJ-45)	
W786C-2IA RJ-45	2	-	6	1 (RJ-45)	"-pin plug (24 VDC) or optional power supply adapter (4-pin 24 VDC or 3-pin 110 - 230 VAC)
W786C-2 RJ-45	2	6 (R-SMA connector female)		1 (RJ-45)	

Article numbers

Table 4- 21

WLC711	Ethernet interface RJ-45	6GK5711-0XC00-1AA0 6GK5711-0XC00-1AB0 ¹⁾ 6GK5711-0XC00-1AD0 ²⁾
W788C-2 RJ-45	Ethernet interface RJ-45, 6 external antennas	6GK5788-2FC00-1AA0 ³⁾
W788C-2 M12	Ethernet interface M12, 6 external antennas	6GK5788-2GD00-1AA0 ³⁾
W786C-2IA RJ-45	Ethernet interface RJ45, 6 internal antennas	6GK5786-2HC00-1AA0 ³⁾
W786C-2 RJ-45	Ethernet interface RJ-45, 6 external antennas with R-SMA female connector	6GK5786-2FC00-1AA0 ³⁾

¹⁾ US wireless approval

²⁾ Wireless approval for Japan

³⁾ Two integrated wireless cards

4.5.9 Antennas

4.5.9.1 How it works

How antennas work

The task of an antenna is to convert electrical current into electromagnetic waves and vice versa. A basic distinction is made between separate and integrated antennas. Detached antennas increase the reliability of wireless links by optimizing the transmit and receive conditions because these antennas can be mounted at a location with optimum wireless conditions.. The connection between the detached antenna and access point or client is via a cable. The antennas operated directly on the device allow compact, low-maintenance installation.

The antennas can communicate in the 2.4 GHz or 5 GHz frequency band or in both frequency bands.

Two further related properties are important for any antenna:

- **Radiation characteristics**

The radiation characteristics describe how strong the directionality of an antenna is. You have three options:

- **Omnidirectional**

Radiation is uniform in all directions of a spatial plane (horizontal or vertical, depending on the position of the antenna).

- **Directional**

Radiation is predominantly in one direction in which the electromagnetic waves are transmitted with higher intensity. In the other spatial areas, the field strength is correspondingly weaker.

- **Antenna gain**

The antenna gain is the characteristic value for the directionality of an antenna. This parameter is obtained by comparing the maximum radiated power of the antenna with the power of an isotropic radiator. The antenna gain G is calculated in dBi according to the following formula:

$$G = 10 * \log (\text{max. power density antenna} / \text{max. power density of an isotropic radiator})$$

Antennas with multiple connectors: Dual or MIMO antennas according to IEEE 802.11n

Dual antennas are antennas with two connectors. These are integrated in an antenna housing as two individual antennas offset by 90° from each other or have a suitable clearance to each other. These antennas can be used to transmit two data streams at the same time.

MIMO antennas are antennas with three connectors. They contain three individual radiators combined in one antenna housing and operating either in different polarization planes (0°, +/- 45°) or with a suitable clearance between them. The MIMO antennas can transmit three data streams simultaneously making use of multipath propagation.

Transmitting multiple data streams increases the data throughput while at the same time making data transfer more reliable.

Radiating cable IWLAN RCoax cable

In environments that make the use of wireless difficult, or when the node only moves along predefined rails, it is sometimes preferable to replace the omnidirectional antennas with an RCoax radiating cable. The radiating cable is a special antenna in the form of a thick, flexible cable that produces an RF field with high intensity but only over a very limited range. As long as it can be guaranteed that the communication partner moves in an area close to the RCoax cable, the radiating cable provides a reliable RF field and an excellent connection to the nodes.

- Reliable coverage in difficult wireless areas, for example cranes,
- High-bay loader units, production lines, tunnels or overhead monorails
- Generation of a cone-shaped limited RF field
- Low interference or mutual disturbance due to low transmit power
- Cost saving due to direct substitution of sliding contacts and trailing cables
- Highly flexible application

4.5.9.2 Product overview

Table 4- 22 Omnidirectional antennas

Device type	Horizontal radiation angle/ characteristics	Antenna gain at 2.4 GHz	Antenna gain 5 GHz	Number and types of connectors	Direct mounting	Detached mounting	Degree of protection
 ANT795-4MA	360°	3 dBi	5 dBi	1 x R-SMA male	•	-	IP30
 ANT795-4MC	360°	3 dBi	5 dBi	1 x N-Connect male	•	-	IP65
 ANT795-4MD	360°	3 dBi	5 dBi	1 x N-Connect female	•	-	IP65
 ANT795-4MX	360°	2 dBi	2.5 dBi	1 x N-Connect male	•	-	IP69K
 ANT795-6MP	360°	5 dBi	7 dBi	1 x N-Connect female	-	•	IP67

Device type	Horizontal radiation angle/ characteristics	Antenna gain at 2.4 GHz	Antenna gain 5 GHz	Number and types of connectors	Direct mounting	Detached mounting	Degree of protection
 ANT792-6MN	360°	6 dBi	-	1 x N-Connect female	-	•	IP65
 ANT793-6MN	360°	-	5 dBi	1 x N-Connect female	-	•	IP65
 ANT795-6MN	360°	6 dBi	8 dBi	1 x N-Connect female	-	•	IP65 ¹⁾
 ANT795-6MT	360°	4 dBi	6 dBi	3 x QMA socket female	-	•	IP65

¹⁾ Degree of protection IP20 when using the mounting adapter.

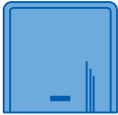
Table 4- 23 Antennas with directionality

Device type	Horizontal radiation angle/ characteristics	Antenna gain 2.4 GHz / dBi	Antenna gain 5 GHz / dBi	Number and types of connectors	Direct mounting	Detached mounting	Degree of protection
 ANT795-6DC	75° ²⁾ 55° ³⁾	9 dBi	9 dBi	1 x N-Connect female	-	•	IP67
 ANT793-6DG	70° ³⁾	-	9 dBi	2 x N-Connect female	-	•	IP67
 ANT793-6DT	65° ³⁾	-	8 dBi	3 x QMA socket female	-	•	IP67

²⁾ In the frequency band of 2.4 GHz

³⁾ In the frequency band of 5 GHz

Table 4- 24 Antennas with strong directionality

Device type	Horizontal radiation angle/ characteristics	Antenna gain 2.4 GHz / dBi	Antenna gain 5 GHz / dBi	Number and types of connectors	Direct mounting	Detached mounting	Degree of protection
 ANT793-8DP	40°	-	13.5 dBi	1 x N-Connect female	-	•	IP66/67
 ANT792-8DN	35°	14 dBi	-	1 x N-Connect female	-	•	IP23
 ANT793-8DL	30°	-	14 dBi	2 x N-Connect female	-	•	IP66/67
 ANT793-8DJ	17° ³⁾	-	18 dBi	2 x N-Connect female	-	•	IP67
 ANT793-8DK	9° ³⁾	-	23 dBi	2 x N-Connect female	-	•	IP67

³⁾ In the frequency band of 5 GHz

Table 4- 25 RCoax antennas for SCALANCE W-700 IWLAN RCoax cable according to IEEE802.11a/b/g/n

Device type	Horizontal radiation angle/ characteristics	Antenna gain 2.4 GHz / dBi	Antenna gain 5 GHz / dBi	Number and types of connectors	Direct mounting	Detached mounting	Degree of protection
 ANT792-4DN	90° ²⁾	4 dBi	-	1 x N-Connect female	-	•	IP65
 ANT793-4MN	360° ³⁾	-	6 dBi	1 x N-Connect female	-	•	IP65
 RCoax cable	-	-	-	-	-	•	IP65

²⁾ In the frequency band of 2.4 GHz

³⁾In the frequency band of 5 GHz

Article numbers

Table 4- 26 Omnidirectional antennas

ANT795-4MA ¹⁾	Antenna gain incl. connector 3 / 5 dBi for 2.4 / 5 GHz, IP30 rotatable, with extra joint, R-SMA male, pack of: 1 antenna	6GK5795-4MA00-0AA3
ANT795-4MC ¹⁾	Antenna gain incl. plug 3 / 5 dBi for 2.4 GHz / 5 GHz, IP65 (-20 °C to +65 °C), straight connector, N-Connect male, pack of: 1 antenna	6GK5795-4MC00-0AA3
ANT795-4MD ¹⁾	Antenna gain incl. plug 3 / 5 dBi for 2.4 GHz / 5 GHz, IP65 (-20 °C to +65 °C), connector at fixed angle of 90°, pack of 1 antenna	6GK5795-4MD00-0AA3
ANT795-4MX ¹⁾	Antenna gain incl. N-Connect plug 2 / 2,5 dBi for 2.4 GHz / 5 GHz, IP69K (-40 °C to +85 °C), pack of: 1 antenna	6GK5795-4MX00-0AA0
ANT795-6MP	Antenna gain incl. N-Connect plug 5 / 7 dBi for 2.4 GHz / 5 GHz, IP67 (-40 °C to +80 °C), pack of: 1 antenna, mounting fittings for wall and mast mounting.	6GK5795-6MP00-0AA0
ANT792-6MN	Antenna gain incl. N-Connect plug 6 dBi for 2.4 GHz, IP65 (-40 °C to +80 °C), with terminating resistor 1 x T1795-1R incl. mounting material	6GK5792-6MN00-0AA6

ANT793-6MN	Antenna gain incl. N-Connect plug 5 dBi for 5 GHz, IP65 (-45 °C to +70 °C), with terminating resistor 1 x TI795-1R incl. mounting material	6GK5793-6MN00-0AA6
ANT795-6MN	Antenna gain incl. plug 6/8Bi for 2.4 GHz / 5 GHz-IP65 (-40 °C to +80 °C), with terminating resistor 1 x TI795-1R	6GK5795-6MN10-0AA6
ANT795-6MN Mounting tool	Mounting aid for installing the ANT795-6MN below a roof, including installation fittings.	6GK5795-6MN01-0AA6
ANT795-6MT	MIMO antenna with 3 QMA sockets, antenna gain 6 dBi, for 2.4 GHz / 5 GHz, IP65 (-40 °C to +80 °C), incl. securing bracket	6GK5795-6MT00-0AA0

1) Mounting directly on SCALANCE W

Table 4- 27 **Antennas with weak directionality**

ANT795-6DC	Wide-angle antenna with slight directionality; antenna gain incl. N-Connect plug 9 / 9 dBi, for 2.4 GHz / 5 GHz, IP67 (-40 °C to +80 °C)	6GK5795-6DC00-0AA0
ANT793-6DG	Dual-slant angled antenna with slight directionality; antenna gain incl. 2 N-Connect plugs 9 dBi, for 5 GHz, IP67 (-40 °C to +80 °C)	6GK5793-6DG00-0AA0
ANT793-6DT	MIMO antenna with 3 QMA sockets; wide-angle antenna with slight directionality; antenna gain 9 dBi for 5 GHz, IP67 (-40 °C to +85 °C)	6GK5793-6DT00-0AA0

Table 4- 28 **Antennas with strong directionality**

ANT793-8DP	Antenna with strong directionality; antenna gain incl. N-Connect plug 13.5 dBi for 5 GHz, IP67 (-40 °C to +80 °C),	6GK5793-8DP00-0AA0
ANT792-8DN	Antenna with strong directionality; Antenna gain incl. N-Connect plug 14 dBi, for 2.4 GHz, IP23 (-40 °C to +80 °C), with terminating resistor 1 x TI795-1R	6GK5792-8DN00-0AA6
ANT793-8DL	Antenna with strong directionality; antenna gain 14 dBi for 5 GHz, IP65/67 (-40 °C to +70 °C), 2 x N-Connector, pack of: 1 antenna, fixing accessories for wall installation	6GK5793-8DL00-0AA0
ANT793-8DJ	Vertically-horizontally polarized antenna with strong directionality; Antenna gain incl. 2 N-Connect plugs 18 dBi, for 5 GHz, IP67 (-45 °C to +70 °C)	6GK5793-8DJ00-0AA0
ANT793-8DK	Vertically-horizontally polarized antenna with strong directionality; Antenna gain incl. 2 N-Connect plugs 23 dBi, for 5 GHz, IP67 (-45 °C to +70 °C)	6GK5793-8DK00-0AA0

Table 4- 29 RCoax antennas

Antennas for RCoax systems		
ANT792-4DN	RCoax helical antenna circular, polarized for RCoax systems; Connector N-Connect female; antenna gain at 2.4 GHz 1 dBi, IP65	6GK5792-4DN00-0AA6
ANT793-4MN	RCoax λ 5/ 8 vertically polarized for RCoax systems; connector N-Connect female; Antenna gain at 5.2 GHz/ 5.7 GHz 6/ 5 dBi; IP65	6GK5793-4MN00-0AA6
RCoax cable	IWLAN RCoax cable for 2.4 GHz Radiating cable for difficult wireless areas as a special antenna for SCALANCE W access points in the expanded temperature range of -40 °C to 85 °C, sold by the meter, minimum order 20 m.	6XV1875-2A
RCoax cable	IWLAN RCoax cable for 5 GHz Radiating cable for difficult wireless areas as a special antenna for SCALANCE W access points in the expanded temperature range of -40 °C to 85 °C, sold by the meter, minimum order 20 m.	6XV1875-2D

Accessories for IWLAN

In the product range of SIMATIC NET there are other accessories for IWLAN, for example connection cables, connectors, couplers and lightning protection elements. For more detailed information, refer to the following document:

SIMATIC NET Industrial Wireless LAN Passive network components IWLAN - System Manual

Document number C79000-G8976-C282

This document is also available on the Internet.

(<https://support.industry.siemens.com/cs/document/109480868/simatic-net-industrial-wireless-lan-passive-netzkomponenten-iwlan-systemhandbuch?dti=0&pnid=15861&lc=en-US>)

4.6 SCALANCE M routers and modems

4.6.1 SCALANCE M devices

Areas of application for SCALANCE M and components of GPRS

The widespread availability of GPRS (General Packet Radio Service) the expansion of LTE and advantageous volume tariffs allow wireless connection of stations to a control center in many countries without users needing to set up their own wireless network. The stations can be either stationary or mobile.

The online wireless connection is permanently available and provides properties similar to those of a dedicated line. Data changes can be transferred immediately and station or connection failures are detected and localized in a very short time.

Among others, the following systems can be controlled and monitored with the SCALANCE M devices:

- Sewage works, water treatment
- Oil and gas supply
- District heating networks
- Energy distributors
- Pumping stations
- Traffic control technology
- Building
- Wind energy and photovoltaic systems
- Machines
- Electronic advertising boards
- Weather stations
- Lighthouses and buoys

GPRS / UMTS / LTE for complex stations with increased security requirements

GPRS, UMTS and LTE packet oriented mobile communications services. With their high high transmission speeds, UMTS and LTE allow fast communication and are suitable above all for mobile Internet access. Devices like the SCALANCE M874-x or the SCALANCE M876-x combine the functionality of a VPN router with higher data security (IPsec protocol) and firewall. Via Industrial Ethernet other devices connected to the SCALANCE M_800 can be reached from a master station for diagnostics and parameter assignment.

A control center PC must be reachable constantly from the mobile wireless network. To achieve this, it is connected directly to the mobile wireless provider via a dedicated line or permanently to the Internet, for example using DSL. A SCALANCE S612 or SCALANCE S623 security module takes over the firewall function in the control center and represents the partner for the VPN connections of the GPRS stations. The VPN configuration is performed

with the SIMATIC NET "Security Configuration Tool" and allows configuration without special IT experience. The IP address of the master station should ideally be fixed, those of the stations can be assigned dynamically.

Wired communication via public or the company's own networks

The modules SCALANCE M812-1, SCALANCE M816-1 and SCALANCE M826-2 allow the connection of stations via wired networks. This can either be public or the company's own communications infrastructure. When a station is connected to the Internet via ADSL, the Internet services are available to you. For example a device can send an e-mail if an alarm event occurs. The SCALANCE M devices for wired communication also have proven security functions (firewall with stateful packet inspection, VPN, IPsec etc.).

If stations are connected via the company's own 2-wire copper cables, point-to-point and linear bus structures can be set up. The SCALANCE M826-2 device supports not only 2-wire but also 4-wire operation. With this two 2-wire cables are aggregated to form a virtual connection which allows the data rate to be doubled.

Example of a topology

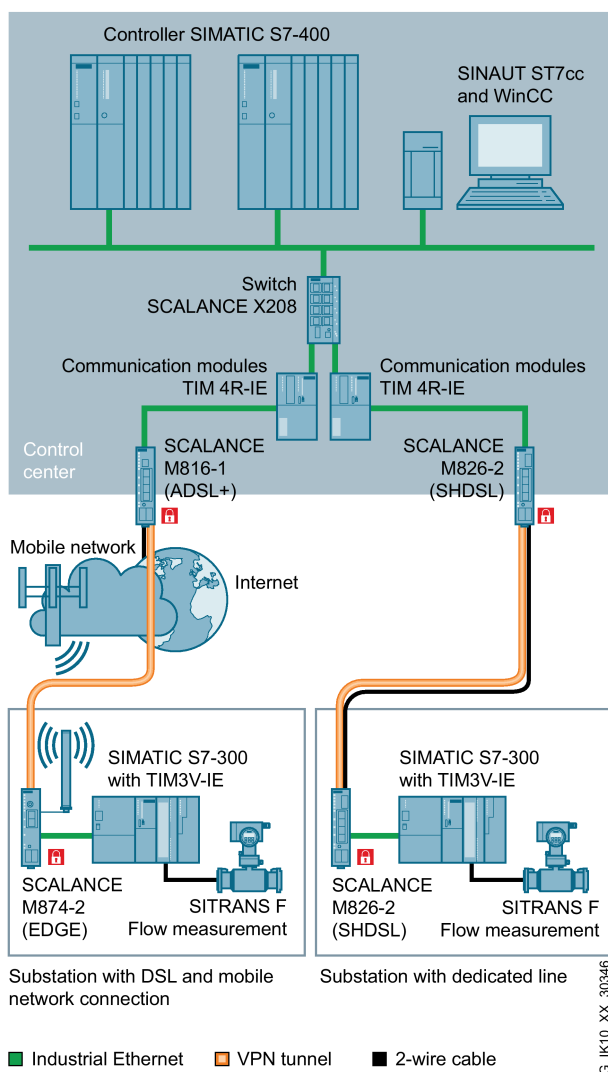


Figure 4-31 Example of a topology for the telecontrol network: Industrial Remote Communication

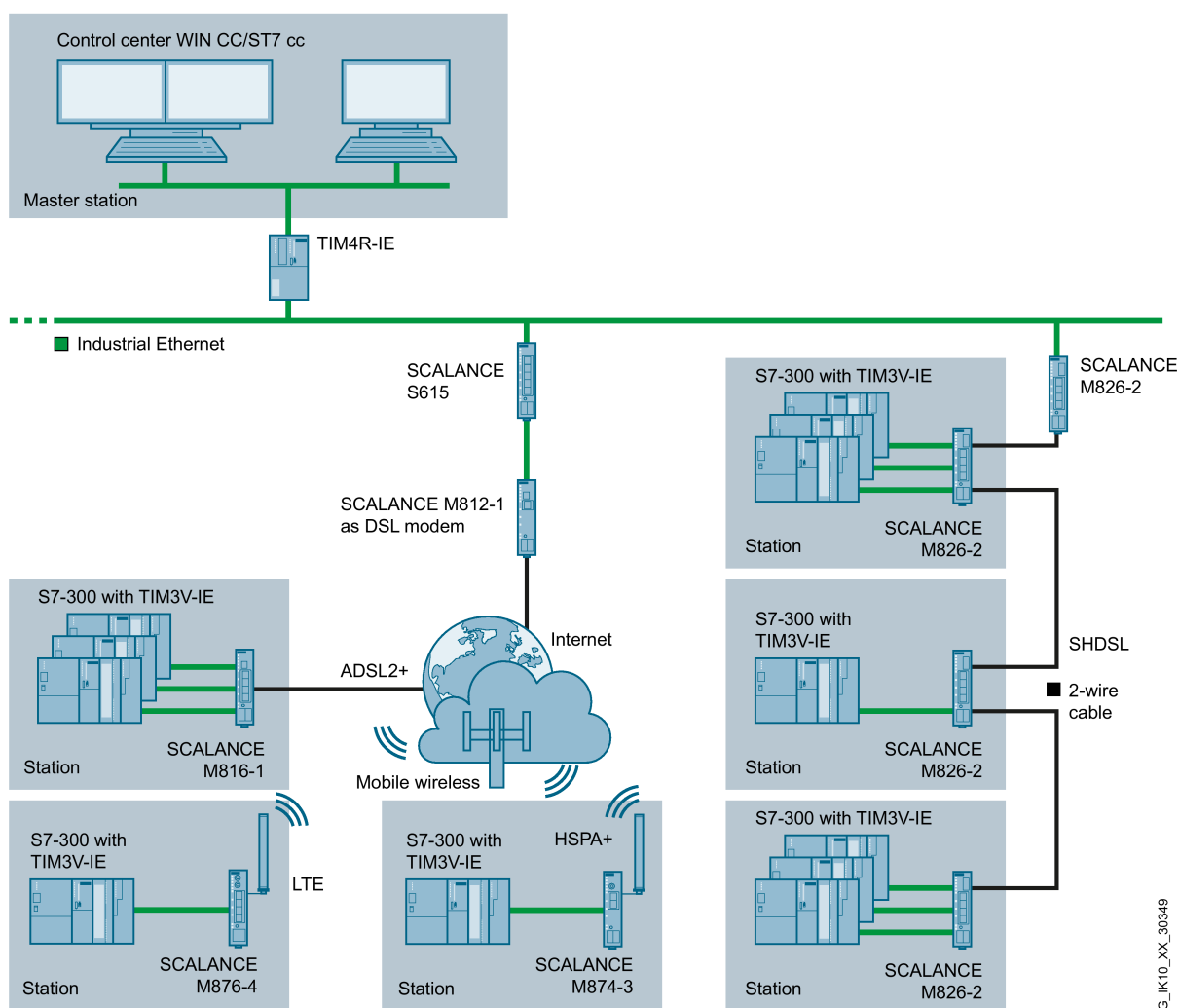
4.6.2 SCALANCE M812-1, M816-1 and M826-2

4.6.2.1 Description



Figure 4-32 SCALANCE M812-1, SCALANCE M816-1 and SCALANCE M826-2

The routers of the SCALANCE M81x/M826 series allow wired communication of programmable controllers via the Internet or via 2- or 4-wire cable. All devices have proven security mechanisms such as firewall (stateful packet inspection) and VPN. The robust plastic housings in the S7-1500 design are suitable for all common types of fastening (mounting on a DIN rail, S7-300 standard rail, S7-1500 standard rail, wall mounting). They also have a digital input and a digital output and a redundant power supply. The SCALANCE M816-1 and SCALANCE M826-2 also have a 4-port switch.



