

SIEMENS

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

Cloud Gateway 5

TeleControl 6

Communications processors
for PCs 7

Communications processors
for SIMATIC S7 8

Compact switch module 9

Gateways 10

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. On the other hand, it provides configuration engineers and commissioning personnel with extensive information data to which they can refer when setting up their network systems.

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 - 9	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 for most network components of SIMATIC NET, such as 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 principle of operation 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 different 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 on the Internet at the following address:

50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

Table of contents

	Preface	3
1	Basics of communication with Industrial Ethernet	15
1.1	Terminology	15
1.2	Industrial Ethernet.....	16
1.2.1	Basics of Industrial Ethernet	16
1.2.2	PROFINET	18
1.2.2.1	Basics of PROFINET	18
1.2.2.2	PROFINET IO	20
1.2.3	SIMATIC NET	20
1.2.4	Transmission procedures and real-time response	23
1.2.5	Time-Sensitive Networking	24
1.2.5.1	Introduction	24
1.2.5.2	Time synchronization	25
1.2.5.3	TSN configuration (IEEE 802.1Q).....	26
1.2.5.4	OPC UA PubSub	26
1.3	Technologies of Industrial Ethernet	27
1.3.1	Communications media	27
1.3.2	Basics of communication with IP	28
1.3.2.1	IPv4 address	28
1.3.2.2	Structure of an IPv6 address	30
1.3.2.3	IPv4 / IPv6.....	32
1.3.2.4	IPv6 terms	35
1.3.3	Active and passive network components.....	37
1.3.4	Management functions.....	40
1.3.5	Power over Ethernet (PoE).....	41
1.3.6	Fault tolerance and redundancy	44
1.3.7	Access Methods.....	45
1.3.8	Layer 3 functions.....	46
1.3.9	EtherNet/IP	49
1.4	Switches and switched LANs.....	50
1.5	Wireless LAN	52
1.5.1	What is wireless LAN?	52
1.5.2	Differences between wireless LAN and wired networks.....	52
1.5.3	Preferred areas of application for WLANs	53
1.5.4	The standards of the "IEEE 802.11" series	53
1.5.5	IEEE 802.11n/ac	55
1.5.6	IEEE 802.11r.....	57
1.5.7	Encryption and data security	58
1.5.8	Avoiding collisions in wireless networks	59
1.5.9	Structure of an IWLAN	60

1.5.10	Network structures	61
1.5.10.1	Infrastructure mode	61
1.5.10.2	Ad hoc networks.....	66
1.5.11	Other wireless technologies	66
1.6	Industrial Wireless Control	67
1.6.1	Mobile wireless standards GSM, UMTS and LTE	67
1.6.2	The mobile wireless standard of the 5th generation	68
2	Network structures and network configuration	71
2.1	Integration of a production network in an enterprise network	71
2.2	Network structures	75
2.2.1	Network topologies	75
2.2.2	Linear structure	75
2.2.3	Star structure.....	76
2.2.4	Ring structure.....	79
2.2.5	Redundant coupling of network segments with electrical and fiber-optic components	81
2.2.6	VLAN.....	82
2.3	Media redundancy	82
2.3.1	Options of media redundancy	82
2.3.2	Media redundancy in ring topologies	83
2.3.3	MRP	84
2.3.4	MRP Interconnection	86
2.3.5	MRPD.....	88
2.3.6	HRP.....	89
2.3.7	PRP.....	89
2.3.8	RNA.....	91
2.3.9	STP / RSTP / MSTP	92
2.3.10	RSTP+.....	93
2.3.10.1	Properties and functions of RSTP+	93
2.3.10.2	Topology for RSTP+	94
2.3.11	Link aggregation.....	97
2.4	Network security.....	98
2.4.1	The Industrial Security concept of Siemens	98
2.4.2	Firewalls	100
2.4.3	NAT/NAPT	101
2.4.4	"Virtual Private Networks" (VPNs)	102
2.4.5	Cell protection concept	102
2.4.6	SIMATIC NET products for network security	104
3	Examples of applications	107
3.1	Virtual segmentation	107
3.2	Redundantly coupled networks.....	108
3.3	Data protection during remote maintenance.....	110
3.4	Cell protection concept	111
3.5	Network for high data throughput and many nodes.....	113
3.6	Optimization of a power screwdriver control.....	114
3.7	Controlling material transportation with SCALANCE components	116

3.8	Crane carriage control for a high-bay warehouse	118
3.9	Using Power over Ethernet	120
3.10	Connecting a PROFIBUS network to a PROFINET installation	121
3.11	Communication components for extreme ambient conditions	123
3.12	Process automation in hazardous areas	125
4	SCALANCE network components	127
4.1	Industrial networks with SIMATIC NET	127
4.2	Product families	128
4.3	Common properties of all SCALANCE devices	129
4.4	Web Based Management for configuring networks	131
4.5	SCALANCE X Industrial Ethernet Switches	133
4.5.1	Overview of the performance classes	133
4.5.2	Type designations	134
4.5.3	Functions of SCALANCE X devices	137
4.5.4	SCALANCE TAP	139
4.5.4.1	Description	139
4.5.4.2	Characteristics	140
4.5.4.3	Interfaces	140
4.5.4.4	Article numbers	140
4.5.5	SCALANCE X-000	140
4.5.5.1	Description	140
4.5.5.2	Features	141
4.5.5.3	Interfaces	141
4.5.5.4	Article numbers	141
4.5.6	SCALANCE XB-000	142
4.5.6.1	Description	142
4.5.6.2	Characteristics	143
4.5.6.3	Interfaces	143
4.5.6.4	Article numbers	143
4.5.7	SCALANCE X-100	144
4.5.7.1	Description	144
4.5.7.2	Characteristics	145
4.5.7.3	Interfaces	145
4.5.7.4	Article numbers	146
4.5.8	SCALANCE XB-100	146
4.5.8.1	Description	146
4.5.8.2	Features	147
4.5.8.3	Interfaces	147
4.5.8.4	Article numbers	147
4.5.9	SCALANCE XC-100	148
4.5.9.1	Description	148
4.5.9.2	Features	148
4.5.9.3	Interfaces	149
4.5.9.4	Article numbers	149