G_IK10_XX_30349

Figure 4-33 Example of a topology for using the devices SCALANCE M816-1 and M826-2

4.6.2.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	M812-1	M816-1	M826-2
Connectors	ADSL ADSL2 ADSL2+	ADSL ADSL2 ADSL2+	SHDSL
Number and types of connectors - internal network	1 x RJ-45 port	4 x RJ-45 ports	4 x RJ-45 ports
Connectors - external network	RJ-45 port	RJ-45 port	Terminal strip for 2-wire/5-wire cable

Power supply	24 VDC
Degree of protection	IP20

Functions of the devices SCALANCE M812-1, M816-1 and M826-2

- Configuration using the WBM
- MIB support
- HTTP, HTTPS
- SNMPv1, SNMPv2, SNMPv2c and SNMPv3
- DHCP client
- DHCP server for internal network
- NAT (IP masquerading, NAT traversal, 1:1 NAT)
- Port forwarding
- DNS cache
- Firewall (stateful packet inspection)
- VPN with up to 20 connections
- IPsec

Article numbers

M812-1	ADSL router with a connector for the internal network	6GK5812-1AA00-2AA2
M816-1	ADSL router 4-port switch.	6GK5816-1AA00-2AA2
M826-2	SHDSL router with 4-port switch.	6GK5826-2AB00-2AB2

4.6.3 SCALANCE M874-3 and M-876-4

4.6.3.1 Description



Figure 4-34 SCALANCE M874-x and SCALANCE M876-x

The routers of the SCALANCE M87x series allow mobile wireless connection of Ethernet-based devices. All devices have proven security mechanisms such as firewall (stateful packet inspection) and VPN. The robust plastic housings in the S7-1500 design are suitable for all common types of fastening (mounting on a DIN rail, S7-300 standard rail, S7-1500 standard rail, wall mounting). They also have a digital input and a digital output and a redundant power supply. The SCALANCE M874-x devices have a 2-port-switch, the SCALANCE M876-x devices have a 4-port switch.

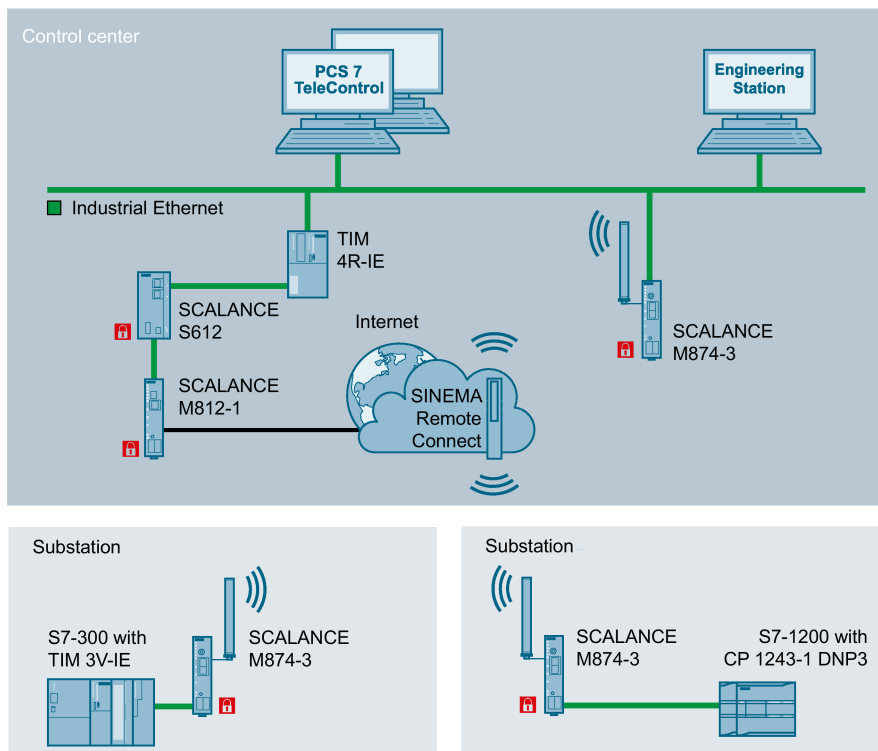


Figure 4-35 Example of a topology for using the SCALANCE M874-3 device

4.6.3.2 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	M874-2	M874-3	M876-3	M876-4
Supported wireless networks	GSM	GSM UMTS	GSM UMTS CDMA EV-DO	LTE
Supported mobile wireless services	GPRS eGPRS	GPRS eGPRS HSPA+	GPRS eGPRS HSPA+	GPRS eGPRS HSPA+ LTE Cat. 3
Number and types of connectors - internal network	2 x RJ-45 ports		4 x RJ-45 ports	
Number of SMA antenna sockets	1		2	
Power supply	24 VDC			
Degree of protection	IP20			

G_IK10_XX_30329

Functions of the devices SCALANCE M874-x and M876-x

- Configuration using the WBM, CLI or SNMP
- MIB support
- HTTP, HTTPS
- SNMPv1, SNMPv2, SNMPv2c and SNMPv3
- DHCP client
- DHCP server for internal network
- NAT (IP masquerading, NAT traversal, 1:1 NAT)
- Port forwarding
- DNS cache
- Firewall (stateful packet inspection)
- VPN with up to 20 connections
- IPsec
- OpenVPN client to SINEMA Remote Connect

Article numbers

M874-2	Mobile wireless router with 2-port switch	6GK5874-2AA00-2AA2
M874-3	Mobile wireless router for GSM and UMTS with 2-port switch.	6GK5874-3AA00-2AA2
M876-3	Mobile wireless router for GSM, UMTS, CDMA and EV-DO with 4-port switch.	6GK5876-3AA02-2BA2
M876-3 ROK	Mobile wireless router for GSM, UMTS, CDMA and EV-DO with 4-port switch. Version for Korea.	6GK5876-3AA02-2EA2
M876-4	Mobile wireless router for LTE with 4-port switch	6GK5876-4AA00-2BA2

4.6.4 SCALANCE M875

4.6.4.1 Description

SCALANCE M875



Figure 4-36 SCALANCE M785

The SCALANCE M875 router is designed as UMTS, EGPRS (GPRS with Edge) and GPRS router for wireless IP communication of Industrial Ethernet-based programmable controllers via UMTS / GSM mobile wireless networks. SCALANCE M875 has a high transmission rate using UMTS. The device is equipped with integrated security functions incl. firewall, VPN server and client (IPsec).

SCALANCE M875 has a rugged plastic housing and is designed for mounting on a DIN rail. The device is equipped with an RJ-45 interface for Industrial Ethernet, diagnostics LEDs for the modem status, the field strength and connection control, DI/DO channels, an SMA antenna connector for the GSM/UMTS antenna and a SET service button. The 4-pin screw terminal is for connection to the 24 VDC power supply. In addition to this, a 4-pin screw terminal is integrated for a digital input and output.

The following properties distinguish the SCALANCE M875 router:

- Low investment and operating costs for monitoring and controlling telecontrol substations connected by wireless
- Reduction of traveling costs or telephone costs thanks to remote programming and remote diagnostics using UMTS.
- High security thanks to the integrated firewall
- M875 can also be used as a VPN server and client (IPsec).

- The use of the existing UMTS /GSM infrastructure of mobile wireless providers
- Simple planning and commissioning of telecontrol substations without the user needing special wireless knowledge.

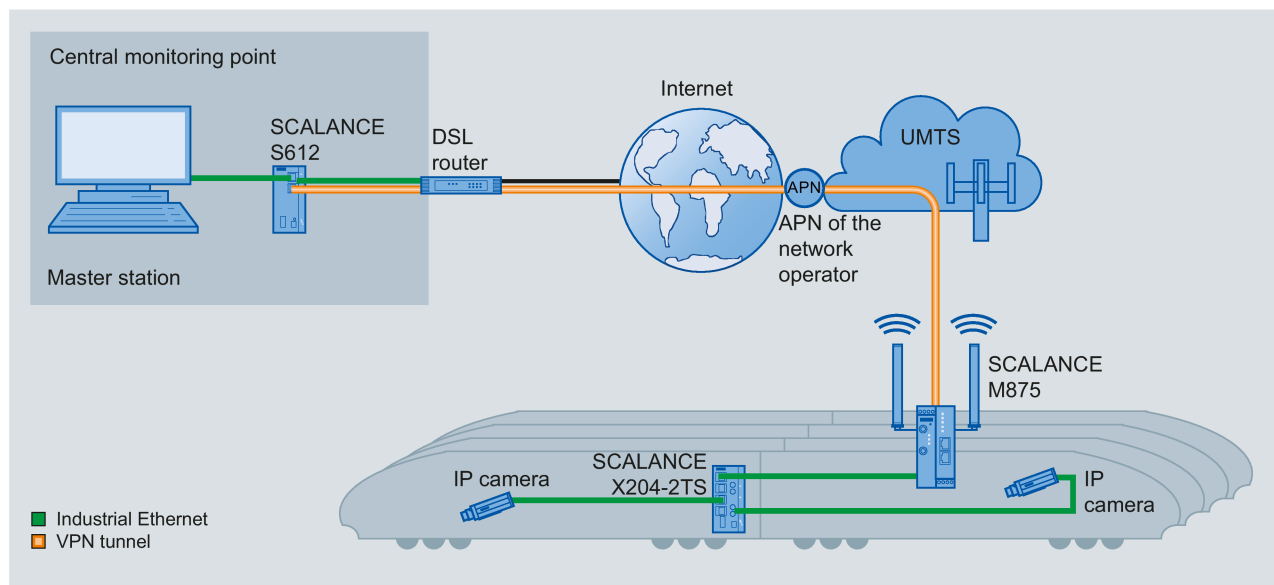


Figure 4-37 Example of a topology for use of the UMTS router M875 to improve passenger safety

4.6.4.2 Features and functions

Characteristics of the SCALANCE M875 router

	SCALANCE M875
Interface Ethernet	2 x RJ-45
Interface mobile wireless	2 x SMA
Redundant power supply	•
Digital inputs and outputs	•
Supported wireless networks	GSM UMTS
Firewall (incl. VPN server and IPsec)	•

- Suitable / available or according to the specified standard.

Functions of the SCALANCE M875 router

The SCALANCE M875 router has the following functions:

- Triband UMTS with the frequency bands 850 / 1900 / 2100 MHz
- Quadband GSM with the frequency bands 850 / 850 / 1900 / 2100 MHz
- Without a UMTS network, there is an automatic changeover to EGPRS (multislot class 12) or GPRS mode.

- The automatic establishment and keeping open of the IP-based online connection to the Internet.
- The linking of distributed, IP-based networks using UMTS/GSM mobile wireless networks
- Bidirectional, IP-based data communication with the telecontrol control center, for example ST7cc or ST7sc, WinCC or PCS 7.
- Integrated security functions including firewall
- The data exchange between telecontrol stations (inter-station communication) via a TIM communications module in the master station.
- Secure data communication with the SINAUT ST7 stations, including communication via mobile wireless provider networks that do not provide public and fixed IP addresses for the modem.
- Automatic and user-defined sending of SMS messages

Configuration

- Convenient configuration of all network and firewall parameters of the router via a Web browser

Security

- Router for data transfer via public networks with NAT functionality (NAT traversal)
- Suitable VPN termination of the control center using SCALANCE S
- A firewall for protection against unauthorized access The dynamic packet filter examines data packets based on their source and destination addresses (stateful packet inspection) and blocks undesirable data traffic (anti-spoofing).

Diagnostics and upkeep

- Status of connection establishment and an existing connection displayed by front panel LEDs and via a Web browser

Requirements for using the SCALANCE M875 UMTS router

- The SIM card of a UMTS network operator with HSPA support (HSUPA and HSDPA) or a SIM card of a GSM network operator with EGPRS or GPRS support.

Note

For further technical details, refer to the operating instructions of the SCALANCE M875.

Article number

M875	UMTS routers for wireless IP communication of Industrial Ethernet-based programmable controllers via UMTS/GSM mobile wireless networks; EGPRS multislot class 12	6GK5875-0AA10-1AA2
-------------	--	---------------------------

4.6.5 Teleservice adapter IE

4.6.5.1 Description



Figure 4-38 Teleservice adapter IE basic

The teleservice adapter is available in two versions: Teleservice adapter IE basic and teleservice adapter IE advanced. Both devices allow the connection of an Ethernet network to the phone network. A full device consists of a TeleService adapter IE as the basic device and a TS module suitable for the telecommunications infrastructure. The following variants exist:

- **TS Module Modem**
Modem for the analog telephone network.
- **TS Module ISDN**
Terminal adapter for the ISDN network
- **TS Module RS232**
Device with a 9-pin D-sub plug for connection of an external modem.
- **TS Module GSM**
Wireless modem for the GSM/GPRS network.

The TeleService adapter IE advanced also provides two switched LAN ports and can only be used in conjunction with the TS module GSM. As an alternative, a router for example a SCALANCE M874 can be connected to the WAN port. In this case, no TS module GSM is necessary. Basic device and modules have a rugged plastic housing in the S7-1200 design and are suitable for installation on a DIN rail or for wall mounting. There is also a mounting adapter for the S7-300 standard rail.

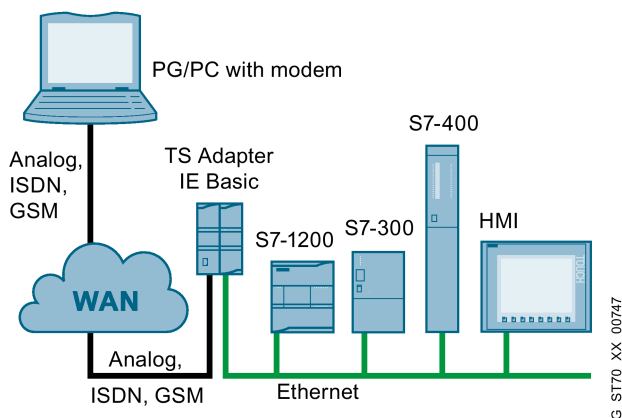


Figure 4-39 Example of a configuration of a teleservice adapter IE basic with TS module

4.6.5.2 Features and functions

Features of the basic devices and modules

The basic devices have the features listed in the table:

	TS adapter IE basic	TS adapter IE advanced
Suitable for module	TS Module Modem TS Module ISDN TS Module RS-232 TS Module GSM	TS Module GSM or Router at WAN port
Number and type of the LAN interfaces	1 x RJ-45 port	2 x RJ-45 port (switched)
Number and type of the LAN interfaces	-	1 x RJ-45 port
Power supply	24 VDC(19.2 to 28.8 VDC)	
Degree of protection	IP20	

The modules have the characteristics shown in the following table:

	Modem	ISDN	RS-232	GSM
Number and type of the LAN interfaces	1 x RJ-11 socket	1 x RJ-11 socket	1 x D-sub plug, 9-pin	1 x SMA female
Power supply	Modules are supplied with power via the basic device.			

Functions of the devices

- Configuration via TIA Portal V11 and WBM. The TS adapter IE basic can also be used with the standalone software TeleService as of V6.1 or with the SIMATIC Manager
- Remote maintenance via the telephone network.
- Sending e-mails via an outgoing modem connection to a dial-in server.
- Internet access by establishing a connection to an Internet service provider.
- Access only after authentication with user name and password. Up to 8 users can be configured.

Article numbers

TS adapter IE basic	Basic device without its own WAN interface.	6ES7972-0EB00-0XA0
TS adapter IE advanced	Basic device with its own WAN interface and two switched LAN ports.	6ES7972-0EA00-0XA0
TS module modem	Modem for the analog telephone network.	6ES7972-0MM00-0XA0
TS module ISDN	Terminal adapter for the ISDN network.	6ES7972-0MD00-0XA0
TS module RS-232	Module for connection of an external modem.	6ES7972-0MS00-0XA0
TS module GSM	Wireless modem for the GSM/GPRS network.	6ES7972-0MG00-0XA0

4.6.6 Modem MD720

4.6.6.1 Description



Figure 4-40 Modem MD720

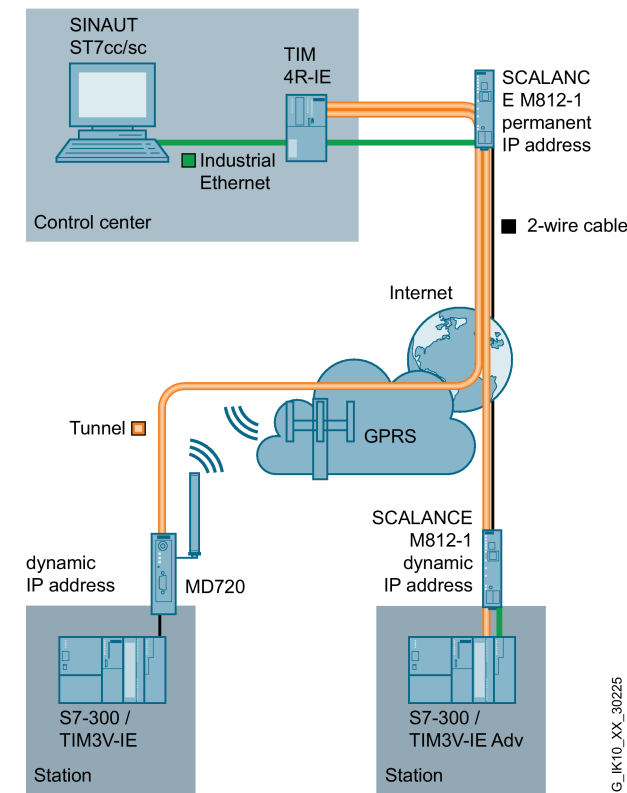
The GSM/GPRS modem MD720 is used for the telecontrol system SINAUT ST7 for data transmission via a dial-up connection (CSD service) and for a telecontrol system based on TeleControl Server Basic for data transmission via GPRS. It is used to set up systems for monitoring and controlling simple telecontrol stations. This device also allows energy-saving

concepts in systems and the connection of mobile nodes with central monitoring/control of rail-guided vehicles, special vehicles, local public transport, complex machines, and shipping in inland waters and coastal areas.

The GSM/GPRS modem MD720 consists of a rugged plastic housing and is designed for mounting on a DIN rail and for wall mounting. The device is equipped with an RS-232 interface, diagnostics LEDs for the modem status, the field strength and connection control, an SMA antenna connector for the GSM/EGPRS antenna and a SET service button. The 4-pin terminal strip is for connection to the 24 VDC power supply.

Example of a topology

IP-based communication via GPRS/DSL with the MSC protocol



4.6.6.2 Features and functions

Features of the MD720 modem

	Modem MD720
Interface - internal network	1 x D-sub 9-pin
Interface mobile wireless	1 x SMA
Digital inputs and outputs	-

Supported wireless networks	GSM
Supported wireless services	GPRS CSD SMS
AT command interface	•

- Suitable / available or according to the specified standard.

Functions of the MD720 modem

The MD720 modem has the following functions:

- Quadband GSM (850/900/1800/1900 MHz)
- GPRS multislots class 10 (gross: 13.4-27 kbps upload, 40-54 kbps download).
- Automatic establishment and keeping up of the IP-based online connection via GPRS to the Internet
- IP-based data exchange with the PC-based application TeleControl Server Basic (router and OPC server)
- Data exchange with other MS720 modems via the routing of TeleControl Server Basic
- Changeover between GPRS and CSD (modem operation) during operation
- CSD and GPRS connection controllable using AT commands
- Sending of SMS messages and fax (via SMS) using GSM services
- Secure access to data of the S7-200 also via mobile wireless provider networks that do not provide public and fixed IP addresses for the modem.

Project engineering

- Parameter assignment via SPS blocks with the programming tool Micro/Win for S7-200 (blocks part of TeleControl Server Basic)
- AT command interface

Security

- Release of up to 3 call numbers for incoming GSM connection (CLIP function) for teleservice
- User name and password for GSM connection
- Unrestricted client and server operation also in protected GPRS networks with private addresses of the mobile wireless provider.
- Encrypted data traffic between modem, Internet and SINAUT MICRO SC

Diagnostics / maintenance

- Status of connection establishment and an existing connection displayed by front panel LEDs
- Reading out configuration data via the RS-232 interface

- Connection status to the modem and PLC monitorable in TeleControl Server Basic
- Direct additional access via GSM (modem operation) for teleservice (remote programming, remote diagnostics)

Article number

Modem MD720	Mobile wireless modem with RS-232 interface for the GSM services CSD, GPRS, SMS, quadband GSM, AT command interface. Automatic GPRS connection establishment incl. gender changer for RS-232/PPI adapter	6NH9720-3AA01-0XX0
--------------------	--	---------------------------

4.6.7 SINEMA Remote Connect

Management platform for remote networks

The server application SINEMA Remote Connect allows the convenient and secure maintenance of distributed stations using remote access. Based on VPN tunnel connections, SINEMA Remote Connect manages access to the installed machines and systems. Direct access to the company network is not necessary because the service technician establishes a connection to SINEMA Remote Connect.

You will find detailed information on the Internet at the following address:

(<http://www.siemens.com/sinema-remote-connect>)

4.6.8 Antennas for mobile wireless

4.6.8.1 Product overview

Table 4- 30 Antennas for mounting directly on the device

Antenna	GSM (2G)	GPRS	UMTS	LTE Europe	LTE North America	GPS	WLAN
 ANT896-4MA	•	•	•	•	•	-	-

Table 4- 31 Antennas for detached mounting

Antenna	GSM (2G)	GPRS	UMTS	LTE Europe	LTE North America	GPS	WLAN
 ANT896-4ME	•	•	•	•	•	-	-
 ANT794-4MR	•	•	•	•	-	-	-
 ANT794-3M	•	•	-	-	-	-	-
 ANT895-6ML	-	-	-	-	-	•	-

Table 4- 32 Antennas for mounting on vehicles

Antenna	GSM (2G)	GPRS	UMTS	LTE Europe	LTE North America	GPS	WLAN
 ANT896-6MM	•	•	•	•	-	•	•
 ANT896-6MH	•	•	•	•	-	-	-

• Suitable / available or according to the specified standard.

Technical specifications

Antenna	Antenna gain	Connector	Permitted ambient temperature	Degree of protection
ANT896-4MA	2 dBi	SMA male	-40 °C to +85 °C	IP54
ANT896-4ME	3 dBi	N-Connect female	-40 °C to +70 °C	IP66
ANT794-4MR	0 dBi	SMA male	-40 °C to +70 °C	IP65
ANT794-3M	0 dBi	SMA male	-40 °C to +75 °C	IP64
ANT895-6ML	3 dBi at 90° -2 dBi at 20°	N-Connect female	-40 °C to +85 °C	IP67
ANT896-6MM	4 ... 7 dBi ⁽¹⁾	3 x QMA	-40 °C to +85 °C	IP69K IP68
ANT896-6MH	5 ... 6 dBi ⁽¹⁾	N-Connect female	-40 °C to +85 °C	IP69K

⁽¹⁾ Depending on the frequency band you will find detailed information in the operating instructions

Article numbers

ANT896-4MA	Omnidirectional antenna for mounting directly on the device	6GK5896-4MA00-0AA3
ANT896-4ME	Omnidirectional antenna for detached mounting	6GK5896-4ME00-0AA0
ANT794-4MR	Omnidirectional antenna for indoors and outdoors	6NH9860-1AA00
ANT794-3M	Omnidirectional flat antenna for GSM and GPRS	6NH9870-1AA00
ANT895-6ML	GPS antenna with integrated signal amplifier.	6GK5895-6ML00-0AA0
ANT896-6MM	Omnidirectional antenna with E1 approval for mounting on a vehicle roof.	6GK5896-6MM00-0AA0
ANT896-6MH	Omnidirectional antenna with railway approval for mounting on a vehicle roof.	6GK5896-6MH00-0AA0

Accessories for mobile wireless devices

In the product range of SIMATIC NET there are other accessories for mobile wireless devices, for example connection cables, connectors, couplers and lightning protection elements. For more detailed information, refer to the following document:

SIMATIC NET Industrial Wireless LAN Passive network components IWLAN - System Manual

Document number C79000-G8976-C282

This document is also available on the Internet.

(<https://support.industry.siemens.com/cs/document/109480868/simatic-net-industrial-wireless-lan-passive-netzkomponenten-iwlan-systemhandbuch?dti=0&pnid=15861&lc=en-US>)

4.7 SCALANCE S security module

4.7.1 Introduction

Areas of application of SCALANCE S

The SCALANCE S security modules protect nodes connected to the protected network with a combination of different security measures. SCALANCE S devices have different protective functions and individual devices or even entire automation cells can be integrated into the protected area. The security modules can be operated not only in bridge mode but also in router mode. This means that the security modules are used directly at IP subnet boundaries. There are different product variants to meet specific requirements such as the use of FO cables or standby mode. For secure remote access via Internet, suitable devices of the SCALANCE M800 series are available.

SCALANCE S is optimized for use in an automation or industrial environment. It meets the specific requirements of automation engineering, for example easy upgrading of existing systems, simple installation and minimum downtimes if a fault occurs.

Advantages of the cell protection concept:

- Protection from data espionage and data manipulation
- Protection against overload of the communications system
- Protection from external influences
- Protection from addressing errors
- Secure remote access via Internet
- Changes to or adaptation of the existing network structure are not necessary.
- Changes to or adaptation of the existing applications or network nodes are not necessary.



Figure 4-41 SCALANCE S product family

The range of devices is expanded by the SOFTNET Security Client. This is a software application that allows secure access to automation systems protected by SCALANCE S.

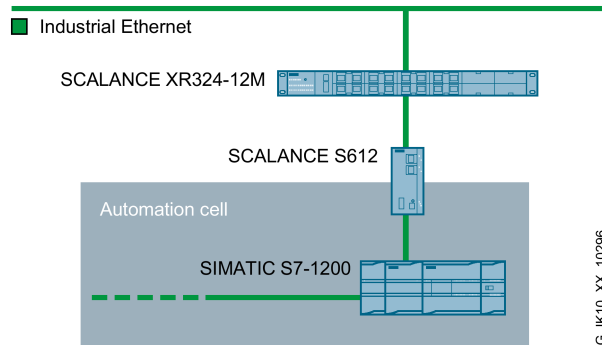


Figure 4-42 Example of a topology: Protection of an automation cell with a SCALANCE S612

4.7.2 Technical basics

Internal and external network nodes

SCALANCE S devices divide networks into two areas:

- Internal network: Protected areas with the "internal nodes".
Internal nodes are the nodes protected by a SCALANCE S device.
- External network: Unprotected areas with the "external nodes".
External nodes are all the nodes located outside the protected areas.

The internal network is considered to be secure and trustworthy. Connect an internal network segment to the external network segments only over a SCALANCE S device. There must be no other paths connecting the internal and external networks.

Configuration and administration

A CD ships with the SCALANCE S modules containing not only the manual but also the Security Configuration Tool.

The Security Configuration Tool is designed for the following tasks:

- For configuration of the SCALANCE S security modules.
- For configuration of the SOFTNET Security Client (not possible for SCALANCE S602).
- For test and diagnostics functions and status displays.

To operate the SCALANCE S modules, you need to download a configuration created with the Security Configuration Tool. The configuration of a SCALANCE S module involves the IP parameters and the configuration of the firewall rules. With all devices except the

SCALANCE S602, it is also possible, when necessary, to configure IPsec tunnels. For the SCALANCE S602 router operation can be configured.

Firewall

The firewall functionality of SCALANCE S security modules protects the internal network from influences or disturbances from external networks. This means that; depending on the configuration, only certain specified communication relations between the network nodes from the internal network and network nodes of the external networks are allowed. All network nodes located in the internal network segment of a SCALANCE S security module are protected by its firewall.

The firewall functionality can be configured for the following protocol levels:

- IP firewall incl. stateful inspection
- Firewall for Ethernet "non-IP" frames according to IEEE 802.3; (layer 2 frames)

The stateful inspection firewall (also known as Stateful Packet Filter or Dynamic Packet Filter) is a firewall technology that operates both on the network and at the application layer. The IP packets are accepted on the network layer, checked according to their state by an analysis module and compared with a status table. For the communication partner, a firewall with stateful inspection appears as a direct connection that only allows communication according to the rules.

Firewall rules are the rules for data traffic in the following directions:

- From the internal to the external network and vice versa,
- from the internal network into an IPsec tunnel and vice versa (not possible with the SCALANCE S602).

For all devices, user-specific firewall rules can also be specified. This means a predefined set of rules that is assigned at the login user-dependent for a limited time.

SCALANCE S in routing mode

If SCALANCE S modules are operated in routing mode, they separate the internal network from the external network based on the evaluation of the IP addresses. The internal network separated by SCALANCE S602 therefore becomes a separate subnet.

The following options are available:

- Routing can be configured in standard mode and advanced mode.

Frames intended for an existing IP address in the subnet (internal or external) are forwarded. The firewall rules for the direction of transmission also apply. For this mode, you must also configure an IP address for the internal subnet.

Note

In contrast to the bridge mode of the SCALANCE S security modules, VLAN tags are lost in routing mode.

- NAT/NAPT routing can be configured in the advanced mode.

In this mode, the IP addresses are also translated. The IP addresses of the devices in the internal subnet are translated to external IP addresses and are therefore "invisible" in the external network.

SCALANCE S as DHCP server

A DHCP server assigns an IP address to each client throughout the network. DHCP (Dynamic Host Configuration Protocol) in conjunction with a suitable server, allows the dynamic assignment of an IP address and other configuration parameters to computers within the network. SCALANCE S security modules can be operated in the internal network as DHCP servers. This allows IP addresses to be assigned automatically to the devices connected to the internal network. The IP addresses are assigned either dynamically from a defined range of addresses or a specific device is assigned a specific IP address according to the definition.

Testing, diagnostics, logging and Syslog

For testing and monitoring, the Security Configuration Tool (SCT) has diagnostics and logging functions.

- Diagnostics functions
In online mode various system and status functions can be used for diagnostics.
- Logging functions
The system and security events are logged. The events are logged in the buffer areas of the security module (local logging) or of a server (network Syslog). You select the events to be logged in the log settings for the relevant security module.

IPsec tunnel (not possible for the SCALANCE S602)

IPSec the short form of Internet Protocol Security is a layer 3 tunneling protocol. It is supported by all SCALANCE S devices except the SCALANCE S602. The IPsec tunnel provides the nodes with a secure data connection through the non-secure external network to other devices protected by the SCALANCE S modules.

The encryption of the data transmission with VPN (IPsec) provides the following:

- Protection against espionage: The data exchanged is safe from eavesdropping (ensuring confidentiality).
- Protection against manipulation: The data exchanged is safe from corruption/counterfeiting (ensuring the integrity).
- Authenticity: Only authorized nodes can establish a tunnel (ensuring the legitimacy of the communication).

The Security Configuration Tool also allows the configuration of Virtual Private Networks (VPN). To do this SCALANCE S modules as well as the SOFTNET Security Client modules integrated in an internal network are put together in groups in the configuration. IPsec tunnels are established automatically between the SCALANCE S modules and SOFTNET Security Client modules that belong to the same group. Tunneling also includes Ethernet frames according to the IEEE standard 802.3 (layer 2 frames). Both IP and non-IP frames are transmitted through the IPsec tunnel.

4.7.3 Description

SCALANCE S devices are available in different housing designs (metal or plastic housing) and port configurations. Configuration and engineering data is stored in internal non-volatile memory. As an options, storage on a C-PLUG is also possible. If a SCALANCE S device needs to be replaced, the configuration data can be transferred simply to the new device.

SCALANCE S602



Figure 4-43 SCALANCE S602

The SCALANCE S602 protects from unauthorized access with a stateful inspection firewall. In "Ghost mode" protection of individual, even changing devices is possible due to dynamic adoption of the IP address. Data transmission rates of 10/100/1000 Mbps are supported.

SCALANCE S612



Figure 4-44 SCALANCE S612

The SCALANCE S612 provides the same range of functions as the SCALANCE S602. In addition, the device supports IPsec with up to 128 VPN connections.

SCALANCE S615



Figure 4-45 SCALANCE S615

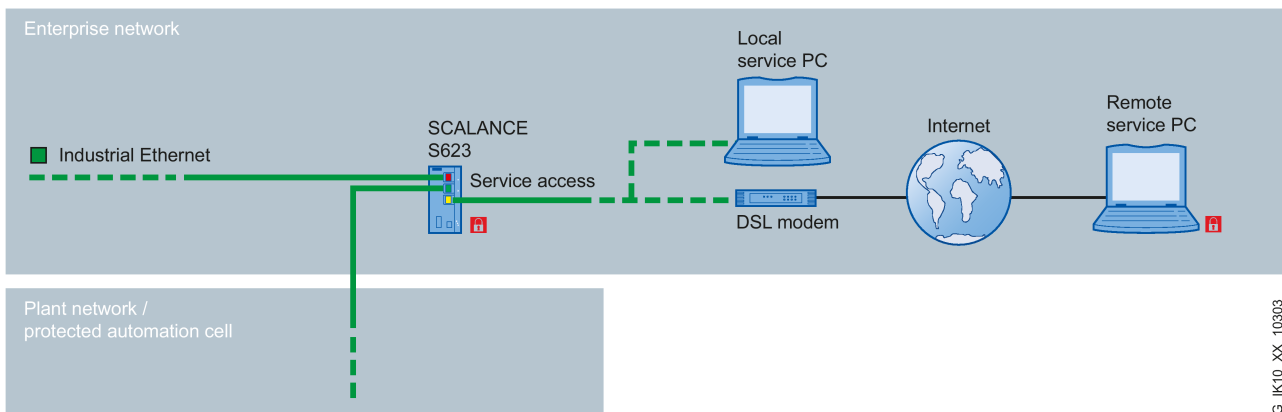
The SCALANCE S615 protects from unauthorized access with a stateful inspection firewall. In addition, the device supports IPsec and OpenVPN (as a client in SINEMA RC) with up to 20 VPN connections. Up to 5 variable security zones per port-based VLAN can be set up. The firewall rules can be configured as required between the security zones. A key switch function on the digital input allows the controlled establishment of a tunnel connection. There is an auto-configuration interface for simple configuration to SINEMA Remote Connect.

SCALANCE S623



Figure 4-46 SCALANCE S623

The SCALANCE S623 provides the same range of functions as the SCALANCE S612. The device also has a DMZ port (DMZ: "Demilitarized Zone") for the secure connection of remote maintenance modems, laptops or an additional network. This yellow port is secured towards the red and green port with a firewall and can also terminate VPNs. There can also be a standby link to a redundant device via the yellow port.



G_IK10_XX_10303

Figure 4-47 Local connection of a service PC or Internet access via the DMZ interface of the SCALANCE S623

SCALANCE S627-2M



Figure 4-48 SCALANCE S627-2M

The SCALANCE S627-2M provides the same range of functions as the SCALANCE S623. Two additional slots for media modules each with a red and green port per module allow the direct integration in ring structures and FO networks. Existing 2-wire cables, for example for PROFIBUS, can be used by using the media module MM992-2VD.

4.7.4 Features and functions

Features

The individual devices have the characteristics shown in the following table:

	S602	S612	S615	S623	S627-2M
10 / 100 / 1000 Mbps ports	•	•	•	•	•
DMZ port	-	-	-	•	•
C-PLUG slot	•	•	•	•	•

- Suitable / available or according to the specified standard.

Functions

The following table indicates the functions provided by the individual devices:

	S602	S612	S615	S623	S627-2M
Firewall	•	•	•	•	•
Router and firewall redundancy	-	-	-	•	•
NAT/NAPT router	•	•	•	•	•
DHCP server (internal network)	•	•	•	•	•
DHCP client	-	-	•	-	-
SysLog	•	•	•	•	•

IPsec support	-	•	•	•	•
Max. number of VPN connections	-	128	20	128	128
Softnet security client	-	•	•	•	•
Configuration with the Security Configuration Tool	•	•	•	•	•
Configuration with WBM, CLI, SNMP	-	-	•	-	-

- Suitable / available or according to the specified standard.

4.7.5 Interfaces

The SCALANCE S modules have the following connectors or interfaces:

Connectors/interface	S602	S612	S615	S623	S627-2M
Number of RJ-45 sockets for end devices and network components	2	2	5	3	3
Number of slots for media modules	-	-	-	-	2
4-pin terminal block for power supply 24 VDC (19.2 ... 28.8 V)	•	•	-	•	•
5-pin terminal block for power supply 24 VDC (10.8 ... 28.2 V)	-	-	•	-	-
2-pin terminal block for signaling contact	•	•	-	•	•
2-pin terminal block for digital input	-	-	•	-	-
2-pin terminal block for digital output	-	-	•	-	-

- Suitable / available or according to the specified standard.

The two Industrial Ethernet connectors, port 1 and port 2 are handled differently by SCALANCE S modules. For this reason, these interfaces must not be confused when connecting to the communications network.

- **Port 1: External network**

Marked **red**, this interface is for the unprotected network area.

- **Port 2: Internal network**

Marked **green**, this interface is intended for the network area protected by SCALANCE S.

The same applies to ports P4 to P7 of the optional media modules of the SCALANCE S627-2M. With the SCALANCE S615 there is no color marking of the ports because the assignment of a port to the external or internal network can be freely configured.

Note

If these marked ports are swapped over, the devices lose their protective function.

Article numbers

S602	Stateful Inspection Firewall	6GK5602-0BA10-2AA3
S612	Stateful Inspection Firewall, IPsec support with max. 128 VPN connections.	6GK5612-0BA10-2AA3
S615	Stateful Inspection Firewall, IPsec support with max. 20 VPN connections, port-based VLAN with five variable security zones.	6GK5615-0AA00-2AA2
S623	Stateful Inspection Firewall, IPsec support with max. 128 VPN connections, DMZ port.	6GK5623-0BA10-2AA3
S627-2M	Stateful Inspection Firewall, IPsec support with max. 128 VPN connections, DMZ port two slots for media modules.	6GK5627-2BA10-2AA3

4.7.6 SOFTNET Security Client

Description

The SOFTNET Security Client is a software application that serves as an integral part of the Industrial Security concept to protect programmable controllers. This ensures security when data is exchanged between programmable controllers and entire automation systems or automation cells.

- The SOFTNET Security Client application is available as a VPN client for programming devices, PCs and notebooks in an industrial environment. The application allows secure client access via LAN or also via WAN to automation systems protected with SCALANCE S functionality. For example remote maintenance via the Internet.
- Protection of the data transfer from incorrect operator input, eavesdropping / espionage and manipulation.
Communication is only possible between authenticated and authorized devices.
- The SOFTNET Security Client uses proven IPsec mechanisms to establish and operate Virtual Private Networks (VPNs).
- End-to-end intuitive configuration without specialist security knowledge.
- A common configuration tool with a common database for SCALANCE S modules and the SOFTNET Security Client.
 - Automatic generation of the certificates by the Security Configuration Tool.
 - Automatic identification of the nodes of the internal network and detection of SCALANCE S modules in the external network.

Principle of the application

With the PC software SOFTNET Security Client, VPN services are made available on the PG or notebook. This makes secure IP-based access from the PC / PG to programmable controllers possible that are protected by SCALANCE S612 or SCALANCE S623.

Details

- Easy handling due to minimum configuration
- No specialist knowledge of IT security is necessary.
- Changes to or adaptation of the existing network structure are not necessary.
- Automatic generation of the certificates by the configuration tool.
- Little configuration effort due to automatic identification of the nodes of the internal network and detection of other security modules in the external network.

Benefits

- The secure access from programming devices or notebooks to complete automation cells / systems.
- The simple use of mobile PCs.
- The protection of data transfer from espionage and manipulation using certified standards.
- Devices classified as not secure can be included in the secure data traffic.

Area of application - access via VPN

With the SOFTNET Security Client, a PC/PG is configured automatically so that it can establish IPsec tunnels to one or more SCALANCE S modules.

This communication via these IPsec tunnels makes it possible for PG/PC applications such as NCM (Network and Communication Management) diagnostics or with STEP 7 to securely access devices or networks that are located in an internal network protected by SCALANCE S.

Note

Note that you can only use the SOFTNET Security Client in groups with modules in the active bridge mode.

Automatic communication via VPN

For your application, it is important that the SOFTNET Security Client automatically detects when there is access to the IP address of a VPN node. The nodes are addressed via the IP address as if they were in the local subnet to which the programming device / PC is also connected with this application.

How it works

The SOFTNET Security Client reads in the configuration created by the Security Configuration Tool and obtains the required information on the certificates to be imported from the relevant file. The root certificate and the private keys are imported and stored on the local PG / PC. Following this, security settings are made based on the data from the configuration so that applications can access IP addresses downstream from the SCALANCE S modules.

If a learning mode for the internal nodes or programmable controllers is enabled, the configuration module first sets a security policy for the secure access to the SCALANCE S modules. The SOFTNET Security Client then addresses the SCALANCE S modules to obtain the IP addresses of the relevant internal nodes. The SOFTNET Security Client registers these IP addresses in special filter lists belonging to this security policy. Following this, applications such as STEP 7 can communicate with the programmable controllers via VPN.