4.5.10	SCALANCE XR-100WG	150
4.5.10.1	Description	150
4.5.10.2	Features	150
4.5.10.3	Interfaces	150
4.5.10.4	Article numbers	151
4.5.11	SCALANCE X-200IRT	151
4.5.11.1	Description	151
4.5.11.2	Features and functions	152
4.5.11.3	Interfaces	153
4.5.11.4	Article numbers	154
4.5.12	SCALANCE X-200RNA	154
4.5.12.1	Description	154
4.5.12.2	Features and functions	155
4.5.12.3	Interfaces	156
4.5.12.4	Article numbers	156
4.5.12.5	Accessories SFP transceiver	157
4.5.13	SCALANCE XB-200	158
4.5.13.1	Description	158
4.5.13.2	Features and functions	158
4.5.13.3	Interfaces	160
4.5.13.4	Article numbers	160
4.5.14	SCALANCE XC-200	161
4.5.14.1	Description	161
4.5.14.2	Features and functions	162
4.5.14.3	Interfaces	163
4.5.14.4	Article numbers	164
4.5.14.5	Accessories SFP transceiver	165
4.5.15	SCALANCE XF-200/XF-200IRT	168
4.5.15.1	Description	168
4.5.15.2	Features and functions	169
4.5.15.3	Interfaces	170
4.5.15.4	Article numbers	170
4.5.15.5	Accessories bus adapter	171
4.5.16	SCALANCE XF-200BA	172
4.5.16.1	Description	172
4.5.16.2	Features and functions	173
4.5.16.3	Interfaces	174
4.5.16.4	Article numbers	175
4.5.17	SCALANCE XP-200	175
4.5.17.1	Description	175
4.5.17.2	Features and functions	176
4.5.17.3	Interfaces	177
4.5.17.4	Article numbers	177
4.5.18	SCALANCE X-300	178
4.5.18.1	Description	178
4.5.18.2	Features and functions	180
4.5.18.3	Interfaces	181
4.5.18.4	Article numbers	181
4.5.18.5	Media modules and SFP transceivers	183

4.5.19	SCALANCE XR-300WG	185
4.5.19.1	Description	185
4.5.19.2	Features and functions	185
4.5.19.3	Interfaces	186
4.5.19.4	Article numbers	187
4.5.19.5	Accessories SFP transceiver	187
4.5.20	SCALANCE XM-400	189
4.5.20.1	Description	189
4.5.20.2	Features and functions	189
4.5.20.3	Interfaces	191
4.5.20.4	Article numbers	191
4.5.20.5	Accessories SFP transceiver	192
4.5.20.6	Extender modules SCALANCE PE-400	194
4.5.20.7	External power supply units SCALANCE PS-900PoE	195
4.5.21	SCALANCE XR-500	197
4.5.21.1	Description	197
4.5.21.2	Features and functions	198
4.5.21.3	Interfaces	199
4.5.21.4	Article numbers	199
4.5.21.5	Media modules and SFP transceivers	201
4.5.21.6	External power supply unit SCALANCE PS598-1	202
4.6	SCALANCE W components for the Industrial Wireless LAN.....	203
4.6.1	SCALANCE W devices	203
4.6.2	Type designations	206
4.6.3	IEEE 802.11r.....	206
4.6.4	Functions of WLAN devices.....	207
4.6.5	IEEE 802.11n/ac	209
4.6.6	SCALANCE W760/W720.....	212
4.6.6.1	Description	212
4.6.6.2	Features and functions	213
4.6.6.3	Interfaces	214
4.6.6.4	Article numbers	214
4.6.7	SCALANCE W774/W734.....	215
4.6.7.1	Description	215
4.6.7.2	Features and functions	216
4.6.7.3	Interfaces	217
4.6.7.4	Article numbers	217
4.6.8	SCALANCE W778/W738.....	218
4.6.8.1	Description	218
4.6.8.2	Features and functions	219
4.6.8.3	Interfaces	220
4.6.8.4	Article numbers	220
4.6.9	SCALANCE W786	221
4.6.9.1	Description	221
4.6.9.2	Features and functions	221
4.6.9.3	Interfaces	223
4.6.9.4	Article numbers	223
4.6.10	SCALANCE W788/W748.....	224
4.6.10.1	Description	224
4.6.10.2	Features and functions	225
4.6.10.3	Interfaces	226
4.6.10.4	Article numbers	226

4.6.11	SCALANCE W1788/W1748	227
4.6.11.1	Description	227
4.6.11.2	Features and functions	228
4.6.11.3	Interfaces	229
4.6.11.4	Article numbers	230
4.6.12	SCALANCE W1750D	231
4.6.12.1	Description	231
4.6.12.2	Features and functions	231
4.6.12.3	Interfaces	233
4.6.13	Antennas	233
4.6.13.1	How it works	233
4.6.13.2	Product overview	236
4.7	SCALANCE M industry router	241
4.7.1	Overview	241
4.7.2	SCALANCE M812-1, M816-1 and M826-2	244
4.7.2.1	Description	244
4.7.2.2	Features and functions	245
4.7.2.3	Article numbers	246
4.7.3	SCALANCE M874-3 and M-876-4	247
4.7.3.1	Description	247
4.7.3.2	Features and functions	249
4.7.3.3	Article numbers	250
4.7.4	SCALANCE M804PB	250
4.7.4.1	Description	250
4.7.4.2	Features and functions	251
4.7.4.3	Interfaces	252
4.7.4.4	Article numbers	252
4.7.5	TeleService Adapter IE	252
4.7.5.1	Description	252
4.7.5.2	Features and functions	254
4.7.5.3	Article numbers	254
4.7.6	Modem MD720	255
4.7.6.1	Description	255
4.7.6.2	Features and functions	256
4.7.7	Antennas for mobile wireless	258
4.7.7.1	Product overview	258
4.8	SCALANCE S Industrial Security Appliance	261
4.8.1	Overview	261
4.8.2	Technical basics	262
4.8.3	Description	265
4.8.4	Features and functions	266
4.8.5	Interfaces	267
4.8.6	Article numbers	268
4.8.7	SOFTNET Security Client	268
4.8.8	SINEMA RC	271
4.9	Network management software	274
4.9.1	Primary Setup Tool	274
4.9.2	SINEC NMS	277
4.9.3	SOFTNET TSN	280

4.10	Accessories	282
4.10.1	C-PLUG Configuration Memory	282
4.10.2	KEY-PLUG	283
4.10.3	Configuration License PLUG (CLP)	285
5	Cloud Gateway	287
5.1	Description	287
5.2	Features and functions	289
5.3	Article numbers	290
6	TeleControl	291
6.1	SIMATIC RTU3000C	291
6.2	Description	293
6.3	Features and functions	294
6.4	Interfaces	295
6.5	Article numbers	296
7	Communications processors for PCs.....	299
7.1	CP 1604	300
7.2	CP 1616	302
7.3	CP 1623	303
7.4	CP 1626	304
7.5	CP 1628	306
8	Communications processors for SIMATIC S7.....	309
8.1	SIPLUS version.....	310
8.2	Communications processors for SIMATIC S7-300.....	311
8.3	Communications processors SINAUT ST7 for SIMATIC S7-300.....	317
8.4	Communications processors for SIMATIC S7-400.....	319
8.5	Communications processors for SIMATIC S7-1200.....	327
8.6	Communications processors for SIMATIC S7-1500.....	330
8.7	Communication module TIM 1531 IRC.....	335
8.8	Communication processors for SIMATIC ET 200SP.....	339
9	Compact switch module	343
9.1	CSM 377	344
9.2	CSM 1277	346
9.3	LOGO! CSM.....	348

10	Gateways	351
10.1	IE/PB Link PN IO.....	353
10.2	IE/AS-i Link PN IO.....	355
10.3	PN/BACnet Link Gateway	356
10.4	PN/CAN link	358
A	Appendix	361
A.1	Overview of the standards relevant for network installation	361
A.2	Content of the standards.....	363
A.3	Application of the standards.....	364
	Index	365

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
- Plant-specific network topologies with a focus on linear, redundant network structures.