Article numbers

The SOFTNET Security Client software for establishing secure IP-based VPN connections from the PG /PC to network segments secured by SCALANCE S can be supplied for the following Windows operating systems.

- 1 single license for one installation,
- runtime software (German / English),
- Configuration tool (German / English),
- The electronic manual on CD-ROM is available in the following languages:
 - German
 - English
 - French
 - Spanish
 - Italian

SOFTNET Security Client Edition 2008	For Microsoft Windows XP Professional, 32-bit incl. SP1, SP2 and SP3	6GK1 704-1VW02-0AA0
SOFTNET Security Client V3	For Microsoft Windows 7 Professional, Ultimate and XP Professional 32-bit, incl. SP3	6GK1 704-1VW03-0AA0
SOFTNET Security Client V4	For Microsoft Windows 7 Professional, Ultimate, 32/64-bit	6GK1 704-1VW04-0AA0

4.8 Network management software

4.8.1 SINEMA server

Introduction

The SINEMA Server software was specifically developed for industrial applications. By using SNMP for all classic network components and by evaluating SIMATIC and PROFINET modules in the automation environment, networks can be fully analyzed and monitored. The acquired data is stored in a long-term archive and can be evaluated as necessary and shown in reports. The acquired network diagnostics can also be integrated seamlessly via OPC and Web mechanisms in HMI/SCADA systems (e.g. WinCC, PCS 7).

Note

You will find more detailed information on SINEMA Server in SINEMA (<http://www.siemens.com/sinema>)

Features and functions

- **Simple operability**
All the user interfaces are designed to make operation simple and clear. Complex training can therefore be greatly reduced.
- **Automatic detection of all components in the network**
Via SNMP but also by reading out PROFINET data produces clear lists of all the components in the network. Apart from the classic I&M data, here detailed information e.g. on PROFINET properties, redundancy protocols or WLAN status can be read out and displayed.
- **Clear representation of the network topology**
The topology of a network is read out using SNMP and PROFINET and displayed clearly. Topologies can be displayed in detail or in a structural icon view.
- **Event-based message system for transparent presentation of the network diagnostics**
The network is monitored continuously and the user is informed of status changes (e.g. redundancy errors, PROFINET diagnostics, bad frames).
- **SIMATIC diagnostics (S7-300, S7-400)**
By reading out and monitoring cycle times or the evaluation of specific SIMATIC diagnostics, the classic network diagnostics can be enriched with applicative SIMATIC diagnostics.
- **PROFINET diagnostics**
By using PROFINET, the diagnostics of modules does not end at their Ethernet interface. The applicative status of a PROFINET module now provides detailed status information.
- **Standardized network documentation (reports), even over longer periods** Reports are available for a wide range of evaluations (availability, performance, device inventory,

events). Thanks to the database-based architecture evaluations can be made over long periods of the past.

- **User-based adaptation of the user interfaces**
The user and user group management allows users with staggered rights to be managed. Users can not only be assigned different rights but also different plant areas. User interface settings are also stored for specific users.
- **Access possible via every standard browser**
SINEMA Server is Web-based application. This has the advantage that up to 20 users can connect to the server at the same time. For this, a local Internet browser is adequate.
- **Multiple server status view "Server Overview"**
With the "Server Overview" function, the status of up to 100 servers can be displayed. Trend graphs provide detailed information of the diagnostics development of servers.
- **Export of data by CSV for multiple server evaluation**
With a URL call, information (as CSV) of many servers can be queried. This makes it possible to bundle and evaluate cross-server data.
- **Profile concept for integration of any network nodes**
Using profiles that can be adapted to your own requirements, it is possible to make any network components known in SINEMA Server. Profiles can be imported/exported manually or loaded automatically with "Device profile synchronization".
- **HMI connection via URL and OPC server**
To integrate diagnostics data from SINEMA Server in an HMI system, there is a flexible URL mechanism and a fully fledged OPC server available.

4.8.2 Primary Setup Tool

Description

With the Primary Setup Tool (PST), an address assignment (for example an IP address) is made via the network for unconfigured SIMATIC NET network components, Ethernet CPs and gateways. This is only possible if the SIMATIC NET devices have a default ETHERNET (MAC) address and can be reached online in the network. The nodes must also support the DCP protocol. The PST uses a filter view to allow a clear presentation of modules and devices.

Note

The Primary Setup Tool supports only SIMATIC NET Ethernet network components with management functionality (Web-based Management and/or SNMP). With these components, you also have the option of calling Web-based Management for diagnostics and configuration.

Functions

Depending on the properties of the addressed components and interfaces, the following functions are available in the PST:

- Basic functions:
 - Browsing for devices with an Ethernet interface
 - Calling up Web Based Management
 - Downloading configurations to the components
 - Using functions via the DOS command line
- Configuration for Ind. Ethernet / PROFINET
 - Settings for IP addresses
- Configuration for PROFIBUS (for devices with Ethernet and PROFIBUS interfaces)
 - Setting the PROFIBUS address
 - PROFIBUS bus parameters

The PST provides these functions via a user-friendly user interface.

Requirements

- The devices have a preset ETHERNET (MAC) address or an IP address and can be reached on the network online.
- PROFIBUS interfaces can also be configured using PST only for modules that also have a reachable Ethernet interface in the network in addition to the PROFIBUS interface.

Supported operating systems

The Primary Setup Tool can be installed and executed under the following operating systems:

- 32-bit operating systems
 - Windows XP Professional SP2 and SP3
 - Windows 7 Professional / Ultimate
- 64-bit operating systems
 - Windows 7 Professional / Ultimate SP1
 - Windows Server 2008 Standard Server R2

It is possible to set addresses for the following SIMATIC NET network components using PST:

- ELS TP40 M
- SCALANCE W700
- SCALANCE X200
- SCALANCE X300
- SCALANCE X400
- SCALANCE XR-500M

It is possible to set addresses for the following Ethernet CPs using PST:

- CP 343-1
- CP 343-1 Lean
- CP 343-1 Advanced
- CP343-1 ERPC
- CP 343-1 BACnet
- CP 443-1
- CP 443-1 Advanced

It is possible to set addresses for the following SIMATIC NET gateways using PST:

- IE/PB Link
- IE/PB Link PN IO
- IWLAN/PB Link

DCP protocol and DLC protocol

The Primary Setup Tool uses the protocols DCP (Discovery and basic Configuration Protocol) and DLC (Data Link Control) for communication with the modules. The DLC protocol is necessary for devices with older firmware versions.

This includes the following devices:

- CP 443-1 (6GK7 443-1EX10 and 6GK7 443-1EX11)

Note

The DLC protocol is not supported in 64-bit operating systems. The DLC protocol is not available either in the setup or during operation of the Primary Setup Tool.

Note

Depending of the operating system you are using, remember the following if you want to use the DLC protocol:

- Windows 7 Professional / Ultimate
The DLC protocol is not included in Windows, but it can be installed and enabled during installation of the PST.
Hardware requirements at least: Clock frequency 1 GHz / 1 GB RAM / screen resolution 1024 x 768 / color quality 16 bit
 - Windows XP Professional
The DLC protocol is not included in Windows, but it can be installed and enabled during installation of the PST.
Hardware requirements at least: Clock frequency 600 MHz / 512 MB RAM / screen resolution 1024 x 768 / color quality 16 bit
-

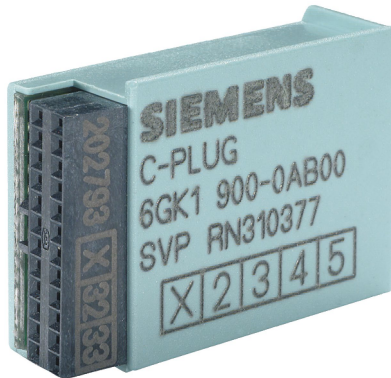
Note

You will find more detailed information on the Primary Setup Tool and on downloading the software at 19440762
(<http://support.automation.siemens.com/WW/view/en/19440762>).

4.9 Accessories

4.9.1 C-PLUG Configuration Memory

Description



The C-PLUG is an exchangeable medium for storage of the configuration and project engineering data of the base device. This means that the configuration data remains available if the basic device is replaced. It is therefore used when the replacement of network components or communications modules needs to be quick if a fault occurs without needing to configure a replacement and without needing specialist personnel. Downtimes of network segments and connected Industrial Ethernet nodes can therefore be minimized if a fault occurs.

It can be used in all SIMATIC NET products with a C-PLUG slot.

Structure

The C-PLUG has degree of protection IP20. With IP65 components, the protection is retained because the C-PLUG is installed inside the protected housing.

Power is supplied by the end device. The C-PLUG retains all data when the power is turned off.

Function

If an empty C-PLUG (as supplied) is inserted in a SIMATIC NET component, the device automatically backs up the configuration data during startup. Changes to the configuration during operation are also saved on the C-PLUG without any additional operator intervention being necessary.

When an unconfigured device starts up, it automatically adopts the configuration data of an inserted C-PLUG assuming the data was written by a compatible device type.

The C-PLUG can also be used to store application data such as documentation or Web pages.

Diagnostics

Incorrect use of the C-PLUG, such as inserting a C-PLUG containing the configuration of a different device group or general malfunctions of the C-PLUG are indicated by diagnostics mechanisms of the end device (LEDs, PROFINET, SNMP, Web based Management, etc.).

Article number

C-PLUG	Exchangeable storage medium for simple replacement of the devices if a fault occurs, can be inserted in SIMATIC NET products with a C-PLUG slot.	6GK1900-0AB00
---------------	--	----------------------

4.9.2 KEY-PLUG

Description



Figure 4-49 KEY-PLUG

With some devices an optional exchangeable medium with a key function is required to enable functions; a KEY-PLUG. In terms of structure, function and behavior, a KEY-PLUG corresponds to the C-PLUG, in addition the KEY-PLUG contains the release licenses. There are several variants of the KEY-PLUG for the SCALANCE W and SCALANCE X series.

KEY-PLUG for SCALANCE W:

With SCALANCE W, the KEY-PLUG releases security functions and iFeatures. The following versions exist:

- **KEY-PLUG W700 SECURITY**
Activates the Inter AP blocking function. This function is available only in access point mode.
- **KEY-PLUG W740 iFeatures**
Activates the iPCF and iPCF-MC functions for clients.
- **KEY-PLUG W780 iFeatures**
Activates the following functions for access points:
 - iPCF
 - iPCF-MC
 - iREF
 - Aeroscout
 - Inter AP blocking

KEY-PLUG for SCALANCE X

With SCALANCE X, the KEY-PLUG activates the layer 3 functions (routing). The following versions exist:

- **KEY-PLUG XM-400 LAYER 3 ROUTING**
- **KEY-PLUG XR-500 LAYER 3 ROUTING**

Inserting/removing the KEY-PLUG.

Inserting or removing the KEY-PLUG is analogous to inserting or removing the C-PLUG. Follow the instructions in the device manual on inserting/removing the C-PLUG.

Article numbers

KEY-PLUG W700 SECURITY	Activates Inter AP blocking function.	6GK5907-0PA00
KEY-PLUG W740 iFeatures	Activates the iFeatures for clients.	6GK5907-4PA00
KEY-PLUG W780 iFeatures	Activates the iFeatures for access points.	6GK5907-8PA00
KEY-PLUG XM-400 LAYER 3 ROUTING	Activates the layer 3 functions for devices of the XM-400 series.	6GK5904-0PA00
KEY-PLUG XR-500 LAYER 3 ROUTING	Activates the layer 3 functions for devices of the XR-500 series.	6GK5905-0PA00

Communications processors for PCs

Application

Communications processors for PCs/PGs allow you to establish a connection to industrial Ethernet with a PC/PG or a SIMATIC Microbox PC (PCI-104 interface). There are two categories of communications processors for PCs/PGs:

- Communications processors with their own microprocessor.
This relieves the PC/PG CPU. This frees up computing power on the PC for other applications, for example HMI (ISO and TCP/IP transport on board).
- Communications processors without their own microprocessor.
These communications processors are less expensive than the communications processors that have their own microprocessor. If there is, however, heavy load on the PC microprocessor, it is possible that the protocol stack does not receive a time slice and this leads to the connection being terminated. When using communications processors with their own microprocessor, this does not occur.

Example of a topology

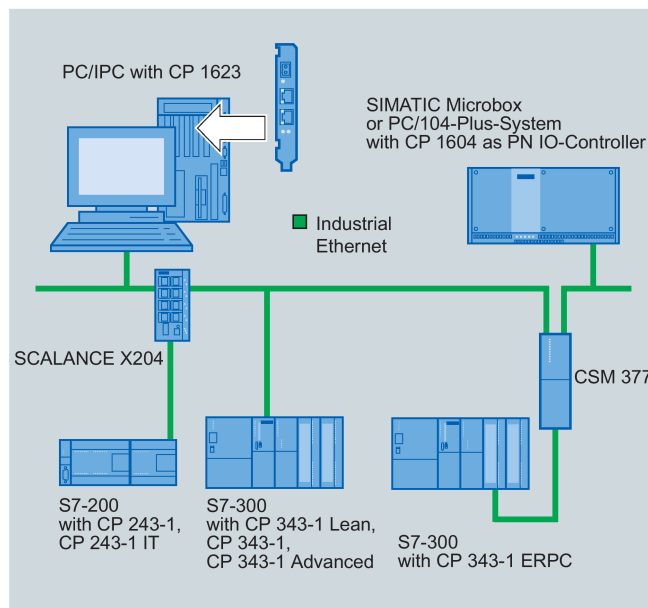


Figure 5-1 Connecting communications processors for PCs/PGs to Industrial Ethernet based on the example of a linear bus topology

Device variants

Functionality	CP 1604	CP 1616	CP 1612 A2	CP 1613 A2	CP 1623	CP 1628 ¹⁾
Interfaces						
→ PCI		•	•	•		
→ PCI Express					•	•
→ PCI-104	•					
Connections						
→ RJ-45	4	4	1	1	2	2
Configurable connections	128	128	64	120	120	120
Gigabit Ethernet			•		•	•
Integrated switch	•	•			•	•
PNIO	•	•	•			

- Suitable / available or according to the specified standard.

5.1 CP 1604

Description

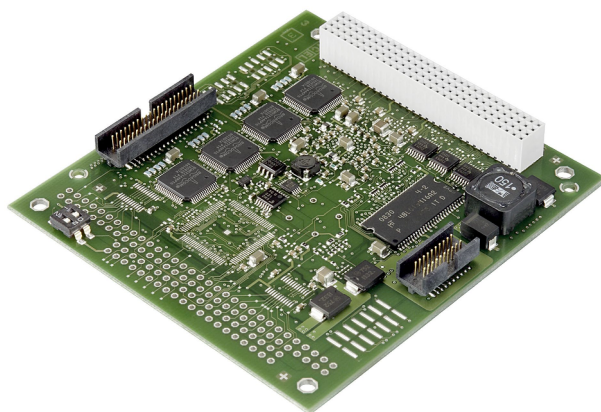


Figure 5-2 CP 1604

The CP 1604 is a PCI-104 card with its own microprocessor Ethernet real-time ASIC ERTEC 400 with which PNIO communication is also possible. This module has an integrated 4-port real-time switch for 10 / 100 Mbps.

Features

	CP 1604
Required slot on the PC	PCI-104
Number and type of the interfaces for Industrial Ethernet	4 x RJ-45
Gigabit Ethernet	-
Own microprocessor	•
Optional external power supply 12 ... 24 VDC	•

Functions

- Up to 128 connections can be configured at one time.
- Data rates 10 / 100 Mbps (half/full duplex) are supported.
- Autocrossover and autonegotiation
- IRT (Isochronous Real Time)
- Network management and diagnostics using SNMP.
- Supported protocols

ISO	TCP/UDP	PN	MRP	OPC	PG/OP	S7/S5	IT
	•	•	•				

- Suitable / available or according to the specified standard.

Article numbers

CP 1604	PCI 104 card (32-bit) with ASIC ERTEC 400 for connection of PCI/104 systems to a PROFINET IO with 4-port real-time switch (RJ-45); including IO-Base software for PROFINET IO controller and NCM PC; 1 single license for one installation, runtime software, software and electronic manual on CD-ROM, class A, for Microsoft Windows XP Professional (32-bit) and Windows 7; other operating systems using the Development Kit DK-16xx PN IO Languages: German / English	6GK1160-4AA00
----------------	--	----------------------

5.2 CP 1616

Description

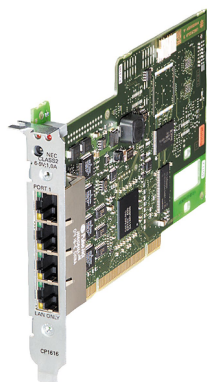


Figure 5-3 CP 1616

The CP 1616 is a PCI card with its own microprocessor and an integrated 4-port switch for connecting PCs and SIMATIC PGs/PCs to PROFINET IO. The module universal keyed 3.3 V and 5 V; 33 MHz / 66 MHz/66 MHz; 32-bit, can operate in 64-bit PCI-X systems)

Features

	CP 1616
Required slot on the PC	PCI
Number and type of the interfaces for Industrial Ethernet	4 x RJ-45
Gigabit Ethernet	-
Own microprocessor	•
Optional external power supply 6 ... 9 VDC	•

Functions

- Up to 128 connections can be configured at one time.
- Data rates 10 / 100 Mbps (half/full duplex) are supported.
- Autosensing, autocrossover and autonegotiation
- IRT (Isochronous Real Time)
- Network management and diagnostics using SNMP.
- Supported protocols

ISO	TCP/UDP	PN	MRP	OPC	PG/OP	S7/S5	IT
	•	•	•				

- Suitable / available or according to the specified standard.

Article numbers

CP 1616	PCI-104 card (32-bit; 3.3 / 5 V universal keyed) with ASIC ERTEC 400 for connecting PCs to PROFINET IO with 4-port real-time switch (RJ-45); including IO-Base software for PROFINET IO controller and NCM PC; 1 single license for one installation, runtime software, software and electronic handbook on CD-ROM, class A, for Microsoft Windows XP Professional (32-bit) and Windows 7; other operating systems using the Development Kit DK-16xx PN IO Languages: German / English	6GK1161-6AA01
----------------	---	----------------------

5.3 CP 1612 A2

Description

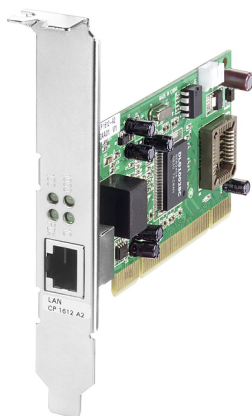


Figure 5-4 CP 1612 A2

The CP 1612 A2 is a PCI card without its own microprocessor for connecting PCs and SIMATIC PGs/PCs to PROFINET IO.

Features

	CP 1612 A2
Required slot on the PC	PCI
Number and type of the interfaces for Industrial Ethernet	1 x RJ-45
Gigabit Ethernet	•
Own microprocessor	-
Optional external power supply	-

Functions

- Up to 512 connections can be configured at one time.
- Data rates 10 / 100 / 1000 Mbps (half/full duplex) are supported.
- Autonegotiation
- Supported protocols

ISO	TCP/UDP	PN	MRP	OPC	PG/OP	S7/S5	IT
•	•	•		•	•	•	•

- Suitable / available or according to the specified standard.

Article numbers

CP 1612 A2	PCI card (32-bit; 33 / 66 MHz, 3.3 / 5 V universal keyed) for connection to Industrial Ethernet (10 / 100 / 1000 Mbps) with RJ-45 connector; including driver for Microsoft Windows XP Professional (32-bit), Service Pack 2 / 3, 2003 R2 Server SP2, Vista Business / Ultimate SP1 and Windows 2008 Server Languages: German / English	6GK1161-2AA01
-------------------	--	----------------------

5.4 CP 1613 A2

Description

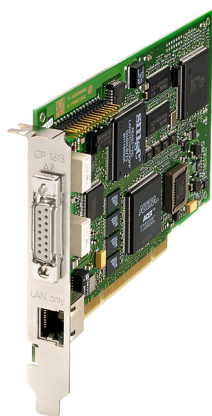


Figure 5-5 CP 1613 A2

The CP 1613 A2 is a PCI card with its own microprocessor for connecting PCs and SIMATIC PGs/PCs to Industrial Ethernet. PNIO is not supported by this module.

Features

	CP 1613 A2
Required slot on the PC	PCI
Number and type of the interfaces for Industrial Ethernet	1 x RJ-45 1 x ITP 15-pin
Gigabit Ethernet	-
Own microprocessor	•
Optional external power supply	-

Functions

- Up to 120 connections can be configured at one time.
- Data rates 10 / 100 / 1000 Mbps (half/full duplex) are supported.
- Autonegotiation
- Time-of-day synchronization
- SNMP-supported diagnostics
- Supported protocols

ISO	TCP/UDP	PN	MRP	OPC	PG/OP	S7/S5	IT
•	•			•	•	•	•

- Suitable / available or according to the specified standard.

Article numbers

CP 1613 A2	PCI card (32-bit; 33 / 66 MHz, 3.3 / 5 V universal keyed) for connection to Industrial Ethernet (10 / 100 Mbps) with RJ-45 connector via HARDNET-IE S7 /S7-1613 and S7 REDCONNECT; Support of operating systems according to the SIMATIC NET software	6GK1161-3AA01
-------------------	--	----------------------

5.5 CP 1623

Description

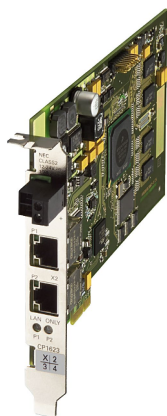


Figure 5-6 CP 1623

The CP 1623 is a PCI Express card with its own microprocessor and integrated 2-port switch for connecting PCs and SIMATIC PGs/PCs to Industrial Ethernet. PNIO is not supported by this module.

Features

	CP 1623
Required slot on the PC	PCI Express
Number and type of the interfaces for Industrial Ethernet	2 x RJ-45
Gigabit Ethernet	•
Own microprocessor	•
Optional external power supply 12 ... 24 VDC	•

Functions

- Up to 120 connections can be configured at one time.
- Data rates 10 / 100 / 1000 Mbps (half/full duplex) are supported.
- Autocrossover and autonegotiation
- Time-of-day synchronization
- SNMP-supported diagnostics
- Supported protocols

ISO	TCP/UDP	PN	MRP	OPC	PG/OP	S7/S5	IT
•	•			•	•	•	•

- Suitable / available or according to the specified standard.

Article numbers

CP 1623	PCI Express x1 card for connection to Industrial Ethernet (10 / 100 / 1000 Mbps), with 2-port switch (RJ-45) via HARDNET-IE S7 /S7-1613 and S7 REDCONNECT; Support of operating systems according to the SIMATIC NET software	6GK1162-3AA00
----------------	--	----------------------

5.6 CP 1628

Description

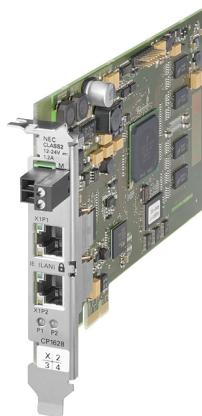


Figure 5-7 CP 1628

The CP 1628 is a PCI Express card with its own microprocessor and integrated 2-port switch for connecting PCs and SIMATIC PGs/PCs to Industrial Ethernet. PNIO is not supported by this module.

Features

	CP 1628
Required slot on the PC	PCI Express
Number and type of the interfaces for Industrial Ethernet	2 x RJ-45
Gigabit Ethernet	•
Own microprocessor	•
Optional external power supply 12 ... 24 VDC	•

Functions

- Up to 512 connections can be configured at one time.
- Data rates 10 / 100 / 1000 Mbps (half/full duplex) are supported.
- Autocrossover and autonegotiation
- Time-of-day synchronization
- SNMP-supported diagnostics
- Security mechanisms
- Supported protocols

ISO	TCP/UDP	PN	MRP	OPC	PG/OP	S7/S5	IT
•	•			•	•	•	•

- Suitable / available or according to the specified standard.

Article numbers

CP 1628	PCI Express x1 card for connection to Industrial Ethernet (110 / 100 / 1000 Mbps), with 2-port switch (RJ-45) and integrated security (fire-wall, VPN) via HARDNET-IE S7 and S7 REDCONNECT; Support of operating systems according to the SIMATIC NET software	6GK1162-8AA00 ¹⁾
----------------	---	------------------------------------

Communications processors for SIMATIC S7

Description

For each SIMATIC S7 system, there are communications processors (CPs) that provide a connection to Industrial Ethernet. This means that S7 controllers can exchange data with other network nodes via Industrial Ethernet. These network nodes can be other S7-CPs/CPU or PCs with an Ethernet card. This allows remote programming and diagnostics via the PG/PC. With the communications processors that support PROFINET, PROFINET IO-compliant field devices can be addressed directly.

SIPLUS

For applications in harsh environmental conditions, in aggressive environments or in extreme temperature ranges, the standard properties of an individual device or system are often inadequate. Due to deployment in such locations, there may be restrictions to the functionality or operational reliability and even total failure of a system.

The product types designed to meet such requirements are identified by '**SIPLUS**' being appended to the name. The products are certified according to EN 60721-3C4, -3S4, -3B2 as well as ISA S71.04-G1, -G2, -G3 and -GX.

The modules are designed for use in humidity of up to 100%, condensation and salty atmospheres due to conformal coating. These properties also protect the products from dendrite formation and micro corrosion.

Based on the industrial automation system SIMATIC S7-300, two upgraded SIPLUS versions are available.

- For an expanded temperature range of -25 °C to +60 °C and some devices up to +70 °C.
- Unusual environmental load (conformal coating) and electronic equipment on rolling stock conforming with EN 50155.

Note

SIPLUS

You will find more detailed information and the technical documentation on SIPLUS in the portal of Siemens AG: <http://www.siemens.eu/siplus-extreme>

Device types of the SIMATIC S7 CPs (communications processors)

The following graphic shows the various device types and the corresponding categories of the **SIMATIC S7** product line.

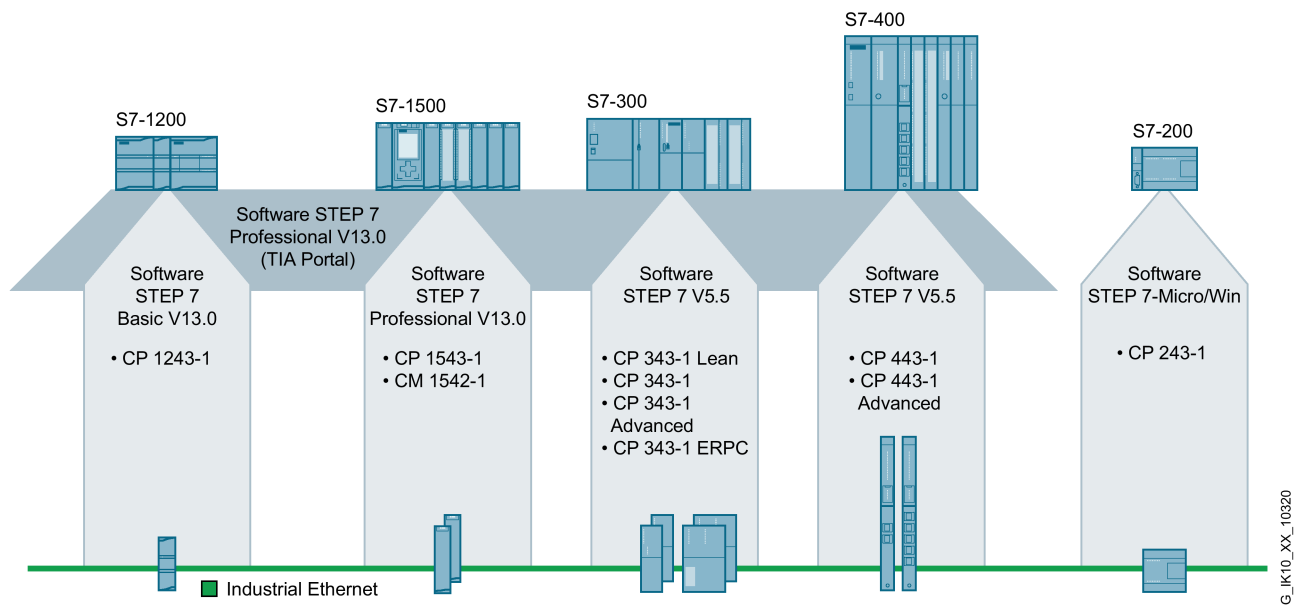


Figure 6-1 SIMATIC S7: CP - communications processors

Example of a topology

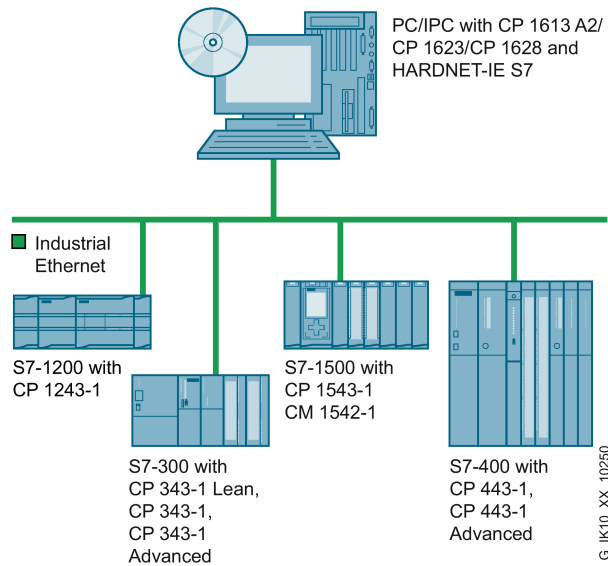


Figure 6-2 Connecting S7 systems to Industrial Ethernet based on the example of a linear bus topology.

6.1 Communications processors for SIMATIC S7-200

Description



Figure 6-3 CP 243-1

The communications processors of the category SIMATIC S-200 have a rugged plastic housing with IP20 degree of protection for installation on a DIN rail or for wall mounting. The connection to an S7-200 is made via a backplane bus.

Features

Functionality	CP 243-1
External power supply 24 VDC	•
Connection to Industrial Ethernet/PROFINET	1 x RJ-45
Gigabit interface	-

- Suitable / available or according to the specified standard.

Functions

- Up to 8 connections can be configured.
- Data rates 10 / 100 Mbps (half/full duplex) are supported along with the autocrossing function.
- A module can be replaced without a programming device because the project engineering data of the CP is stored on the S7-200 CPU.
- Diagnostics LED
- 8 MB flash memory with file system

- File exchange with other computers using FTP.
- Integrated HTTP server for a maximum of four connections that allows write and read access to process and status data of the S7-200 system. This means, for example, that system diagnostics is possible via a Web browser.
- Integrated SMTP client for event-driven sending of e-mails. Up to 32 e-mails can be configured and these can also contain variables. The current value of such a variable is queried as soon as the program of the S7-200 CPU triggers the sending of the corresponding e-mail.
- Supported protocols and technologies:

PROFINET			ISO	TCP/UDP	MRP	IT	IP-R	FTP	PG/OP	S7
IO-C	IO-D	CBA								
						•		•	•	•

- Suitable / available or according to the specified standard.

Article numbers

CP 243-1	For connecting SIMATIC S7-200 to Industrial Ethernet; for S7 communication, PG communication, e-mail and WWW server; incl. electronic manual on CD-ROM in the languages: German, English, French, Italian, Spanish	6GK7243-1EX01-0XE0
-----------------	---	---------------------------

6.2 Communications processors for SIMATIC S7-300

Description



Figure 6-4 SIMATIC S7-300: CP 343-1 Lean and CP 343-1 Advanced

The communications processors of the category SIMATIC S-300 have a rugged plastic housing with IP20 degree of protection for installation on an S7300 standard rail. The connection to S7-300 components is made via a backplane bus.

Features

Functionality	CP 343-1 Lean SIPLUS CP 343-1 Lean	CP 343-1 SIPLUS CP 343-1	CP 343-1 Advanced SIPLUS CP 343-1 Advanced	CP 343-1 ERPC
External power supply 24 VDC	•	•	•	•
Connections to Industrial Ethernet/PROFINET	1 x RJ-45	2 x RJ-45	2 x RJ-45	2 x RJ-45
Integrated 2-port switch	-	•	•	•
Gigabit interface	-	-	•	•
30 MB flash memory 28 MB RAM	-	-	•	-
C-PLUG not included with the product	-	-	•	•

- Suitable / available or according to the specified standard.

Functions

The communications processors of this category support the following protocols and technologies:

Functionality	CP 343-1 Lean SIPLUS CP 343-1 Lean	CP 343-1 SIPLUS CP 343-1	CP 343-1 Advanced SIPLUS CP 343-1 Advanced	CP 343-1 ERPC
PROFINET				
→ IO controller	-	•	•	-
→ IO device	•	•	•	-
→ CBA	-	-	•	-
ISO	-	•	•	-
TCP/UDP	•	•	•	•
MRP	•	•	•	-
IT	-	-	•	-
IP-R	-	-	•	-
FTP	-	-	•	-
PG/OP	•	•	•	•
S7/S5	•	•	•	•

- Suitable / available or according to the specified standard.

CP 343-1 Lean / SIPLUS 343-1 Lean

The CP 343-1 Lean and the SIPLUS 343-1 Lean are designed for connection of a SIMATIC S7-300 system to Industrial Ethernet networks also as a PROFINET IO device.

The device has the following characteristics and functions:

- A PROFINET interface with two RJ-45 connectors,
- 10 /100 Mbps, full / half duplex with the functionality for autosensing and autocrossover via an integrated 2-port switch.
- Media redundancy (MRP):
 - Within an Ethernet network with a ring topology, the communications processor supports the media redundancy protocol MRP
- Diagnostics and network management:
 - Extensive diagnostics functions of all modules of the rack
 - Integration in network management systems by supporting SNMP V1
- Configuration of all functions with STEP 7 as of V5.4 or STEP 7 Professional V11.
- Module replacement without PG by storing the configuration data on the CPU.

- Connector for connecting SIMATIC S7-300 systems to Industrial Ethernet, except for SINUMERIK.
 - Two RJ-45 interfaces for 10 / 100 Mbps full and half duplex connection including autosensing for automatic switchover and the autocrossover function.
 - Integrated 2-port real-time ERTEC switch
 - Multiprotocol operation with TCP and UDP transport protocol and PROFINET IO
 - Keepalive function
- Multicast for UDP
- Full remote programming and initialization are possible via Industrial Ethernet.
- IT communication incl. Web functionality.
- Integration in network management systems using SNMP.
- The data is configured in STEP 7.
- Inter-network PG/OP communication with S7 routing.
- Diagnostics options in STEP 7 and via a Web browser.
- SIPLUS CP 343-1 Lean

The SIPLUS CP 343-1 Lean is intended for use under extreme environmental conditions. One variant of the SIPLUS CP 343-1 Lean for harsh environmental conditions is designed for ambient temperatures from -25 °C to +60 °C.

CP 343-1 / SIPLUS CP 343-1

The CP 343-1 and the SIPLUS CP 343-1 have the following characteristics and functions:

- A PROFINET interface with two RJ-45 connectors.
- 10 /100 Mbps, full / half duplex with the functionality for autosensing and autocrossover via an integrated 2-port switch.
- With access protection with the ACL (Access Control List), CP 343-1 communication can be restricted to partners with specific IP addresses.
- For the PROFINET interface, you can specify how the IP configuration (IP address, subnet mask and gateway address) is obtained.
- PROFINET IO controller or PROFINET IO device
- Communications services:
 - Open communication with TCP/IP, UDP, multicast for UDP and ISO.
 - Inter-network PG/OP communication with S7 routing.
 - S7 communication (client, server, multiplexing)
- Media redundancy (MRP):
 - Within an Ethernet network with a ring topology, the CP 343-1 supports the media redundancy protocol MRP.

- Diagnostics and network management:
 - Extensive diagnostics functions of all modules in the rack.
 - Integration in network management systems by support of SNMP V1.
- Security mechanisms:

Access protection with a configurable IP-ACL (IP Access Control List).
- Configuration of all functions with STEP 7 as of V5.4 or STEP 7 Professional V11.
- Module replacement without PG by storing the configuration data on the CPU.
- SIPLUS CP 343-1

The SIPLUS CP 343-1 module is intended for environmental loads at ambient temperatures of 0°C to +60°C. One variant of the SIPLUS CP 343-1 is designed for harsh environmental conditions at ambient temperatures from -25 °C to +70 °C.

CP 343-1 Advanced / SIPLUS CP 343-1 Advanced

The CP 343-1 Advanced and the SIPLUS CP 343-1 Advanced have the same range of functions as the CP 343-1 / SIPLUS CP 343-1. They also have the following additional characteristics and functions:

- Two separate interfaces (integrated network separation)
 - Gigabit interface
 - PROFINET interfaces:

CBA, IO controller and IO device with the real-time properties RT and IRT.
- 30 MB of flash memory with a file system for user-defined HTML pages and 30 MB of RAM for buffering dynamic data.
- File exchange with other computers using FTP.
- An integrated HTTP server that allows write and read access to process and status data of the S7-300 system. System diagnostics is therefore possible via a secure Web browser.
- An integrated ESMTTP client for secure, event-dependent sending of e-mails that can also contain variables. The current value of such a variable is queried when the program of the S7-300 CPU triggers the sending of the corresponding e-mail.
- A C-PLUG for storing the configuration data ships with the product.
- CP 343-1 Advanced with security function: Security of the system against unauthorized access by
 - Central access protection for any devices within an automation cell, for example by secure authentication of the network nodes.
 - Secure remote access via Internet thanks to data encryption (VPN)
 - Data integrity check
 - Traceability with data logging based on standard IT mechanisms (Syslog)
- SIPLUS CP 343-1 Advanced

The SIPLUS CP 343-1 Advanced module is intended for harsh environmental loads at ambient temperatures of 0°C to +60°C.

CP 343-1 ERPC (Enterprise Connect)

The CP 343-1 ERPC communications processor (Enterprise Connect) is designed to connect a SIMATIC S7-300 system to Industrial Ethernet networks.

The CP supports the following:

- PG/OP communication
- S7 communication
- Open communication (SEND/ RECEIVE)
- ERPC communication
- Direct interfacing with database applications such as ORACLE, MySQL, MS-SQL, DB2. This allows controllers to be supplied with data or jobs directly from databases of manufacturing execution systems (MES) or the enterprise resource planning level (ERP).

Note

Database connection of the SIMATIC S7-300 to various database systems for vertical integration is supported by a firmware expansion from the ILS-Technology company that must be ordered separately.

- A C-PLUG for storing the configuration data ships with the product.
- Optimum support of maintenance with:
 - Web-based diagnostics
 - Remote programming via LAN/WAN
 - Monitoring using the network management tool (SNMP)
 - Module replacement without PG using the C-PLUG exchangeable medium
- Access protection with a configurable IP-ACL (IP Access Control List)

The CP 343-1 ERPC communications processor allows subsequent connection to existing SIMATIC S7 systems within Industrial Ethernet.

Article numbers

CP 343-1 Lean	To connect SIMATIC S7-300 in Industrial Ethernet using TCP/IP and UDP multicast. S7 communication, open communication (SEND/RECEIVE), FETCH/WRITE, PROFINET IO device, MRP, integrated 2-port switch ERTEC, wide-ranging diagnostics options, module replacement without PG, SNMP, initialization via LAN; incl. electronic manual on CD-ROM.	6GK7343-1CX10-0XE0
SIPLUS CP 343-1 Lean	For an extended temperature range and harsh environmental loads. To connect SIMATIC S7-300 in Industrial Ethernet using TCP/IP and UDP, multicast. S7 communication, open communication (SEND/RECEIVE), FETCH/WRITE, PROFINET IO device, integrated 2-port switch ERTEC, wide-ranging diagnostics options, module replacement without PG, SNMP, initialization via LAN; incl. electronic manual on CD-ROM. Ambient temperature from 0 °C to +60 °C	6AG1343-1CX10-4XE0
	Ambient temperature from -25 °C to +60 °C	6AG1343-1CX10-2XE0
CP 343-1	For connecting SIMATIC S7-300 in Industrial Ethernet via ISO and TCP/IP; PROFINET IO controller or PROFINET IO device, MRP, integrated 2-port switch ERTEC. S7 communication, open communication (SEND/RECEIVE), FETCH/WRITE, with and without RFC 1006, multicast, DHCP, time-of-day synchronization of CPU with SIMATIC mode and NTP, diagnostics, SNMP, access protection using IP access list, initialization via LAN 10/100 Mbps; incl. electronic manual on DVD.	6GK7343-1EX30-0XE0
SIPLUS CP 343-1	For an extended temperature range and harsh environmental loads. For connecting SIMATIC S7-300 in Industrial Ethernet using ISO and TCP/IP, PROFINET IO controller or PROFINET IO device. S7 communication, open communication (SEND/RECEIVE), FETCH/WRITE, with and without RFC 1006, multicast, DHCP, time-of-day synchronization of CPU with SIMATIC mode and NTP, diagnostics, SNMP, access protection using IP access list, initialization via LAN 10/100 Mbps; incl. electronic manual on DVD. Ambient temperature from 0 °C to +60 °C	6AG1343-1EX30-4XE0
	Ambient temperature from -25 °C to +70 °C	6AG1343-1EX30-7XE0
CP 343-1 Advanced	For connecting SIMATIC S7-300 in Industrial Ethernet. 1 x 10 / 100 / 1000 Mbps; 2 x 10 / 100 Mbps (IE SWITCH); RJ-45 ports; TCP; UDP; ISO; PROFINET IO controller and IO device, S7 communication (client and server). Open communication (SEND/RECEIVE); S7 routing; IP configuration using DHCP/block; advanced Web diagnostics; time-of-day synchronization; IP access control list; IP routing; FTP; e-mail; PROFINET CBA; C-PLUG. Without security function.	6GK7343-1GX30-0XE0
	With security function, firewall, VPN and PROFINET energy (controller and device).	6GK7343-1GX31-0XE0

SIPLUS CP 343-1 Advanced	For connecting SIMATIC S7-300 in Industrial Ethernet. 1 x 10/100/1000 Mbps; 2 x 10/100 Mbps (IE SWITCH); RJ-45 ports; TCP; UDP; ISO; PROFINET IO controller and IO device, S7 communication (client and server). Open communication (SEND/RECEIVE); S7 routing; IP configuration using DHCP/block; advanced Web diagnostics; time-of-day synchronization; IP access control list; IP routing; FTP; e-mail; PROFINET CBA; C-PLUG. Ambient temperature from 0 °C to +60 °C	6AG1343-1GX30-4XE0
CP 343-1 ERPC (Enterprise Connect)	For connecting SIMATIC S7-300 in Industrial Ethernet and to support the database connection of the SIMATIC S7-300 to various databases, TCP/UDP. S7 communication, open communication (SEND/RECEIVE), with and without RFC 1006; multicast; Web server, time-of-day synchronization of the CPU with SIMATIC mode and NTP, access protection using IP access list, SNMP, DHCP, initialization via LAN 10/100/1000 Mbps, incl. electronic manual on DVD. A C-PLUG ships with the product.	6GK7343-1FX00-0XE0

6.3 Communications processors SINAUT ST7 for SIMATIC S7-300

Description



Figure 6-5 SINAUT TIM 3V-IE

The SINAUT ST7 communications modules allow S7-300 stations SINAUT communication via telecommunications networks or IP-based networks. The devices have a rugged plastic housing with IP20 degree of protection for installation on an S7-300 standard rail.