The components must meet the following requirements:

- Industrial equipment, for example, signaling contacts, secure cables and plug-in connectors
- Capability of withstanding extreme environmental conditions, for example extreme temperatures, vibration, dust, dampness, electromagnetic interference.

PROFINET

The term PROFINET refers to the standard for Industrial Ethernet (IEC 61158/61784) that is drawn up and supported by the Profibus & Profinet International (PI).

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
- High transmission safety, reliability and availability requirements

PROFINET contrasts with the office environment whose emphasis is more on high data throughput and an extensive network. 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 variety of **network components** that are available for innovative, consistent realization of automation solutions under the umbrella of "Totally Integrated Automation". PROFINET is the protocol that is used most often by SIMATIC NET components in the context of the 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) that 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 through FastConnect cabling system:
 - Assembly of copper cables with RJ45 and M12 technology
 - Assembly of POF, PCF and glass fiber-optic cables (multimode)
- High transmission performance even with large numbers of nodes thanks to the end-to-end availability of components with 10/100, 1 Gbps and 10 Gbps
- Ethernet with real-time capability that fulfils high requirements for the reaction time (PROFINET IRT, TSN)
- 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, since scalable performance available through switching technology when necessary
- Networking of different areas of application such as office and production
- Procedure for extremely fast handover of mobile IWLAN nodes between different access points and therefore fast cyclic data communication (iPCF and iPCF-MC)
- Communication throughout the enterprise with the option of linking via WAN (Wide Area Network), such as DSL or mobile wireless, for example

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 cables.

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 1 Gbps or 10 Gbps.

The relevant standards are as follows:

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

The increase in the transmission speed is achieved not only by adaptation of the protocol but also by using category 5e, 6, 6A and 7 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.
- Determinism
The same conditions always lead to the same results and there are no undefined statuses.

See also

Transmission procedures and real-time response (Page 23)

Fault tolerance and redundancy (Page 44)

Access Methods (Page 45)

1.2.2 PROFINET

1.2.2.1 Basics of PROFINET

What is PROFINET?

PROFINET is the 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 23)".

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.

- PROFI-safe

The PROFI-safe 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 (PROFI-safe 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 PROFI-safe frame. Existing solutions can be expanded without needing to change cabling.

PROFI-safe prevents errors such as address corruption, loss, delay, etc. when transferring messages by consecutively numbering the PROFI-safe 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**.
- 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 (<https://www.profibus.com>) of PROFIBUS & PROFINET (PI) International.

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

1.2.2.2 PROFINET IO

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).

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 that offers a consistent basis for the realization of 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 compatible. In addition to the previous wired solutions, wireless communication is gaining ground in industry. SIMATIC NET offers products for company-wide data transmission over local networks, intranet, Internet or wireless networks.

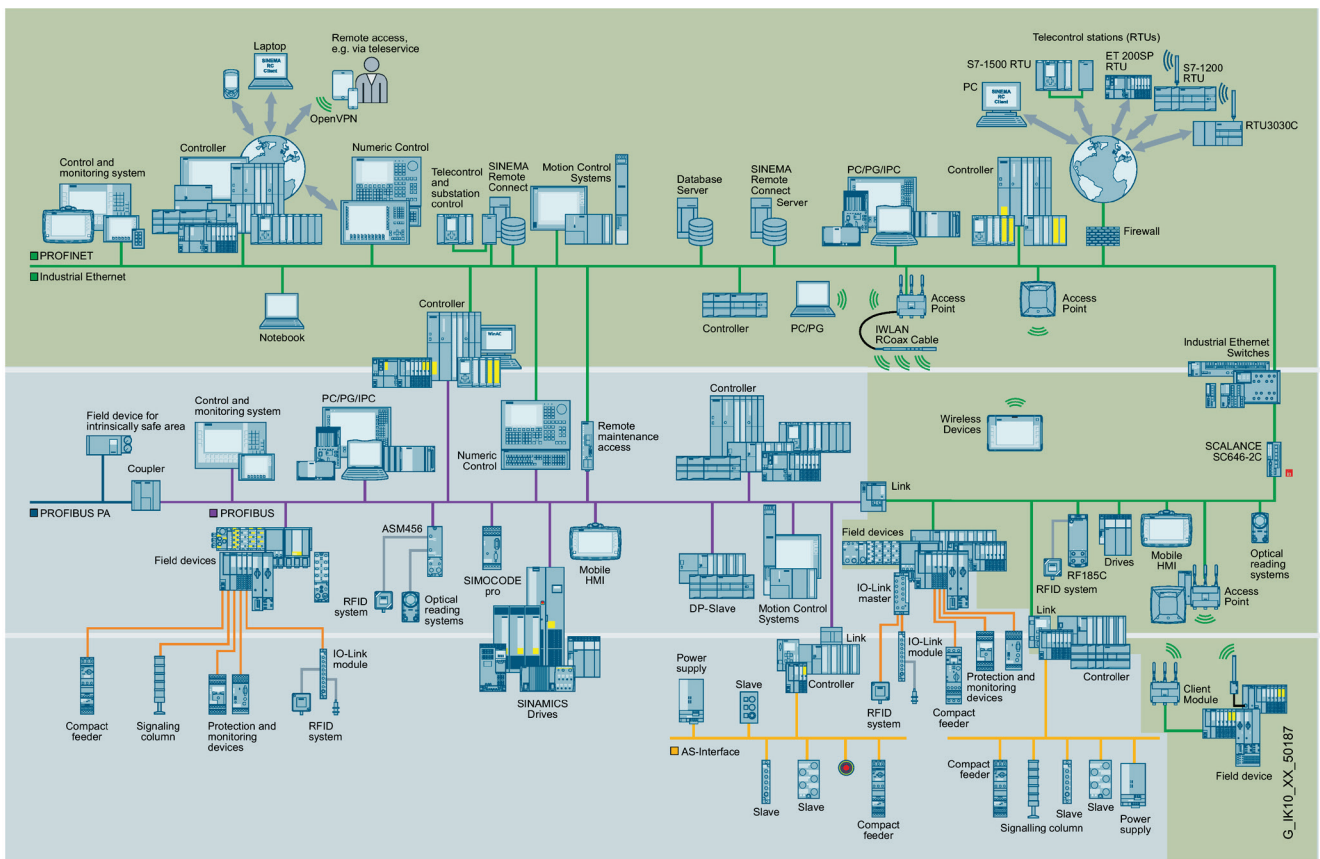


Figure 1-1 Industrial Ethernet and PROFINET in the SIMATIC NET environment

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 constitute the latest and most progressive generation of active SIMATIC NET network components.