Features

Functionality	TIM 3V-IE	TIM 3V-IE Advanced	TIM 3V-IE DNP3	TIM 4R-IE	TIM 4R-IE DNP3
Connections RS-232	1 x D-sub 9-pin	1 x D-sub 9-pin	1 x D-sub 9-pin	2 x D-sub 9-pin	2 x D-sub 9-pin
Connectors Industrial Ethernet	1 x RJ-45	1 x RJ-45	1 x RJ-45	2 x RJ-45	2 x RJ-45
Number of active connections multiprotocol mode	12	24	128	-	-
No. of TIMs per S7-300	1	Several ⁽¹⁾	Several ⁽¹⁾	1	1
DNP3 support	-	-	•	-	•
C-PLUG not included with the product	-	-	-	-	-

- Suitable / available or according to the specified standard.

Functions

The communications processors of this category support the following protocols:

Protocol	TIM 3V-IE	TIM 3V-IE Advanced	TIM 3V-IE DNP3	TIM 4R-IE	TIM 4R-IE DNP3
TCP/IP	•	•	•	•	•
DNP3	-	-	•	-	•
SINAUT ST1	•	•	-	•	-
SINAUT ST1	•	•	-	•	-
Modbus RTU	-	-	-	-	•

- Suitable / available or according to the specified standard.

The communications processors of this category have the following functions:

- Data buffering when there is a connection abort
- Configuration with SINAUT ST7 ES

Article numbers

TIM 3V-IE	SINAUT ST7, TIM 3V communications module for SIMATIC S7-300 with an RS-232 interface for SINAUT communication via a WAN and an RJ-45 interface for SINAUT communication via an IP-based network.	6NH7800-3BA00
TIM 3V-IE Advanced	SINAUT ST7, TIM 3V communications module for SIMATIC S7-300 with an RS-232 interface for SINAUT communication via a WAN and an RJ-45 interface for SINAUT communication via an IP-based network.	6NH7800-3CA00
TIM 3V-IE DNP3	TIM 3V communications module for SIMATIC S7-300 with an RS-232 interface for DNP3 communication via a WAN and an RJ-45 interface for DNP3 communication via an IP-based network.	6NH7803-3BA00-0AA0
TIM 4R-IE	SINAUT ST7, TIM 4R IE communications module for SIMATIC S7-300 with two RS-232 interfaces for SINAUT communication via a WAN and two RJ-45 interfaces for SINAUT communication via an IP-based network.	6NH7800-4BA00
TIM 4R-IE DNP3	TIM 4R IE communications module for SIMATIC S7-300 with two RS-232 interfaces for DNP3 communication via a WAN and two RJ-45 interfaces for DNP3 communication via an IP-based network.	6NH7803-4BA00-0AA0

6.4 Communications processors for SIMATIC S7-400

Description



Figure 6-6 CP 443-1, CP 443-1 Advanced and CP 443-1 RNA

The communications processors of the category SIMATIC S-400 have a rugged plastic housing with IP20 degree of protection for installation on an S7-400 rack. The connection to S7-400 components is made via a backplane bus.

Features

Functionality	CP 443-1 SIPLUS CP 443-1	CP 443-1 Advanced SIPLUS CP 443-1 Advanced	CP 443-1 RNA
Connections Industrial Ethernet/PROFINET	1 x RJ-45 1 x D sub socket 15-pin	4 x RJ-45	3 x RJ-45
Integrated switch	-	•	-
Gigabit interface	-	•	-
30 MB flash memory 28 MB RAM	-	•	-
C-PLUG not included with the product	-	•	-

- Suitable / available or according to the specified standard.

Functions

The communications processors of this category support the following protocols and technologies:

Functionality		CP 443-1 SIPLUS CP 443-1	CP 443-1 Advanced SIPLUS CP 443-1 Advanced	CP443-1 RNA	
				Ethernet interface	RNA interface
PROFINET	IO controller	•	•	-	-
	IO device	-	-	-	-
	CBA	-	•	-	-
IT ¹⁾		•	•	-	-
IP-R ²⁾		-	•	-	-
MRP		•	•	-	-
PRP		-	-	-	•
FTP		-	•	-	-
S7 communication	PG function operator control and monitoring	•	•	• (only ISO)	•
	Data exchange	•	•	• (only ISO)	•
SEND/RECEIVE	ISO transport connection	•	•	•	•
	TCP, ISO-on-TCP, UDP	•	•	-	•
	multicast with UDP	•	•	-	•
	FETCH/WRITE	•	•	• (only ISO)	•
Open TCP/IP communication		•	•	-	•

- Suitable / available or according to the specified standard.

1) IT stands for Web server, e-mail, FTP

2) IP-R stands for routing between the interfaces

CP 443-1 SIPLUS CP 443-1

The CP 443-1 and the SIPLUS CP 443-1 are designed to connect a SIMATIC S7-400 system to Industrial Ethernet networks.

The communications processors support:

- PG/OP communication
- S7 communication
- Open communication (SEND/ RECEIVE)
- PROFINET communication
- IT communication

The communications processors are also suitable for redundant S7 communication in SIMATIC H systems and for applications for the functional safety of the communications technology, for example PROFIsafe in conjunction with an S7-400 F-CPU.

The additional characteristics and functions are as follows:

- A PROFINET interface with two RJ-45 connectors. Connection is via an IE FC RJ-45 plug 180 with 180° cable outlet or via a standard patch cable.
- Diagnostics LEDs for displaying the operational and communication status.
- 10 /100 Mbps, full / half duplex with the functionality for autosensing and autocrossover via an integrated 2-port switch.
- Simple installation, the CP 443-1 is installed in the rack of the SIMATIC S7-400 and connected to the other modules via the backplane bus. There are no slot rules.
- In conjunction with the interface module IM 460/461, the CP 443-1 can also be operated in an expansion rack (ER).
- Fanless operation of the communications processor.
- The communications services operate over the following interfaces:
 - Open communication (TCP/IP and UDP), multicast for UDP incl. routing between the two interfaces.
 - Inter-network PG/OP communication with S7 routing.
 - S7 communication (client, server, multiplexing) incl. routing between the two interfaces.
 - S7-H communication for SIMATIC S7-400 H systems
 - PROFINET IO controller with real-time properties due to RT and IRT
 - The IP address is assigned using DHCP, a simple PC tool or a program block, for example for HMI.
- Media redundancy (MRP):
 - Within an Ethernet network with a ring topology, the communications processor supports the media redundancy protocol MRP
- Diagnostics and network management:
 - Extensive diagnostics functions of all modules of the rack
 - Integration in network management systems by supporting SNMP V1/V3
- A wide range of diagnostics options with LEDs, in STEP 7 and Web-based diagnostics units incl. monitoring by IT network management tools (SNMP V1 MIB II)
- Security mechanisms:
 - Access protection with a configurable IP-ACL (IP Access Control List)
- Configuration of all functions with STEP 7 as of V5.4
- Configuration with STEP 7 Professional V11 or higher.
- Module replacement without PG by storing all data on the CPU.
- SIPLUS CP 443-1
- The SIPLUS CP 443-1 module is intended for environmental loads at ambient temperatures of 0°C to +60°C.

CP 443-1 Advanced / SIPLUS CP 443-1 Advanced

The CP 443-1 Advanced and the SIPLUS CP 443-1 Advanced are designed for connection of a SIMATIC S7-400 system to Industrial Ethernet networks also as a PROFINET IO controller or in SIMATIC H systems.

The additional characteristics and functions are as follows:

- PROFINET communication
 - In addition to PROFINET IO communication, PROFINET CBA (Component-Based Automation) is also available here.
 - This makes communication between technological modules (distributed intelligence) possible.
 - Users can choose between cyclic and acyclic communication.
This form of communication is suitable both for non time-critical as well as time-critical applications.
- Configurable keepalive function
- Two separate interfaces (integrated network separation):
 - Gigabit interface with an RJ-45 connector for 10 / 100 / 1000 Mbps full / half duplex with the autosensing functionality.
 - PROFINET interface with four RJ-45 connectors for 10 / 100 Mbps full / half duplex incl. autosensing and autocrossover functionality via an integrated 4-port switch.
- 30 MB of flash memory with a file system for user-defined HTML pages and 30 MB of RAM for buffering dynamic data.
- File exchange with other computers using FTP.
- Integrated HTTP server that allows write and read access to process and status data of the S7-400 system. This means, for example, that system diagnostics is possible via a secure Web browser.
- Integrated ESMTP client for reliable event-driven sending of e-mails that can also include variables. The current value of such a variable is queried when the program of the S7-400 CPU triggers the sending of the corresponding e-mail.
- A C-PLUG for storing the configuration data ships with the product.
- CP 443-1 Advanced with security function: Security of the system against unauthorized access by
 - Central access protection for any devices within an automation cell, for example by secure authentication of the network nodes.
 - Secure remote access via Internet thanks to data encryption (VPN)
 - Data integrity check
 - Traceability with data logging based on standard IT mechanisms (Syslog)
- SIPLUS CP 443-1 Advanced

The SIPLUS CP 443-1 module is intended for environmental loads at ambient temperatures of 0°C to +60°C.

CP 443-1 RNA

The CP 443-1 RNA is designed to connect a SIMATIC S7-400 system to Industrial Ethernet networks. The special feature of this device is support of the redundancy protocol PRP (Parallel Redundancy Protocol). This allows the connection of devices to redundant Ethernet networks. In addition to this fault-tolerant systems (known as H systems) are supported. The device has the following characteristics and functions:

- **Time-of-day synchronization over the RNA interface using the following configurable methods:**

- SIMATIC mode

The CP receives MMS timeofday messages and synchronizes its local time.

You can choose whether or not the time of day is forwarded. You can also decide on the direction in which it is forwarded.

or

- NTP mode (NTP: Network Time Protocol)

The CP sends timeofday queries at regular intervals to an NTP server and synchronizes its local time of day.

The time can also be forwarded automatically to the CPU modules in the S7 station allowing the time to be synchronized in the entire S7 station.

- **Addressable with the factoryset MAC address**

To assign the IP address to a new CP (direct from the factory), it can be accessed using the preset MAC address on port X2P1 of the RNA interface. The online address assignment is made in STEP 7.

- **SNMP agent on the RNA interface**

The CP supports data queries via SNMP in version V1 (Simple Network Management Protocol). It delivers the content of certain MIB objects according to the MIB II standard (RFC 1213), PRP-MIB IEC62439 (IEC-62439-3-MIB) and Automation MIB.

- **Module access protection**

To protect the module from accidental or unauthorized access, protection can be configured at various levels.

- **IP access protection on the RNA interface (IP-ACL)**

Using IP access protection gives you the opportunity of restricting communication over the CP of the local S7 station to partners with specific IP addresses.

- **Web diagnostics on the RNA interface**

With the aid of Web diagnostics, you can read out the diagnostics data from a station connected via the CP to a PG/PC with a Web browser.

The Web pages contain the following information:

- Module and status information

- **Diagnostics buffer extract request**

With the aid of a Web browser, the CP supports the option of obtaining an extract of the diagnostics buffer containing the most recent diagnostics events of the CPUs and CPs located in the same S7 station as the CP.

- **Connection diagnostics with the AG_CNTEX program block**

With the AG_CNTEX program block, you can diagnose connections.

- When necessary, you can activate or deactivate connections or initiate reestablishment of a connection.
- You can check the reachability of the connection partners using the PING function (on the RNA interface).
- You can find out which connection types are set up on the RNA interface for the SEND / RECEIVE function.

- **S5/S7 addressing mode**

The addressing mode can be configured for FETCH/WRITE access as the S7 or S5 addressing mode (S7 addressing mode only for data blocks / DBs).

- **Detecting IP double addressing in the network on the RNA interface**

To save you timeconsuming troubleshooting in the network, the CP detects double addressing in the network.

- **Support in the fault-tolerant system (H system)**

S7 communication is supported in the H system with the following protocols:

- Ethernet interface
ISO transport
- RNA interface
ISO transport and ISO-on-TCP (RFC1006)

Article numbers

CP 443-1	For connecting SIMATIC S7-400 to Industrial Ethernet using TCP/IP, ISO and UDP; PROFINET IO controller, MRP, integrated real-time switch ERTEC with two ports and two RJ-45 interfaces. S7 communication, open communication (SEND/RECEIVE) incl. FETCH/WRITE, with or without RFC 1006, DHCP, SNMP V2, diagnostics, multicast, access protection with IP access control list, initialization via LAN 10/100 Mbps; incl. electronic manual on DVD.	6GK7443-1EX30-0XE0
SIPLUS CP 443-1	For connecting SIMATIC S7-400 to Industrial Ethernet using TCP/IP, ISO and UDP; PROFINET IO controller, MRP, integrated real-time switch ERTEC with two ports and two RJ-45 interfaces. S7 communication, open communication (SEND/RECEIVE) incl. FETCH/WRITE, with or without RFC 1006, DHCP, SNMP V2, diagnostics, multicast, access protection with IP access control list, initialization via LAN 10/100 Mbps; incl. electronic manual on DVD. Ambient temperature from 0 °C to +60 °C (For harsh environmental load.)	6AG1443-1EX30-4XE0

CP 443-1 Advanced	For connecting the SIMATIC S7-400 CPU to Industrial Ethernet: 1 x 10 / 100 / 1000 Mbps, 4 x 10 / 100 Mbps (IE switch). RJ-45 ports, ISO, TCP, UDP, PROFINET IO controller, S7 communication; open communication (SEND/RECEIVE). S7 routing, IP configuration using DHCP/block. Access protection with IP access control list; time-of-day synchronization, advanced Web diagnostics; fast startup, PROFINET energy support; IP routing; FTP, Web server, e-mail, PROFINET CBA. With security function: Firewall and VPN.	6GK7443-1GX30-0XE0
SIPLUS CP 443-1 Advanced	For connecting the SIMATIC S7-400 CPU to Industrial Ethernet: 4 x 10 / 100 / 1000 Mbps, 4 x 10 / 100 Mbps (IE switch). RJ-45 ports, ISO, TCP, UDP, PROFINET IO controller, S7 communication; open communication (SEND/RECEIVE). S7 routing, IP configuration using DHCP/block. Access protection with IP access control list; time-of-day synchronization, advanced Web diagnostics; fast startup, PROFINET energy support; IP routing; FTP, Web server, e-mail, PROFINET CBA Ambient temperature from 0 °C to +60 °C (For harsh environmental load.)	6AG1443-1GX30-4XE0
CP 443-1 RNA	For connection of SIMATIC S7-400 to Industrial Ethernet via TCP/IP, ISO and UDP, S7 communication, open communication (SEND/RECEIVE) incl. FETCH/WRITE, support of the redundancy protocol PRP and fault-tolerant systems, SNMP V1, diagnostics, multicast, access protection with IP access control list for the RNA interface, initialization via LAN 10/100 Mbps; incl. electronic manual on DVD.	6GK7443-1RX00-0XE0

6.5 Communications processors for SIMATIC S7-1200

Description



Figure 6-7 SIMATIC S7-1200: CP 1242-7 (GPRS) and communication with S7-1200

The communications modules for the SIMATIC S7-1200 connect S7-1200 controllers with higher-level systems or a control room. The modules have either an Ethernet interface or a mobile wireless interface (GSM or LTE). With the CP 1243-8 IRC as second interface can be configured via a TS module. The Ethernet interface is intended for connection to router, This allows remote terminal units to be implemented, that transfer measured values and alarms to the control room either cyclically or event-driven. As an alternative this interface can also be used to connect the device to a network. The devices have a rugged plastic housing for installation on a DIN rail or for wall mounting.

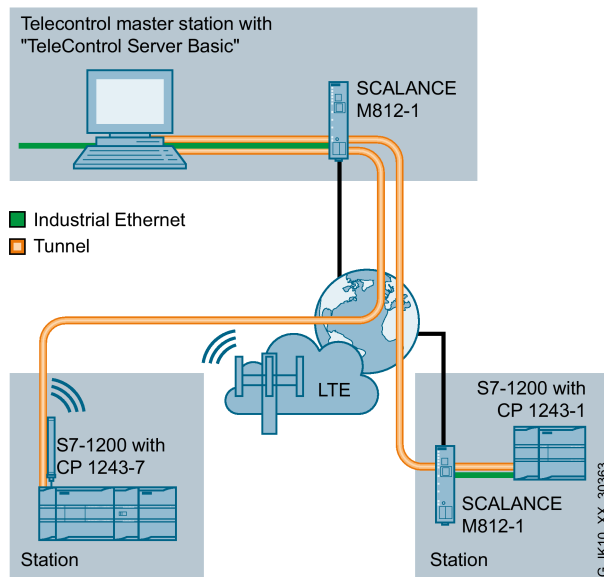


Figure 6-8 Example of the configuration for connecting two stations with a CP 1243-7 and a CP 1243-1

The following product variants exist:

Modules with Ethernet interface

- **CP 1243-1**
for connecting SIMATIC S7-1200 to Telecontrol Server Basic.
- **CP 1243-1 DNP3**
with support of the transfer protocol DNP3.
- **CP 1243-1 IEC**
with support of the communications standard IEC 60870-5.
- **CP 1243-8 IRC**
for the connection to control room capable of ST7. Optionally expandable with a TS module.

Modules with mobile wireless interface

- **CP 1242-7 V2**
for connecting SIMATIC S7-1200 to Telecontrol Server Basic via a GSM/GPRS network.
- **CP 1243-7 LTE EU**
for connecting SIMATIC S7-1200 to Telecontrol Server Basic via an LTE network with the frequencies used in Europe.

Features

The devices have the features listed in the table:

	CP 1243-1	CP 1243-1 DNP3	CP 1243-1 IEC	CP 1243-8 IRC	CP 1242-7 V2 CP 1243-7 LTE
RJ-45 interface	•	•	•	•	-
Interface / TS module	-	-	-	•	-
SMA socket	-	-	-	-	•
External power supply	-	-	-	•	•

- Suitable / available or according to the specified standard.

Functions

The following table indicates the functions provided by the individual devices:

	CP 1243-1	CP 1243-1 DNP3	CP 1243-1 IEC	CP 1243-8 IRC	CP 1242-7 V2 CP 1243-7 LTE
Time-of-day synchronization with NTP	•	-	-	•	•
Configuration with STEP 7 Basic	•	•	•	•	•
Control center connection					
Telecontrol Server Basic	•	-	-	-	•
Siemens Industrial Services Operating Center	-	-	-	-	-
Control room capable of DNP3	-	•	-	-	-
Control room capable of IEC 60870-5	-	-	•	-	-
Control room capable of ST7	-	-	-	•	-

Article numbers

CP 1243-1	For connecting SIMATIC S7-1200 to Telecontrol Server Basic.	6GK7243-1BX30-0XE0
CP 1243-1 DNP3	With support of the transfer protocol DNP3.	6GK7243-1JX30-0XE0
CP 1243-1 IEC	With support of the communications standard IEC 60870-5.	6GK7243-1PX30-0XE0
CP 1243-8 IRC	For the connection to control room capable of ST7. Optionally expandable with a TS module.	6GK7243-8RX30-0XE0
CP 1242-7 V2	For connecting SIMATIC S7-1200 to Telecontrol Server Basic via a GSM/GPRS network.	6GK7242-7KX31-0XE0 ¹⁾
CP 1243-7 LTE EU	For connecting SIMATIC S7-1200 to Telecontrol Server Basic via an LTE network with the frequencies used in Europe.	6GK7243-7KX30-0XE0 ¹⁾

¹⁾ Note the national approvals in: <http://www.siemens.en/funkzulassungen>

6.6 Communications processors for SIMATIC S7-1500

Description



Figure 6-9 CP 1543-1

The communications modules for the SIMATIC S7-1500 connect the S7-1500 controllers to Industrial Ethernet or PROFINET. The following modules exist:

CP 1543-1

This communications processor connects an S7-1500 controller to an Ethernet network. It has proven security mechanisms (including firewall with stateful packet inspection, VPN with IPsec, IP/MAC access control list, FTPS) to protect individual devices or entire automation cells from unauthorized access. Data transmission rate up to 1000 Mbps and common IT functions such as FTP, HTTP and e-mail are supported. For configuration, the TIA Portal as of version 12 is used. The graphic shows an example of an application:

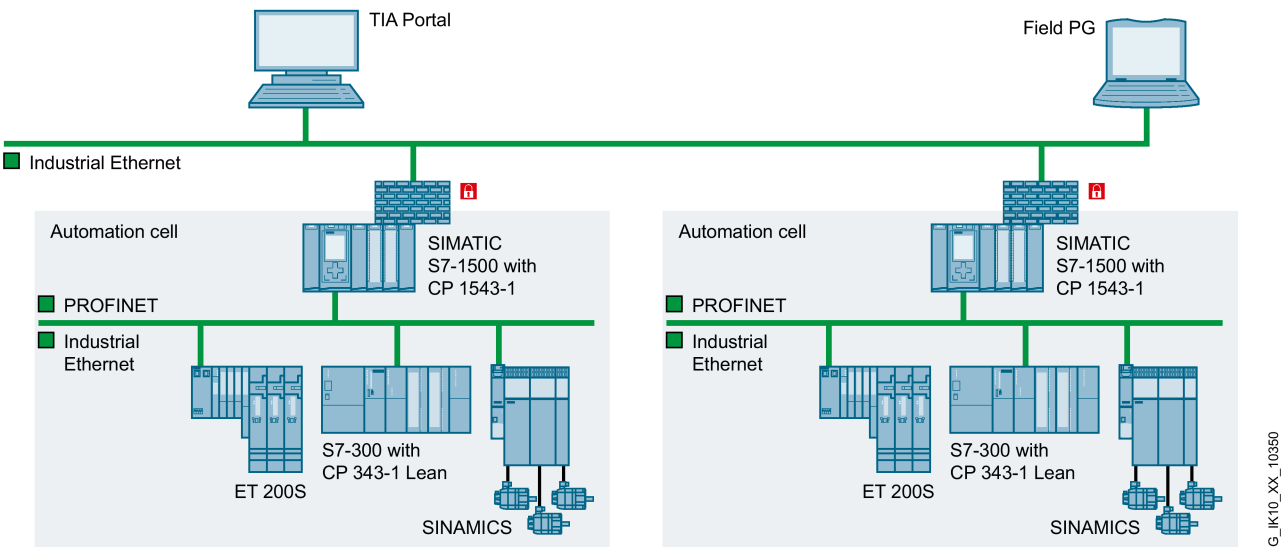


Figure 6-10 Protection and segmentation by firewall with the CP 1543-1

CM 1542-1

This communications module expands an S7-1500 controller with a PROFIBUS connector implemented as a 2-port switch with 10/100 Mbps. With the CM 1542-1 as a PROFINET controller for up to 128 PNIO devices, a separate PROFINET segment can be set up. As IT functions HTTP and e-mail are available. The redundancy protocol MRP is also supported (MRP manager and MRP client). The configuration is created with STEP 7 Professional V13 or higher. The graphic shows an example of the network separation with a an CM1542-1:

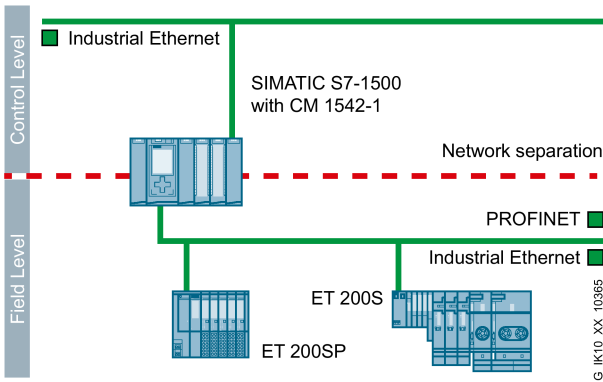


Figure 6-11 PROFINET segment with a CM1542-1

Features

The devices have the features listed in the table:

	CP 1543-1	CM 1542-1
Power supply	15 VDC via backplane bus	
Interface	1 x RJ-45	2 x RJ45 (switched)
Transmission rate	10 / 100 / 1000 Mbps	10/100 Mbps

- Suitable / available or according to the specified standard.

Functions

The following table indicates the functions provided by the individual devices:

	CP 1543-1	CM 1542-1
IPv6	•	-
TCP/IP	•	•
PROFINET IO	-	•
Redundancy manager	-	•
Firewall	•	-
VPN with IPsec	•	-
SNMPv1	•	•
SNMPv3	•	-
DCP	•	•
LLDP	-	•
NTP	•	•

Article numbers

CM 1542-1	Communications module for connection of S7-1500 to PROFINET as IO controller with 2 x RJ-45 ports on the Ethernet interface.	6GK7542-1AX00-0XE0
CP 1543-1	Communications module for connection of S7-1500 to Industrial Ethernet with one RJ-45 port on the Ethernet interface. IT functions (FTP, HTTP, e-mail) and security functions (firewall, VPN with IPsec).	6GK7543-1AX00-0XE0

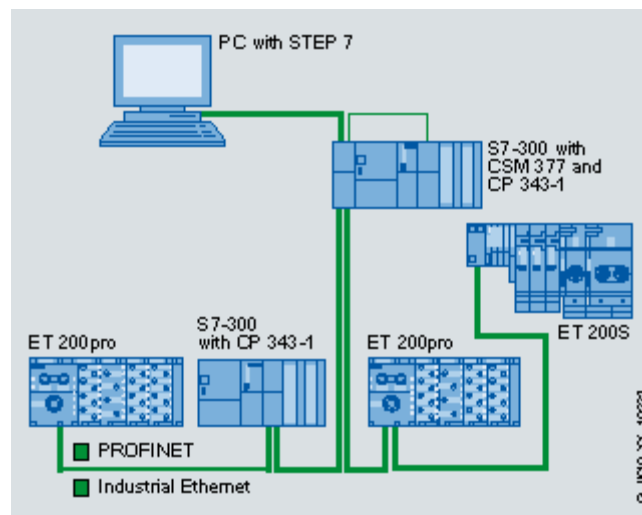
Compact switch module

Description

The Compact Switch Modules are industrial Ethernet switches with a compact, modular design for use in the immediate vicinity of the SIMATIC S7 CPUs. Using a CSM, the Ethernet interface of a SIMATIC S7 CPU can be multiplied. This means that simultaneous communication with operator control and programming devices, other controllers or office networks is possible.

With a CSM and the SIMATIC S7 controller, simple, low-cost automation networks can be implemented.

Example of a topology



Device variants

Currently, there are four device types of the Compact Switch Module available. These differ in terms of their construction and the installation options:

- The CSM 377 unmanaged meets the requirements of rugged SIMATIC S7-300 technology and is installed on an S7-300 standard rail. The module is designed according to the standards EN 61000-6-2:2001 and EN 61000-6-4:2001.
- The CSM 1277 unmanaged meets the technical and industrial requirements of the new SIMATIC generation S7-1200. The CSM 1277 is installed on an S7-1200 standard rail. The module conforms with the standards EN 61000-6-2 and EN 61000-6-4.
- The SIPLUS NET CSM 1277 is an unmanaged switch for unusual environmental conditions. The module complies with the standards EN 60721-3-3, class 3B2,

EN 60721-3-3, class 3C4 incl. salt mist and ISA –S71.04, the immunity test levels G1, G2, G3 and GX.

- LOGO! With four RJ-45 ports, CSM is intended for external access or connection to Industrial Ethernet networks. With the LOGO! With a CSM, an Ethernet interface of the SIMATIC LOGO! can be multiplied. This means that simultaneous communication with operator control and programming devices, other controllers or office environments is possible.

It is installed on a standard rail.

Two product variants are available:

- LOGO! CSM 12/24 for operation with direct current at a voltage of 12 and 24 V.
- LOGO! CSM 230 for operation with AC voltage of 110 and 230 V.

7.1 CSM 377

Description



Figure 7-1 CSM 377 unmanaged

Unmanaged switch for connecting a SIMATIC S7-300 with integrated PROFINET interface or with an Industrial Ethernet CP or ET 200M to an Industrial Ethernet network in an electrical linear bus, tree or star structure.

As an unmanaged switch, the CSM 377 is intended for integration of small machines into existing automation networks or for standalone operation of the machines.

- Rugged plastic housing with degree of protection IP20.
- Easy to mount; the switch module CSM 377 is mounted on the S7-300 rail. It has no connection to the backplane bus of the S7-300 or ET 200M and must therefore be plugged in at the start (first module to the left of the CPU) or at the end (last module far right) of the S7-300 station. The connection to the CPU of the S7-300 is either via an Industrial Ethernet cable or an Industrial Ethernet twisted pair cord.
- Rugged node connectors are designed for industry with four PROFINET-compliant RJ-45 connectors for twisted pair cables that provide additional strain and bending relief with a locking mechanism on the casing.
- Cost-effective solution for the implementation of small, local Ethernet networks.

Features

Functionality	CSM 377
External power supply 24 VDC	•
Connection to Industrial Ethernet/PROFINET	4 x RJ-45
Gigabit interface	-

- Suitable / available or according to the specified standard.

Functions

The unmanaged CSM 377 distinguishes itself with the following functions of SIMATIC S7-300 technology:

- Display LEDs for diagnostics and for the status display of the Industrial Ethernet ports.
- 10/ 100 BaseTX
- Automatic detection of the data rate with autosensing and autocrossover function for connecting IE FC cables via IE FC RJ-45 plug up to 100 m.
- Three further Industrial Ethernet interfaces (TP ports) are available for connecting additional Ethernet nodes such as HMI panels or ET 200.
- The CSM 377 is operated without a fan, a backup battery is unnecessary.
- The module can be replaced without a PG.

Article numbers

CSM 377	Unmanaged switch for connecting a SIMATIC S7-300, ET 200M and up to three further nodes to Industrial Ethernet. 10/ 100 Mbps, 4 x RJ-45 ports, external power supply 24 VDC, LED diagnostics, S7-300 module incl. electronic device manual on CD-ROM.	6GK7377-1AA00-0AA0
----------------	--	---------------------------

7.2 CSM 1277

Description



Figure 7-2 CSM 1277 unmanaged

The compact switch module CSM 1277 is an unmanaged switch for connecting a SIMATIC S7-1200 module to an Industrial Ethernet network with a linear bus, tree or star structure.

With the CSM 1277 the Ethernet interfaces on a SIMATIC S7-1200 module can be multiplied for the additional connection of up to three programming devices, operator input elements and further Ethernet nodes. This makes simultaneous communication with operator input and programming devices, further controllers or the office networks possible.

With the CSM 1277 and the controller of SIMATIC S7-1200 systems simple automation networks can be implemented at low cost.

- Rugged plastic housing with degree of protection IP20
- Simple, space-saving mounting on the SIMATIC S7-1200 standard rail.
- Cost-effective solution for the implementation of small, local Ethernet networks.
- Problem-free connection via RJ-45 standard plug-in connections.
- Simple and fast status display with LEDs on the device.
- The use of straight-through connecting cables is possible thanks to integrated autocrossover function.

Features

Functionality	CSM 1277
External power supply 24 VDC	•
Connection to Industrial Ethernet/PROFINET	4 x RJ-45
Gigabit interface	-

- Suitable / available or according to the specified standard.

Functions

The following section lists the functions of the two product variants CSM 1277 unmanaged and SIPLUS NET CSM 1277.

CSM 1277 unmanaged

- Display for diagnostics and for the status display of the Industrial Ethernet ports via LEDs.
- Automatic data rate detection with autosensing and autocrossover function.
- Replication of the Ethernet interfaces of the SIMATIC S7-1200 systems.
- The module can be replaced without a PG.
- Operation without a fan and low maintenance design

Various network topologies can be implemented with the compact switch module CSM 1277.

- Setup of a small local Industrial Ethernet network with three further nodes.
- Connection of the SIMATIC S7-1200 in a linear bus structure:

At least one RJ-45 connector of the SIMATIC S7-1200 remains free, e.g. for connecting a programming device (PG).

- Connection of the SIMATIC S7-1200 to a higher-level network with a tree or star structure:

At least two RJ-45 connectors of the SIMATIC S7-1200 remain free, e.g. for connecting a PG/OP.

SIPLUS NET CSM 1277

The technical concept of the compact switch module SIPLUS NET CSM corresponds to the functions and characteristics of the CSM 1277 unmanaged. The SIPLUS NET 1277 module is intended for unusual environmental loads at ambient temperatures of 0°C to +55°C.

Note

SIPLUS

The SIPLUS extreme products are based on the Siemens Industry standard products.

You will find more detailed information and the technical documentation on SIPLUS in the portal of Siemens AG: <http://www.siemens.en/siplus-extreme>

Article numbers

CSM 1277	Unmanaged switch for connecting a SIMATIC S7-1200M and up to three further nodes to Industrial Ethernet with 10/ 100 Mbps, 4 x RJ-45 ports. External power supply 24 VDC, LED diagnostics, S7-1200 module. Incl. an electronic device manual on CD-ROM.	6GK7277-1AA10-0AA0
SIPLUS NET CSM 1277	For an extended temperature range and unusually harsh environmental loads. Unmanaged switch for connecting a SIPLUS S7-1200 and up to three further nodes to Industrial Ethernet with 10/ 100 Mbps, 4 x RJ-45 ports. External power supply 24 VDC, LED diagnostics, S7-1200 module. Incl. an electronic manual on CD-ROM. Ambient temperature from 0 °C to +55 °C (Abnormal environmental load.)	6AG1277-1AA00-4AA0

7.3 LOGO! CSM

Description



Figure 7-3 LOGO! CSM 12/24

With the Compact Switch Modules **LOGO! CSM 230** and **LOGO! CSM 12/24**, the logic system modules of the LOGO! product series can be expanded with additional Ethernet interfaces. This allows Ethernet networks to be expanded flexibly in electrical linear bus, tree or star structures.

The design of the logic modules has been adapted to the LOGO! series to allow simple and space-saving installation. The "unmanaged switches" can either connect two logic modules together or provide connectors for additional components such as operator control and monitoring devices, displays or programming devices (PGs).

- Industrial design of the new LOGO! generation
- Space-saving, optimized for connection to LOGO! system modules
- Cost-effective solution for the implementation of small, local Ethernet networks

Features

Functionality	CSM 12/24	CSM 230
Power supply	12/24 VDC (10.2 ... 30.2 VDC)	230 VAC
Connector - Industrial Ethernet	4 x RJ-45	
Transmission rate	10 Mbps, 100 Mbps	
Design	LOGO! module	
Degree of protection	IP20	

- Suitable / available or according to the specified standard.

Functions

The LOGO! CSM unmanaged switch modules have the following characteristics and functions.

- 4-port unmanaged switch
- Straightforward connection with 4 RJ-45 standard connectors
- 1 Ethernet port on the front of the module for direct diagnostics access in the cabinet.
- 2 product variants for the voltage ranges 12 / 24 VDC or 230 VAC/VDC
- Power supply via terminal strip connectors
- Diagnostics LEDs
- Connection of a LOGO! module and up to 3 further nodes to an Industrial Ethernet network at 10 / 100 Mbps in electrical linear bus, tree or star structures.
- Standalone use for networking different Ethernet devices

Article numbers

LOGO! CSM 230	4-port compact switch modules for LOGO!, 230 VAC	6GK7177-1FA10-0AA0
LOGO! CSM 12/24	4-port compact switch modules for LOGO!, 12/24 VDC	6GK7177-1MA20-0AA0

Description

Gateways allow the connection of Industrial Ethernet networks and other networks that differ in terms of the transmission media and handling of the data traffic. This makes data exchange possible with devices that cannot be connected directly to Industrial Ethernet.

Example of a topology

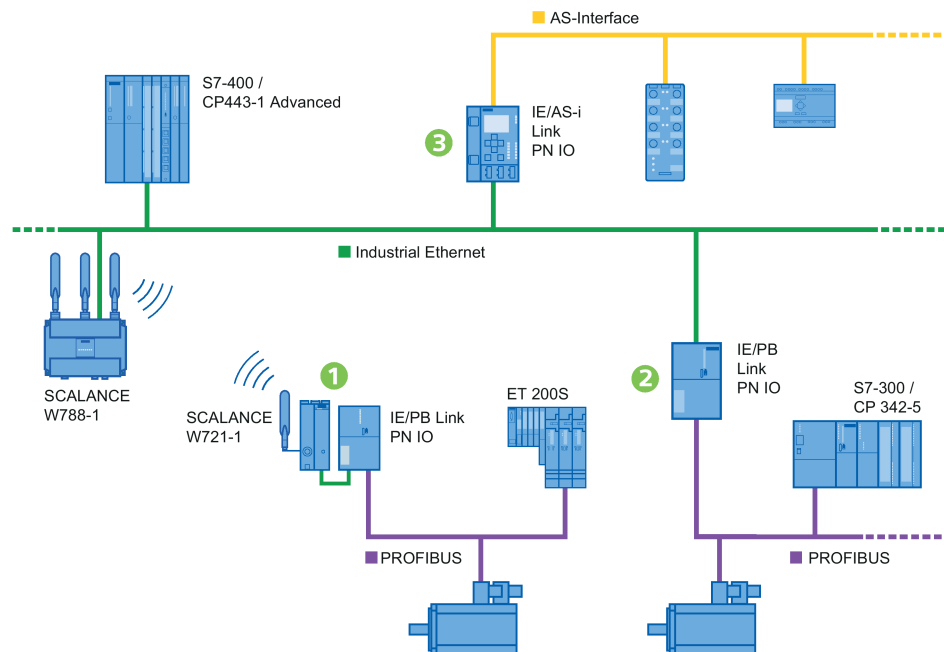


Figure 8-1 ① Connection between IWLAN and PROFIBUS via the IWLAN/PB Link in conjunction with a SCALANCE W721-1
 ② Connection between Industrial Ethernet and PROFIBUS via the IE/PB Link PN IO
 ③ Connection between Industrial Ethernet and AS-interface via the IE/AS-i Link PN IO

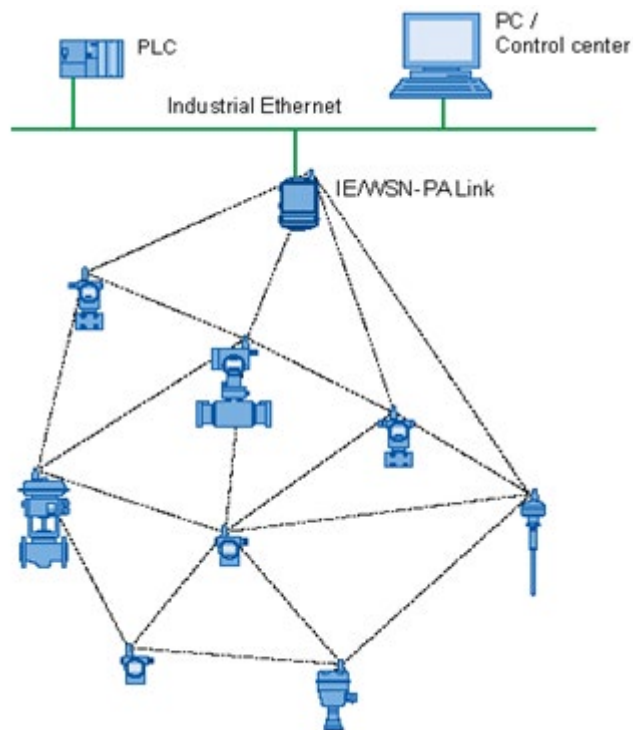


Figure 8-2 Use of the IE/ WSN-PA Link as a gateway between a WirelessHART network (WSN - Wireless Sensor Network) and a wired network.

Device variants

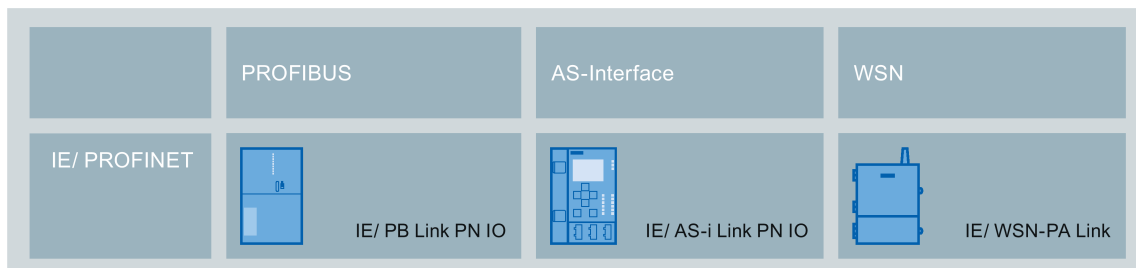


Figure 8-3 Gateways

IE/ PB Link PN IO

The IE /PB Link PN IO is a gateway between Industrial Ethernet and PROFIBUS. This device can also be used as a PROFINET IO proxy. This means that PROFIBUS DP slaves are handled like IO devices with an Ethernet interface.

IE/ AS-i Link PN IO

The IE/ AS-i Link PN IO is a gateway between a PROFINET/Industrial Ethernet (PROFINET IO device) and an AS interface.. This device allows transparent data access to the AS-interface from Industrial Ethernet.

IE/ WSN-PA Link

The IE/ WSN-PA Link is a gateway that connects WirelessHART networks with Ethernet. An IE/WSN-PA Link allows the setup of a self-organizing WirelessHART network and manages the security functions and connectivity. This link is the input point for data sent by WirelessHART sensors. This data is made available to other systems via an Ethernet interface.