Technical requirements

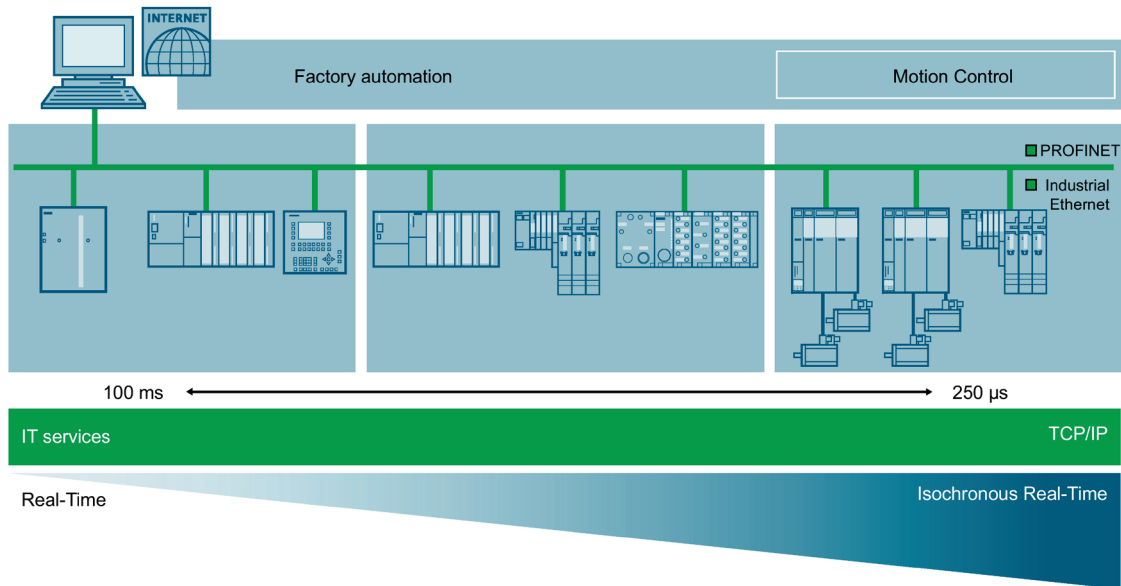
Communication networks are a central part of modern automation solutions. Industrial networks must fulfil special requirements, for example:

- Coupling 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 are part of the LANs (Local Area Networks) and enable the communication in a regionally limited area.

1.2.4 Transmission procedures and real-time response

Overview



G_IK10_XX_30116

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.

The 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 but without the "best possible synchronicity".

Unsynchronized IO devices automatically exchange data using the RT communication.

Isochronous real-time communication (IRT communication)

In PROFINET with the 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. Through these methods update times of up to 31.25 μs can be reached.

The IRT communication is used in areas with particularly stringent requirements for response times that must not 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. The use of special switches is required in this case. In SIMATIC NET, the suitable switches have "IRT" in their product names.

1.2.5 Time-Sensitive Networking

1.2.5.1 Introduction

Definition of terms and purpose

Time-Sensitive Networking (TSN) is the name for a set of standards for Ethernet communication with real-time capability. Real-time capability is the data transfer within fixed assigned time limits.

Standard Ethernet according to IEEE 802.3 does not offer real-time capability. In the past, manufacturer-specific extensions, such as PROFINET IRT, were required for this purpose. The goal of Time-Sensitive Networking is to make Ethernet usable for applications even without manufacturer-specific extensions. This requires a deterministic time behavior, for example, control engineering.

Requirements

To enable real-time communication in a network, a technology must fulfil the following requirements:

- **Time synchronization**
Depending on the application case, time synchronization can reference the work cycle of a machine or "time" in form of a chronologically defined time. Scanning or communication cycles are synchronized to increase the quality of the application or the data transfer. Details on the time-synchronization for TSN are specified in the standards IEEE 1588 and IEEE 802.1AS-2019.
- **Loss-free timely transfer**
The observance of time limits must be ensured for time-critical data packets even under high network loads. Consequently, there have to be mechanisms to identify time-critical data packets and reliably transmit them within the required duration.
- **Configuration of a TSN network**
The requirements placed by the nodes regarding data transfer have to be coordinated with the resources available in the network. This comparison can take place with or without a central system for the network management.
- **Standardized data model on application layer (OPC UA PubSub)**
Standards that take into account the special requirements of real-time capability are required on the application level for manufacturer- and device-independent data exchange. Starting point is the OPC UA communication protocol that has already established itself in the industrial environment and that was originally designed for a client server architecture. If a real-time network exists, the requirements of the real-time communication with cyclic data exchange through the extension OPC UA Publish-Subscribe ("PubSub") are fulfilled.

1.2.5.2 Time synchronization

Precision Time Protocol (PTP)

For TSN there is no specification which system must be used for time synchronization. The Precision Time Protocol (PTP) offers considerable advantages in contrast to other methods of time synchronization:

- PTP allows for time synchronization with very high accuracy in the microsecond range. This high accuracy is reached because PTP considers all delays occurring during data transfer. The frequently used Network Time Protocol (NTP) offers an accuracy in the range of milliseconds, which is not sufficient for application cases with real-time requirements.
- Devices and infrastructure for receiving external time signals, for example, via radio or GSM or for the provision of the work cycle of machines are not required.

The IEEE 802.1ASrev standard for the special features of data transfer with real-time requirements. IEEE 802.1ASrev is a profile for PTP, that is, a specification of attributes and options.

You can find detailed information on the topic Precision Time Protocol in the section "Technical basics > Precision Time Protocol (PTP) complying with IEEE 1588".

1.2.5.3 TSN configuration (IEEE 802.1Q)

The IEEE 802.1Qcc standard describes three possibilities of the TSN configuration. The suitable configuration method is dependent on the application example, the size of the network and the properties of the devices.

- **Distributed configuration of end devices and the network**
Each device reports its requirements to the TSN switch to which it is connected. The TSN switch distributes this information in the network. A central instance is not necessary for this. During the assignment of the resources, the TSN switch does not require any information about the entire network. Only the transmission path of the stream is relevant for the configuration. The talker begins with the data transfer if at least one listener is logged on to the stream and if the required resources are available between talker and listener.
- **Central configuration of the network and distributed configuration of the end devices**
Each switch is configured by a central network management (Centralized Network Configuration, CNC). The network management disposes of complete topology information and information about the properties of the bridge devices. As in distributed configuration, the end device signals its requirements to the TSN switch. The TSN switch transmits this information to the central network management.
- **Central configuration of network and end devices**
All devices, including the end devices, are configured centrally. The central network management creates a configuration for the complete system that considers all requirements of the nodes and makes the required configuration parameters available to each node.

1.2.5.4 OPC UA PubSub

OPC UA as manufacturer-independent interface

For data exchange on the application level, the OPC UA interface can be used for the TSN. OPC was originally developed on the basis of DCOM, a system for remote procedure calls from Microsoft. The acronym OPC was the abbreviation for OLE for Process Control. The goal was to create an open standard for data exchange in automation technology. For the OPC UA further development introduced in 2006, a communication stack was implemented that is independent of COM/DCOM and the Windows operating system. Since then the acronym OPC UA stands for Open Platform Communications Unified Architecture.

Publish-Subscribe-Stack for cyclic data exchange

OPC UA uses the client-server principle. The sequence of query of the client and response of the server ensures a reliable data exchange via a secured connection. For cyclic data exchange, often also with multiple participants (multicast), this principle, however, is only suitable to a limited extent. The Publish-Subscribe communication, shortened "PubSub", was developed additionally for this special application.

A Publisher is the sender of news, Subscriber(s) are the receivers. The Publish-Subscribe communication uses UDP, TSN or MQTT (for the cloud connection) as lower-level protocols. If only TSN-capable devices are used for a transmission link, the OPC UA PubSub enables a deterministic data transfer on the application level ("OPC UA over TSN").

User-Network Interface

A deterministic data transfer between two devices can only work if the communication requirements of the devices match the resources available in the network. A suitable transmission path must be made available for time-critical OPC UA data. The User Network Interface (UNI) automatically takes on this decentralized coordination task. The special advantage for users is that a system is not required for the central configuration.

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
- Optical cabling
- 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	<ul style="list-style-type: none"> • Cables for indoors and outdoors according to the cable characteristics • Trailing cable • Cable free of halogens • Ship cable • FastConnect cables 	<ul style="list-style-type: none"> • Cables for indoors and outdoors • Trailing cable • Cable free of halogens 	--
The effect of failure of a network section	In a ring, no effect. In simple structures, the network breaks down into two isolated subnetworks	In a ring, no effect. In 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) <ul style="list-style-type: none"> • 50 m POF • 100 m PCF • 5000 m multimode • Up to 200 km single mode GE (1000 Mbps) <ul style="list-style-type: none"> • 750 m multimode • 2000 m multimode • 120 km single mode 10 GE (10000 Mbps) <ul style="list-style-type: none"> • 750 m multimode • 40 km single mode 	Up to several kilometers depending on the environmental conditions, Check via Link (https://webservices.siemens.com/tstcloud/#/Start/)
Preassembled cables	yes	yes	--
Redundant network structures	Electrical ring or duplication of the infrastructure (bus, star, tree)	Optical ring or duplication of the infrastructure (line, 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 "1" values 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 subnetwork mask. To this purpose, 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 between 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	<ul style="list-style-type: none"> • DHCP server • Manual 	<ul style="list-style-type: none"> • Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) <ul style="list-style-type: none"> – 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		<p><i>Duplicate address detection</i></p> <p>Procedure to ensure that an IP address is only assigned to one interface within the framework of the Stateless Automatic Address Configuration.</p> <p>What happens if the address is duplicated? An LLA must then be assigned manually.</p>
Available IP addresses	32-bit: $4, 29 * 10^9$ addresses (32-bit)	128-bit: $3, 4 * 10^{38}$ 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	<p>Multiple IP addresses</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Checksum • Variable length • Fragmentation in the header • No security 	<ul style="list-style-type: none"> • 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	<p>ICMPv6</p> <p>Router Solicitation (ICMPv6 type 133) Sent by a client to localize servers.</p> <p>Router Advertisement Messages (ICMPv6 type 134) Sent by a server as response to a Solicit message to indicate availability.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Ports	UDP RIP: UDP 520	DHCP, ports client 546 & server 547 RIPng: 521
Router discovery	optional	<p>mandatory</p> <p>When router discovery is used in addition, the node is informed of the following</p> <ul style="list-style-type: none"> • 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	<p>DUID + IAID(s) = exactly one interface of the host</p> <p>DUID = DHCP unique identifier</p> <p>Identifies server and clients uniquely and should not change. No modification when replacing network components.</p> <p>IAID = Identity Association Identifier</p> <p>at least one per interface is generated by the client and remains unchanged when the DHCP client restarts</p> <p>Three methods of obtaining the DUID</p> <ul style="list-style-type: none"> • 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 all servers and relay agents belong to the corresponding group. These in turn listen on port 547. Local servers and relay agents reach a client by means of 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 the known sub-network prefixes assigned to a link. Nodes use prefixes to distinguish destinations on the local link that can only be reached via a router. Address resolution - helps nodes when detecting the link-local address of a neighbor node provided that 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 the 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 the node to determine whether an address wanted by the 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

Two network nodes are called neighbors when they are located on the same link.

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 nodes located on the same link.

ULA

Unique Local Address

Defined in RFC 4193. The IPv6 interface can be reached via this address in the LAN.

GUA

Global Unicast Address The IPv6 interface can be reached through this address, for example, via the Internet.

Interface ID

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

EUI-64

Extended Unique Identifier (RFC 4291); process 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

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 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
	IE PB Link PN IO	Used to couple PROFINET to PROFIBUS
	SCALANCE S	Industrial Security Appliances 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 SCALANCE W786-2SFP SCALANCE S	see above
Radio (wireless)	SCALANCE W Access Point and Client Module	Components for wireless transmission of Ethernet
	SCALANCE M	For wireless linking of Industrial Ethernet-based programmable controllers on the 2G/3G/4G mobile wireless network

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

Medium	Connectors	Cable type / transmission medium Standard
Copper (electrical)	RJ45 plug-in connector IE FC RJ-45 plug 90/145/180 M12 plug-in connector D-coded, X-coded, A-coded, L-coded	Two pair, symmetric 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 2x2 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)
	ST/BFOC (Bayonet Fiber Optic Connector) ISO/IEC 60874-10 SC plug ISO/IEC 60874-14 LC connector IEC 61754-20	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 duplex FO marine cables (for ST/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 ST/BFOC and SC connector)

Medium	Connectors	Cable type / transmission medium Standard
Radio (wireless)	N-Connect R-SMA SMA QMA	<p>IEEE 802.11/mobile wireless (2G, 3G, 4G)</p> <p>Antenna cables (in each case standard cable and cables suitable for railway applications):</p> <ul style="list-style-type: none"> • 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 W 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 <p>Antennas:</p> <ul style="list-style-type: none"> • 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 installation**

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 a detailed overview of the available modules and accessories in chapters 4 - 9.

Passive components for Industrial Ethernet and accessories

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

Passive components for IWLAN

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

See also

SCALANCE X Industrial Ethernet Switches (Page 133)

SCALANCE W components for the Industrial Wireless LAN (Page 203)

SCALANCE M industry router (Page 241)

SCALANCE S Industrial Security Appliance (Page 261)

Communications processors for PCs (Page 299)

Communications processors for SIMATIC S7 (Page 309)

Compact switch module (Page 343)

Accessories (Page 282)

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 (PoE)

Power supply via Ethernet cables

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+.

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+)
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)

Characteristic	802.3af (also 802.3at type 1 or PoE)	802.3at Type 2 (also PoE+)
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 6 _A and CAT 7
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 as well as 7-8 are used for power supply. All cables CAT 5, CAT 5e, CAT 6, CAT 6_A and CAT 7 fulfil this requirement.