On the wireless side, the IE/ WSN-PA Link supports the WirelessHART standard (HART V 7.1) and on Ethernet side communication using TCP/IP.

8.1 IE/PB Link PN IO

Structure

- Compact module S7-300 double width for mounting on an S7-300 standard rail.
- Degree of protection IP20
- Optional use of the C-PLUG memory medium (does not ship with the product) for storage of device parameters. This makes fast device replacement possible if there is a fault.

Features

Functionality	IE/PB Link PN IO
Connector - Industrial Ethernet	1 x RJ-45
Connector PROFIBUS	1 x D-sub 9-pin, female (RS-485)
Transmission rate - Industrial Ethernet	10 Mbps, 100 Mbps
Power supply	24 VDC

- Suitable / available or according to the specified standard.

Functions

- Ethernet transmission rate 10/100 Mbps full/half duplex, autosensing.
- Data transmission rate PROFIBUS 9.6 kbps to 12 Mbps incl. 45.45 kbps for PROFIBUS PA.
- By using the PROFINET IO proxy function, existing PROFIBUS devices can continue to be used in a PROFINET environment. PROFIBUS DP slaves are connected to the PROFINET IO controller with real-time properties.
- S7 routing
- SNMP diagnostics and integration in the network management systems of the PROFIBUS devices via the IE/PB Link PN IO.

Article number

IE/ PB Link PN IO	Gateway between Industrial Ethernet and PROFIBUS with PROFINET IO functionality, TCP/IP, S7 routing and data record routing. 10/ 100 Mbps Fast Ethernet, 9.6 to 12 Mbps PROFIBUS Including electronic manual on CD-ROM in the languages: German, English, French, Spanish and Italian.	6GK1411-5AB00
-------------------	--	----------------------

8.2 IE/AS-i Link PN IO

Structure

- Compact plastic housing with degree of protection IP20 for installation on a DIN rail.
- Full graphics display and control buttons on the front of the housing for commissioning the entire lower-level AS-i line and diagnostics on site.
- Optional use of the C-PLUG memory medium (does not ship with the product) for storage of device parameters. This makes fast device replacement possible if there is a fault.

Features

Functionality	IE/AS-i Link PN IO
Connector - Industrial Ethernet	2 x RJ45 (switched)
Connector - AS-i	Screw connector
Transmission rate - Industrial Ethernet	10 Mbps, 100 Mbps
Power supply	24 VDC or via AS-i

- Suitable / available or according to the specified standard.

Functions

- AS-Interface bus cycle time 5 ms with 31 slaves, 10 ms with 62 slaves.
- Use as single and double AS-interface master for the connection of 62 AS-interface slaves and integrated analog monitoring.
- Integrated Web server via which configuration with Web-based Management is also possible.
- Integrated short-circuit to ground monitoring for the AS-interface cable.
- PROFINET IO
- TCP/IP
- SNMP

Article numbers

IE/ AS-i Link PN IO	Gateway between PROFINET / Industrial Ethernet and AS-interface with degree of protection IP20. Including plug-in screw connectors COMBICON for connection of an AS-Interface cable, with the double master two AS-interface cables and an optional power supply of 24 V. According to the AS-interface specification 3.0. Dimensions (width x height x depth): 90 mm x 132 mm x 88.5 mm	6GK1411-2AB10
	• Single master with display • Double master with display	6GK1411-2AB20

8.3 IE/WSN-PA Link

Structure

- Rugged metal housing with degree of protection IP65 for wall or mast mounting indoors and outdoors
- Fixed antenna that cannot be removed and connection option for an external antenna.
- Materials for securing to a mast ship with the product. This
- Operation of WirelessHART In the 2.4 GHz frequency band.

Features

Functionality	
Connector - Industrial Ethernet	2 x RJ-45
Connector - Modbus RTU (RS-485)	2-pin terminal block
Connector - external antenna	1 x N-Connect female
Transmission rate - Industrial Ethernet	10 Mbps, 100 Mbps
Power supply	24 VDC

- Suitable / available or according to the specified standard.

Functions

- Support of the wireless standard IEEE 802.15.4 and the Wireless HART standard HART V7.1
- Up to 100 WirelessHART devices can be operated in the WirelessHART network with a maximum latency time of the network of 10 seconds (with the maximum configuration).
- Ethernet transmission rate 10/100 Mbps, autosensing
- System integration can be achieved with: TCP/IP via an HTTPS browser, OPC server, Modbus TCP/IP over Ethernet or via the Modbus RTU via a serial connection.
- THE IE/WSN-PA Link sets up a meshed wireless sensor network on the wireless side via which the wireless measuring transducers communicate with the IE/WSN-PA Link. The data of the wireless field devices is buffered on the IE/WSN-PA Link and transferred to the connected systems via Ethernet.
- The configuration of the IE/WSN-PA Link is via Web user interfaces generated by the IE/WSN-PA Link. Device statuses and measured values can also be displayed using this Web user interface.

Article numbers

IE/ WSN-PA Link	Gateway between WirelessHART and Industrial Ethernet Transmission frequency 2.4 GHz	6GK1411-6CA40-0AA0
	• With integrated antenna • N-connector for connecting external antennas	6GK1411-6CA40-0BA0

Appendix

A.1 Overview of the standards relevant for network installation

Introduction

This section provides with a basic overview of the standards generally relevant for installation of networks in buildings and those particularly relevant for Industrial Ethernet.

Note

This section can only include basic information available at the time of going to print.

For more detailed and up-to-date guidelines, contact the PROFIBUS user organization e.V.

The PROFIBUS user organization

PROFIBUS User Organization e.V.

Haid-und-Neu-Straße 7,

D-76131 Karlsruhe, Germany

Tel. +49 (0) 7 21 · 96 58 590, Fax +49 (0) 7 21 · 96 58 589

germany@profibus.com, www.profibus.com

Standards for general-purpose cable communications networks in an office environment

Standard	Area of application
ISO/IEC 11801	International standard for network planning in office buildings
EN50173	European standard for network planning in office buildings; adopted as national standard

Due to the use of Ethernet in automation engineering, the existing standards needed to be expanded to include the industrial sector.

Standards for general purpose cable communications networks in an industrial environment

Standard	Area of application
ISO/IEC 24702	International standard for planning general-purpose networks in industrial buildings
EN50173-2 EN50173-3	European standard for network planning in industrial buildings; adopted as national standard

For industrial applications, expanded standards are necessary that describe the constraints for these applications

Cabling standards for industrial networks and their scope

Standard	Area of application	Scope
IEC 61918	International standard for communications networks in industrial automation systems; relevant for various fieldbuses, common aspects of planning, installation, operation ¹⁾	Describes the network structure and general requirements in and between automation cells
IEC61784-5-x	International series of standards for special requirements in industrial networks such as PROFINET / PROFIBUS, supplementing IEC 61918	Describes specific requirements of the communication profile

¹⁾ Fieldbus-specific aspects are described in separate, ancillary standards

The "PROFINET Cabling and Interconnection Technology" guideline

Among other things, the PROFIBUS User Organization has produced the "PROFINET Cabling and Interconnection Technology" guideline that served as input for IEC 61918 and IEC 61784 and that also references these standards.

It describes the technical benchmark values for cables and connectors (both electrical and optical) for PROFINET networks. These are intended to help new manufacturers to produce PROFINET-compliant products.

The guideline can be downloaded in English from the URL:

<http://www.profibus.com/pall/meta/downloads/article/00327/>

A.2 Content of the standards

Content of the IEC 24702 and EN50173-3 standards

The standards for general purpose building networking of buildings used for industrial purposes describe:

- The structure of the building network,
- The requirements for cables (fibre-optic, electrical),
- The requirements for connectors (fibre-optic, electrical),
- Limit values for installed links.

IEC 24702 references IEC11801.

Technical aspects of installation described in IEC 14763 (EN50174).

Content of the IEC 61918 and IEC61784 standards

the standards for automation networks include a general section describing the following points:

- Design of the network (network structure, grounding, equipotential bonding),
- Planning and installation,
- Requirements of components (table connectors, cables, grounding, ...)
- Acceptance of an installation,
- Maintenance and service.

IEC 61918 contains general requirements common to all fieldbuses (PROFINET, PB, Interbus,...).

Fieldbus-specific aspects/requirements that differ from the general section described in profile-specific standards, for example in *IEC61784-5-3* for PROFIBUS, PROFIBUS PA and PROFINET; IEC61784-5-6 for Interbus.

A.3 Application of the standards

Application of the EN standards 50173/50174

Standard	Project phase	Tasks
EN50173-1	Planning of cabling	Topology, cables, connection technology, limit values for transmission links
EN50174-1 EN50174-2 EN50174-3	Planning phase	Management of the cabling, safety requirements, laying of cables, equipotential bonding)
EN50174-1 EN50174-2 EN50174-3	Implementation phase	
EN50174-1	Operational phase	Quality assurance, management of the cabling, repair and maintenance

Description of the fieldbus-specific characteristics in IEC 61784

This standard references IEC 61918.

Standard	Fieldbus
IEC 61784-5-2	ControlNet, EtherNet/IP
IEC 61784-5-3	PROFIBUS, PROFINET
IEC 61784-5-6	Interbus
IEC 61784-5-10	Vnet/IP (Yokogawa)
IEC 61784-5-11	TCnet (Toshiba)

General-purpose cabling systems: EN 50173/EN 50174

Standard	Contents
EN50173-1	Part 1: General requirements
EN50173-2	Part 2: Office environment
EN50173-3	Part 3: Industrial area
EN50173-4	Part 4: Domestic environment
EN50174-5	Part 5: Computer centers

Installation of communication cabling: EN 50174

Standard	Contents
EN50174-1	Part 1 Specification and quality assurance
EN50174-2	Part 2 Installation planning and practices in buildings
EN50174-3	Part 3 Installation planning and practices outdoors

Validity of the information

Note

Please note that the data provided here is only intended to give you general information.

Our products are in constant development and the specifications and reference data may change in the course of this development. Despite all our efforts, it is possible that individual items of information in this networking manual are out of date.

You will find the continuously updated data in the compact operating instructions of the individual devices.

Index

5

- 50174
 - Standard, 288
- 5e
 - Category for twisted-pair cable, 13

6

- 6
 - Category for twisted-pair cable, 13

8

- 802.11
 - WLAN standards, 46

A

- Access point, 52, 52, 109
- Active network components
 - in PROFINET, 31
- Ad hoc
 - Wireless network, 59
- Ad hoc networks, 59
- Address of the gateway, 23
- Advanced Encryption Standard, 50
- AES, 50
- Antennas
 - Antenna gain, 176
 - Directional, 176
 - Dual antennas, 176
 - MIMO antennas, 176
 - Omnidirectional, 176
 - Product overview, 178
 - Radiation characteristics, 176
 - RCoax, 184
 - RCOAX cable, 176
- Autocrossover function, 110
- Automated guided vehicle system, 58
- Autonegotiation, 110

B

- Backbone, 61

C

- Cable length, 111
- Carousels, 45
- Cell protection concept, 84
- Client, 52, 109
- Collision detection, 51
- Collision domain, 42
- Communications processor
 - CP 1604, 227
 - CP 1612 A2, 231
 - CP 1616, 229
- Compact switch module
 - CSM 1277 unmanaged, 271
 - CSM 377, 269
 - LOGO!CSM 12/24, 274
 - LOGO!CSM 230, 274
- Component-Based Automation, 15, 16
- Connection diagnostics, 258
- CP 1604
 - Description, 227
 - Features, 227
 - Functions, 227
- CP 1612 A2
 - Description, 231
 - Features, 231
 - Functions, 231
- CP 1613 A2
 - Features, 233
 - Functions, 233
- CP 1616
 - Description, 229
 - Features, 229
 - Functions, 229
- CP 1623
 - Features, 235
 - Functions, 235
- Cranes, 45
- CSM 1277 unmanaged
 - Features, 272
 - Functions, 272
- CSM 377
 - Description, 269
 - Features, 270
 - Functions, 270
- CSMA/CA, 51
- CSMA/CD, 51

Cut through, 39

D

DCP protocol, 221
Denial of Service, 83
Diagnostics buffer extract, 257
DLC protocol, 221
DoS, 83
DSSS, 46
Dynamic routing, 40
 VRRP, 40

E

EAP, 50
E-mail, 82
EN 50173
 Standard, 285, 288
ERTEC-ASIC, 39
EtherNet/IP, 41
Extensible Authentication Protocol, 50

F

Fast Ethernet, 13
Fault mask, 110
Fault-tolerant system, 258
Firewall, 82
Formation of loops, 110
FTP, 82
Functions
 SCALANCE X200/X200 IRT, 131
 SCALANCE X300, 137

G

Gigabit Ethernet, 13
Glossary, 4
GPRS router, 109
GSM, 109
GSM/GPRS modem
 Modem MD720, 199

H

H system, 258, 258
High-Availability, 37
High-bay storage rack, 45

I

IEC 61784
 Standard, 288
IEC 61918
 Standard, 286
IEC 62439-3, 75
IEEE 802.11n
 Channel bonding, 49
 Frame aggregation, 49
 Guard interval, 49
 Maximum ratio combining, 47
 MIMO, 47
 Spatial multiplexing, 48
Industrial Ethernet, 11
Infrastructure mode, 53
 Wireless networks, 53
IP access protection (IP-ACL), 257
IP address, 22
iPCF, 12
iPCF-MC, 12
IPv6
 Notation, 24
IRT, 117
ISO/IEC 11801
 Standard, 285
ISO/IEC 24702
 Standard, 285
Isochronous Real Time, 20, 117
IWLAN, 44
IWLAN/PB Link PN IO, 52

K

KEY-PLUG, 223

L

Layer 3 function
 Dynamic routing, 39
 Static routing, 39
LD, 116
Line
 Network topology, 61
LOGO! CSM 12/24
 Description, 274
 Features, 275
 Functions, 275
LOGO! CSM 230
 Description, 274
 Features, 275
 Functions, 275

M

- MAC address, 257
- Management functions, 116
- MDI/MDIX autocrossover function, 110
- Media modules
 - SCALANCE X300, 141
 - SCALANCE X500, 153
- MIMO, 46
- Mobile wireless, 109
- Modem MD720
 - Description, 199
- Module access protection, 257
- Monorail suspension track, 45

N

- NAPT, 83
- NAT, 83
- Network Address Port Translation, 83
- Network Address Translation, 83
- Network topology, 61
 - Line, 61
 - Star, 62
- NTP mode (NTP: Network Time Protocol),

O

- OFDM, 46
- Operating systems, 220

P

- Packet filter, 82
- Parallel Redundancy Protocol, 75
- Passive network components
 - in PROFINET, 31
- Personal firewall, 83
- PING function, 258
- Plug and play, 110
- Point-to-point, 77
- Port, 82
- Power over Ethernet
 - IEEE 802.3af, 35
 - IEEE 802.3at, 35
- PROFIBUS International, 16
- PROFIBUS User Organization, 285
- PROFINET, 11
 - Cable assembly, 33
 - Fault-tolerant systems, 37
 - Implementation, 15

- Isochronous Real Time, 20
 - Redundancy, 38
 - Standard, 16
 - Switching mechanisms, 38
- PROFINET Cabling and Interconnection Technology
 - Guideline, 286
- PROFINET CBA, 15, 16
- PROFINET IO, 15, 16
- PRP, 75
- Pseudo random numbers, 50

R

- RADIUS
 - Network authentication protocol, 50
- Range of values for IP address, 22
- Rapid roaming, 12
- RCoax cable, 52
- Redundancy manager, 43, 66
- Redundancy methods
 - HRP, 74
 - MRPD, 73
 - MSTP, 78
 - RSTP, 77
 - STP, 77
- Redundant Network Access, 75
- Redundant ring, 43
- Redundant systems, 37
- Repeater, 42
- Ring
 - Network topology, 65
- RNA, 75
- Roaming, 52
- RTS/CTS, 51

S

- S5/S7 addressing mode, 258
- SCALANCE M, 185
 - M875, 194
- SCALANCE M812-1
 - Description, 188
 - Features and functions, 189
- SCALANCE M816-1
 - Description, 188
 - Features and functions, 189
- SCALANCE M826-1
 - Description, 188
- SCALANCE M826-2
 - Features and functions, 189

- SCALANCE M874-x
 - Description, 191
 - Features and functions, 192
- SCALANCE M875
 - Description, 194
 - Features, 195
 - Functions, 195
- SCALANCE M876-x
 - Description, 191
 - Features and functions, 192
- SCALANCE S, 206
 - Configuration and administration, 207
 - How it works, 207
- SCALANCE S602
 - Description, 210
 - Features, 213
 - Functions, 213
 - Interface, 214
- SCALANCE S612
 - Description, 211
 - Features, 213
 - Functions, 213
 - Interface, 214
- SCALANCE S623
 - Description, 212
 - Features, 213
 - Functions, 213
 - Interface, 214
- SCALANCE W
 - Access points, 156
 - Antennas, 176
 - Client modules, 156
 - IWLAN controller WLC711, 172
 - Overview of antennas, 178
 - Performance classes, 157
 - W748-x M12, 166
 - W748-x RJ45, 166
 - W786, 169
 - W786C, 172
 - W788C, 172
 - W788-x M12, 166
 - W788-x RJ-45, 166
 - WLAN controller, 156
- SCALANCE W748-x M12
 - Description, 166
 - Features, 167
 - Functions, 167
 - Interfaces, 168
- SCALANCE W748-x RJ-45
 - Description, 166
 - Features, 167
- Functions, 167
- Interfaces, 168
- SCALANCE W760/720
 - Features, 161, 164
 - Functions, 162, 164
- SCALANCE W760/W720
 - Description, 161
 - Interfaces, 163
- SCALANCE W770/W730
 - Description, 163
 - Interfaces, 165
- SCALANCE W786
 - Description, 169
 - Features, 170
 - Functions, 170
 - Interfaces, 171
- SCALANCE W786C
 - Description, 172
 - Features, 173
 - Functions, 174
 - Interfaces, 175
- SCALANCE W788C
 - Description, 172
 - Features, 173
 - Functions, 174
 - Interfaces, 175
- SCALANCE W788-x M12
 - Description, 166
 - Features, 167
 - Functions, 167
 - Interfaces, 168
- SCALANCE W788-x RJ-45
 - Description, 166
 - Features, 167
 - Functions, 167
 - Interfaces, 168
- SCALANCE WLC711
 - Description, 172
 - Interfaces, 175
- SCALANCE X
 - Performance classes, 114
 - X005, 120
 - X200/X200 IRT, 130
 - X300, 136
 - X500, 149
 - XB000, 122
- SCALANCE X005
 - Description, 120
 - Functions, 121
 - Interfaces, 121
- SCALANCE X200/X200 IRT
 - Description, 130

- Features, 131
- Functions, 131
- Interfaces, 132
- SCALANCE X300
 - Description, 136
 - Features, 136
 - Functions, 137
 - Interfaces, 138
 - Media modules, 141
 - SFP transceiver, 142
- SCALANCE X500
 - Description, 149
 - External power supply unit, 154
 - Features, 150
 - Functions, 151
 - Interfaces, 151
 - Media modules, 153
 - SFP transceiver, 153
- SCALANCE XB000
 - Characteristics, 122
 - Description, 122
 - Interfaces, 122
- SCALANCE XB200
 - Interfaces, 128
- SCALANCE XB-200
 - Functions, 127
- SCALANCE XC100-4OBR
 - Interfaces, 125
- SCALANCE XM-400
 - Features, 144
 - Functions, 144
- Security modules, 109
- SFP transceiver
 - SCALANCE X300, 142
 - SCALANCE X500, 153
- Shared LAN, 42
- Shared medium, 52
- Signaling contact, 118
- Silent listener
 - Wireless network, 45
- SIMATIC iMap, 16
- SIMATIC mode, 257
- SIMATIC NET, 11
- SIMATIC NET glossary, 4
- SIMATIC S7-200
 - CP 243-1, 242
- SIMATIC S7-300
 - CP 343-1 Advanced, 244
 - CP 343-1 Lean, 244
- SINEMA Server, 218
- Slip contacts, 45
- SNMP agent, 257

- Spanning Tree, 77
 - Multiple Spanning Tree, 78
 - Rapid Spanning Tree, 77
- SSH, 82
- Standalone network, 53
- Standards for general purpose cable communications networks
 - Industrial environment, 285
- Standards for general-purpose cable communications networks
 - Office environment, 285
- Standby redundancy, 68
- Star
 - Network topology, 62
- Star coupler, 42
- Stateful packet inspection, 82
- Static routing, 40
- Store and forward, 39
- Subnet mask, 22
- Switch, 42, 62, 109
- Switched LANs, 42

T

- TIA, 17
- Time-of-day synchronization on the RNA interface, 257
- Totally Integrated Automation, 17
- Trailing cable, 45
- Tunneling, 83

U

- UMTS, 109

V

- Virtual Private Network, 83
- VPN, 83

W

- Web diagnostics, 257
- WEP, 50
- Wi-Fi Protected Access, 50
- Wired Equivalent Privacy, 50
- Wireless cell, 52, 52
- Wireless networks
 - Unstructured, 59
- WLAN, 44
- WPA, 50

WPA2, 50