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+, a safety circuit is defined:

- If the PSE identifies a resistance of 25 kΩ 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 Ethernet cables. 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 via unused 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 W1780/W1740 (PD)
- SCALANCE W1750D-2IA RJ45 (PD)
- 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 XP208PoE EEC (PSE)
- SCALANCE XP216PoE EEC (PSE)
- SCALANCE X308-2M PoE (PSE)
- SCALANCE XR324-4M PoE (PSE)
- SCALANCE XR324-4M PoE TS (PSE)

PoE+ 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 XP208PoE EEC (PSE)
- SCALANCE XP216PoE EEC (PSE)
- SCALANCE X308-2M PoE (PSE)
- SCALANCE XR324-4M PoE (PSE)
- SCALANCE XR324-4M PoE TS (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 A" 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, communication via the parallel network remains unaffected.

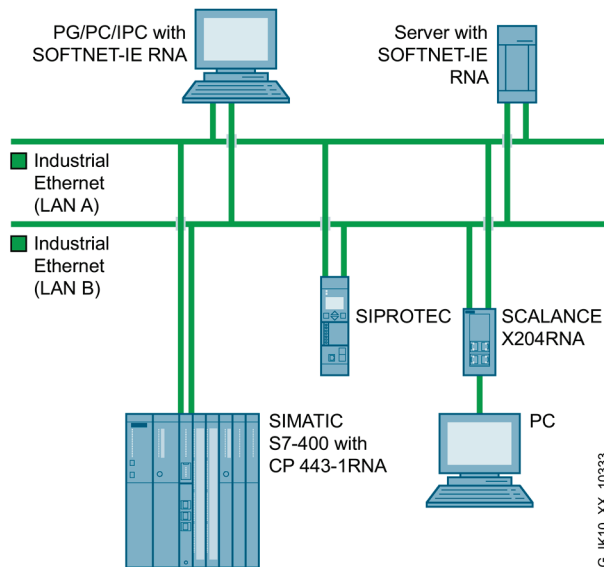


Figure 1-2 Topology example of a redundant network

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 50)

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 subnetworks and VLANs to its ports, for example, subnetwork A and subnetwork B. This allows large networks to be divided into smaller subnetworks with their own address range. 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.

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 VRRPv2

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 affected network area 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.

VRRPv3

Version 3 of VRRP is based on Version 2. VRRPv3 has the following characteristics:

- VRRPv3 supports IPv4 and IPv6. Both can be configured and operated at the same time with VRRP3.
- Simultaneous operation of VRRPv2 and VRRPv3 is not possible.
- You can only use VRRPv3 in conjunction with VLAN interfaces. Router ports are not supported.

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 most inexpensive route is entered. The algorithm uses the costs of the path as a metric. 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.

OSPFv3

Version 3 of OSPF is based on Version 2 and is only used with IPv6. A large part of the routing mechanisms was adopted. In comparison to OSPFv2 the following changes or extensions apply for OSPFv3:

- The authentication available in version 2 has been removed. Instead OSPFv3 uses IPsec, that is implemented in IPv6.
- The neighbor routers are identified via the router ID.
- The neighbor database (link state database - LSDB) is divided into different areas of application: Link Scope LSDB, Area Scope LSDB and AS-Scope LSDB.
- Two new LSA types were defined for OSPFv3 (Link LSA and Intra-Area Prefix LSA).
- In contrast to OSPFv2, OSPFv3 can forward unknown LSA types. Previously, these were deleted and not distributed further.

Dynamic routing with RIPv2

The Routing Information Protocol (RIPv2) is used to create routing tables automatically. RIPv2 is used in autonomous systems (AS) with a maximum of 15 hops. It is based on the Distance-Vector algorithm.

Since a router initially only knows its directly connected networks, it sends a request to its direct neighbor routers. As the reply, it receives the routing tables of the neighbor routers. Based on the received information the router sets up its own routing table.

Once the routing table is set up, the router sends its routing table to each direct neighbor router via the UDP port 520 at intervals of 30 seconds.

The router compares new routing information with its existing routing table. If the new information includes shorter routes, the existing routes are overwritten. The router only keeps the shortest route to a destination.

If a router does not receive messages from a neighbor router for longer than 180 seconds, it marks the router as being invalid. The router assigns the metric 16 for the neighbor router.

RIPng

RIPng (RIP next generation) is only used with IPv6 and is defined in RFC 2080. As with RIP (IPv4), RIPng is based on the distance-vector algorithm of Bellman-Ford.

In contrast to RIPv2, RIPng is activated directly at the interface (VLAN interface / router port) and not globally on the device. RIPng uses the UDP port 521 and RIP the UDP port 520.

PIM

Protocol Independent Multicast (PIM) allows the routing of multicast packets, regardless of lower-level routing protocols such as OSPFv2 or static routing (IPv4). PIM expands the routing information of the unicast routing protocol active on the router with additional information for multicast operation.

The following requirements must be met for the use of PIM:

- IGMP is enabled on the First-Hop and Last-Hop routers of the routing topology.
- PIM is enabled on all routers of the routing topology.
- There is at least one rendezvous point (RP).
- In every subnetwork there is a designated router (DR).
- The DR must also be the IGMP Querier.

NAT

NAT/NAPT is possible only on layer 3 of the ISO/OSI reference model. To use the NAT function, the networks must use the IP protocol.

In Network Address Translation (NAT), IP subnetworks are divided into "Inside" and "Outside". The division is affected from the perspective of a NAT interface. All networks reachable via the NAT interface itself count as "Outside" for this interface. All networks that can be reached via other IP interfaces of the same device count as "Inside" for the NAT interface.

If routing is carried out via a NAT interface, the source or destination IP addresses of the transferred data packets are changed at the transition between "Inside" and "Outside". Whether or not the source or destination IP address is changed depends on the communications direction. It is always the IP address of the communication node which is located "Inside" that is adapted. Depending on the perspective, the IP address of a communication node is referred to as "Local" or "Global".

1.3.9 EtherNet/IP

Introduction

EtherNet/IP is a fieldbus 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 using UDP as multicast, 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 also 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 to be 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 subnetworks 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 faulty 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 a sender does not block the entire network
- Increased protection against failure, 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.
- Possibility of forming subnetworks and network segments,
- Simple rules for network configuration,
- Simple expansion of existing networks

Application example: Redundant ring

Using an IE Switch as the redundancy manager in a ring with a redundancy manager (Page 79) 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 cables, routers or similar devices 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:

- Connecting freely mobile nodes to each other and with stationary nodes
- Connecting mobile nodes with wired networks (Ethernet, etc.)
- Contact to rotating nodes (cranes, carousels, etc.)
- Connection of participants with restricted mobility (overhead monorails, high-bay warehouses, etc.) as a replacement of sliding contacts or trailing cables
- Structure of wireless bridges between physically separated (different buildings, roads, water, etc.) wired subnets
- Communication with stations in areas that are hard to access

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 extensions of the standard are 802.11b, 802.11g, 802.11n, 802.11ac and 802.11ax.

"802.11" standards

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

	802.11a/h	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year of Introduction	1999	1999	2003	2009	2013	2019
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz + 5 GHz	5 GHz	2.4 GHz + 5 GHz
Bandwidth	20	20	20	20 / 40	40 / 80 / 160	80 / 160
Gross data rate	54 Mbps	Max. 11 Mbps	54 Mbps	600 Mbps	1733 Mbps (max. 6.93 Gbps)	19.2 Gbps
Modulation procedure	OFDM	DSSS	OFDM	OFDM	SC-OFDM	SC-OFDMA
Transmission system	SISO	SISO	SISO	SU-MIMO	MU-MIMO (down-link)	MU-MIMO (down-link und uplink)
Max. number of antennas on sender and receiver end	1x1	1x1	1x1	4x4	8x8	4x4

DSSS - direct sequence spread spectrum

OFDM - orthogonal frequency-division multiplex

SC-OFDM - single carrier orthogonal frequency-division multiplex

OFDMA - orthogonal frequency-division multiple access

SISO - Single Input Single Output

MIMO - Multiple Input Multiple Output

SU-MIMO - Single-User MIMO

MU-MIMO - Multi-User 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/ac

Overview

The IEEE 802.11ac standard is a further development of the IEEE 802.11n standard and is downward compatible with the standards IEEE 802.11a, IEEE 802.11h and IEEE 802.11n. The mechanisms of the PHY and MAC layer implemented in the IEEE 802.11n standard have been improved.

The following table contains the most important differences.

	IEEE 802.11n	IEEE 802.11ac
Frequency band	2.4 GHz and 5 GHz	5 GHz
Channel bandwidth	20 MHz, 40 MHz	20 MHz, 40 MHz, 80 MHz Optional: 160 MHz
Spatial streams (data streams)	1 to 4	1 to 8 Up to 4 per client
MIMO	Single-User MIMO	Multi-User MIMO
Modulation scheme	OFDM (BPSK, QPSK, 16-QAM, 64-QAM)	OFDM (BPSK, QPSK, 16-QAM, 64-QAM, 128-QAM, optional 256-QAM)

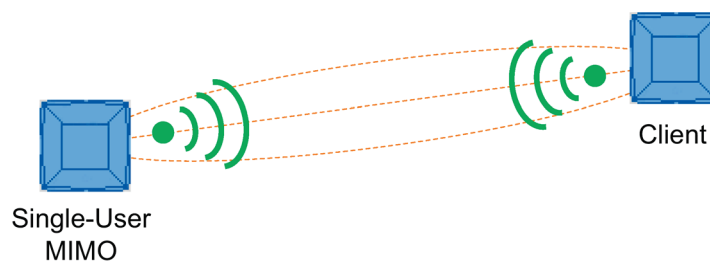
MIMO antenna technology

MIMO (Multiple Input - Multiple Output) is based on an intelligent multiple antenna system. The transmitter and the receiver have several spatially separate antennas. These separated antennas transmit the data streams (spatial streams) at the same time. Up to four data streams are possible with IEEE 802.11n and up to eight data streams with IEEE 802.11ac.

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. The specific characteristics of each sender enable the recipient to separate several signals from each other.

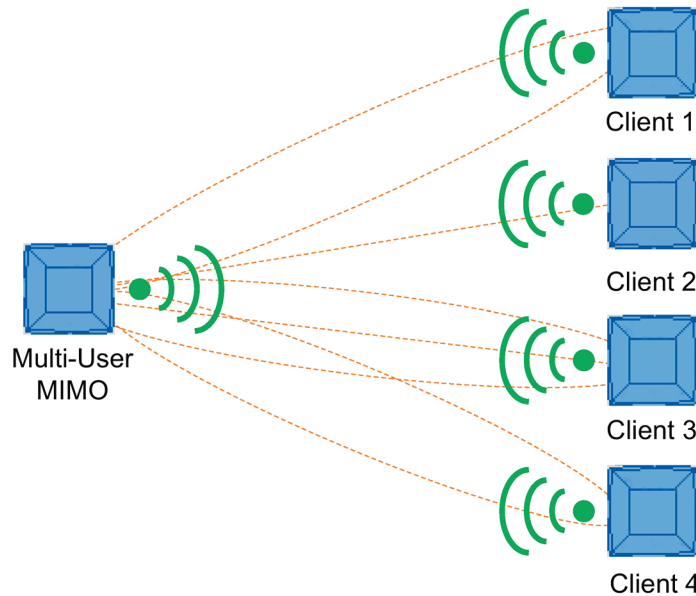
Single-User MIMO

With Single-User MIMO, the same frame is sent over multiple data streams to a single WLAN client. A single-user MIMO can operate up to four devices alternately, but only one device at a time.



Multi-User MIMO

With multi-user MIMO, multiple frames are sent simultaneously to different multi-user MIMO clients over the same frequency range. A multi-user MIMO therefore supplies up to four multi-user MIMO clients with data simultaneously.



Spatial multiplexing

With spatial multiplexing, different information is sent using the same frequency. The data stream is distributed over n transmitting antennas; in other words, each antenna sends only $1/n$ of the data stream. The division of the data stream is restricted by the number of antennas. The signal is reconstructed at the receiver end. Due to the spatial multiplexing, there is a higher signal-to-noise ratio and a higher data throughput.

Accelerated guard interval

The guard interval prevents different transmissions being mixed together. In telecommunications, this mixing is also known as intersymbol interference (ISI). When the send time has elapsed, a send pause (guard interval) must be kept to before the next transmission begins.

The guard interval of IEEE 802.11a /b/g is 800 ns. IEEE 802.11n/ac can use the reduced guard interval of 400 ns. You specify the guard interval on the WBM page "AP 802.11n/ac".

Frame aggregation

With IEEE 802.11n/ac, it is possible to bundle together individual frames to form one larger frame, a process referred to as frame aggregation. There are two types of frame aggregation:

- Aggregated MAC Service Data Unit (A-MSDU)

Multiple MSDU frames with the same destination address are bundled and sent as one A-MSDU. This reduces the network load. Due to their shorter maximum length, A-MSDUs are mainly suitable for bundling several shorter frames.

- Aggregated MAC Protocol Data Unit (A-MPDU)

Multiple MPDU frames with the same destination address are bundled and sent as one large A-MPDU. This allows the total throughput to be increased.

The SCALANCE W devices support both types of frame aggregation. You make the settings on the WBM page "AP 802.11n/ac".

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.

1.5.6 IEEE 802.11r

During roaming, the WLAN client roams from one access point to the next. A delay time of several 100 ms can come about at the connection transition.

The following steps can be executed during this time:

- Client searches for a new access point (scanning)
- Logon at a new access point (authentication and association)
- Allow a data connection via the new access point

Shorter delay times are required for time-critical applications, for example, Voice over IP. The standard IEEE 802.11r contains amendments which optimize roaming and therefore is also referred to as Fast BSS Transition (FT).

With FT, the WLAN client must not authenticate every time the access point changes. For this purpose, the access points are grouped into a mobility domain. The WLAN client receives the mobility domain ID from the first access point to which it logs on. The log-on information is buffered within the mobility domain. This logon is valid for all members of the mobility domain.

Based on the ID, the WLAN client recognizes whether the access point is a member of the same mobility domain and can therefore log on without delay. Only WLAN clients with IEEE 802.11r support can use the improved roaming or handover functions.

Requirement

- The access points are members of the same mobility domain
- Only possible with WPA2 encryption (WPA2-PSK and WPA2 RADIUS)

1.5.7 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 the next number of this series and is 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.

1.5.8 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.

1.5.9 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.

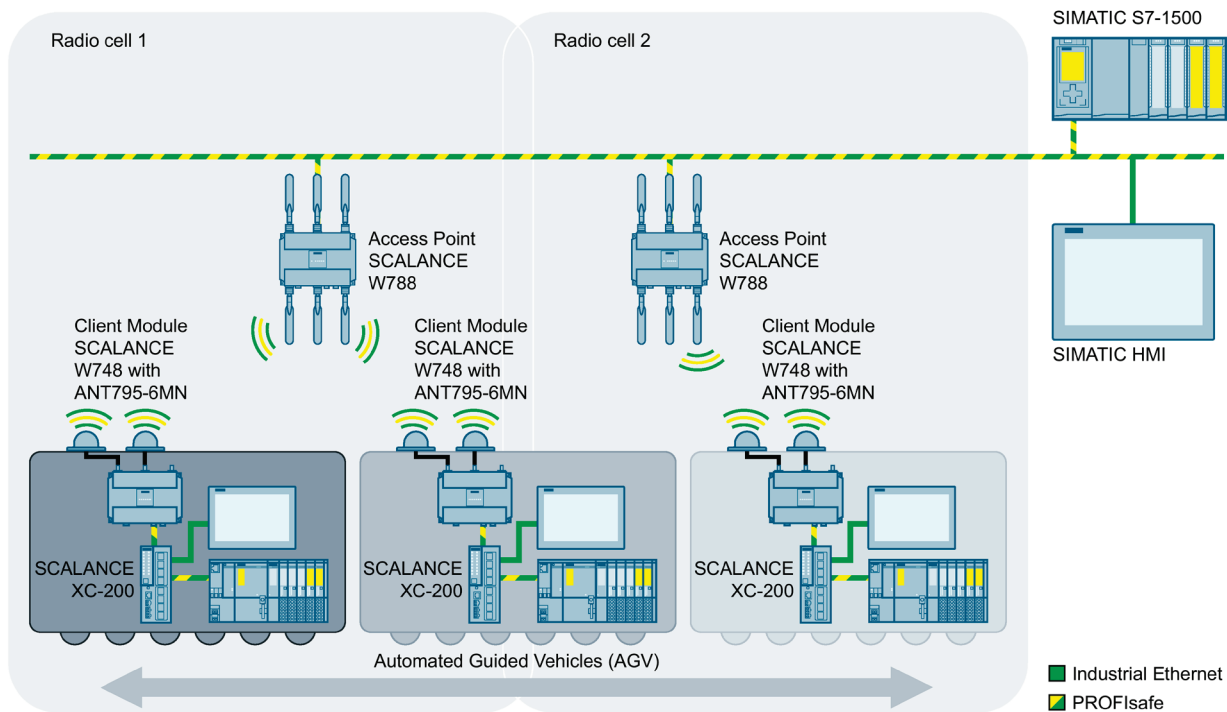


Figure 1-3 Simple WLAN structure with two access points/wireless cells, RCoax cable and IWLAN/PB Link PN IO gateway

Here, access points take over the role of switches. End nodes are connected to the network by turning on "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.

1.5.10 Network structures

1.5.10.1 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.

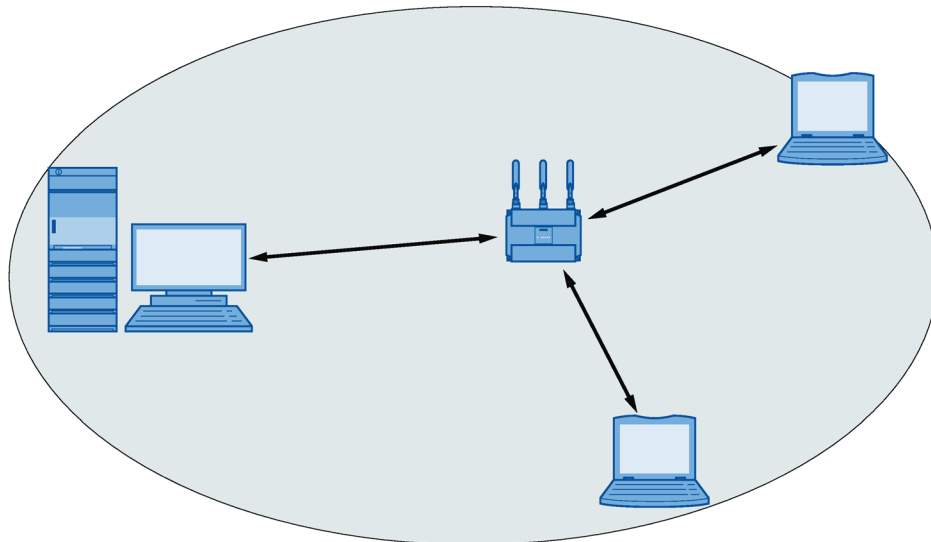
In the simplest case there is a group of clients in the wireless range of the access point. Such a network is also called a standalone network.

If the wireless range of an access point is inadequate either because the range 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.

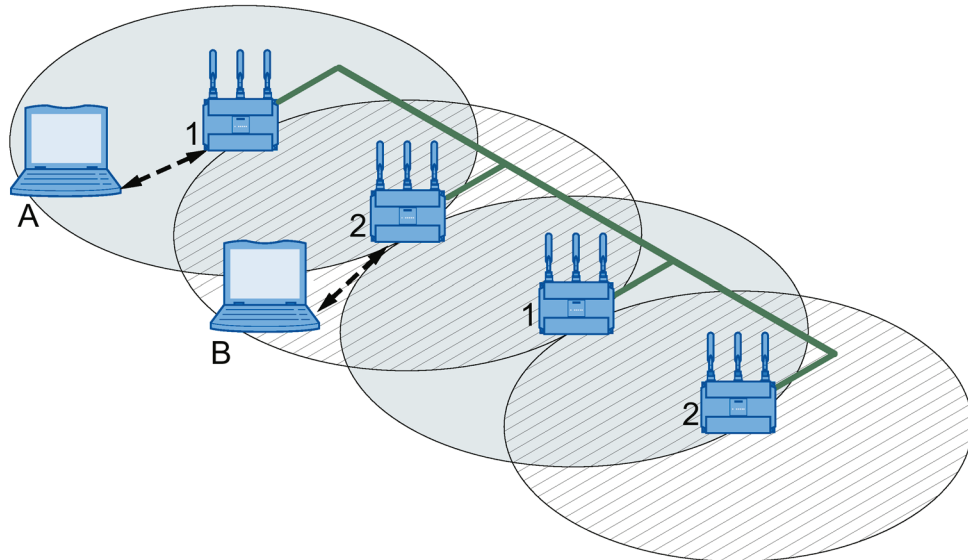


Figure 1-4 Multichannel configuration on channels 1 and 7 with four SCALANCE W access points

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.

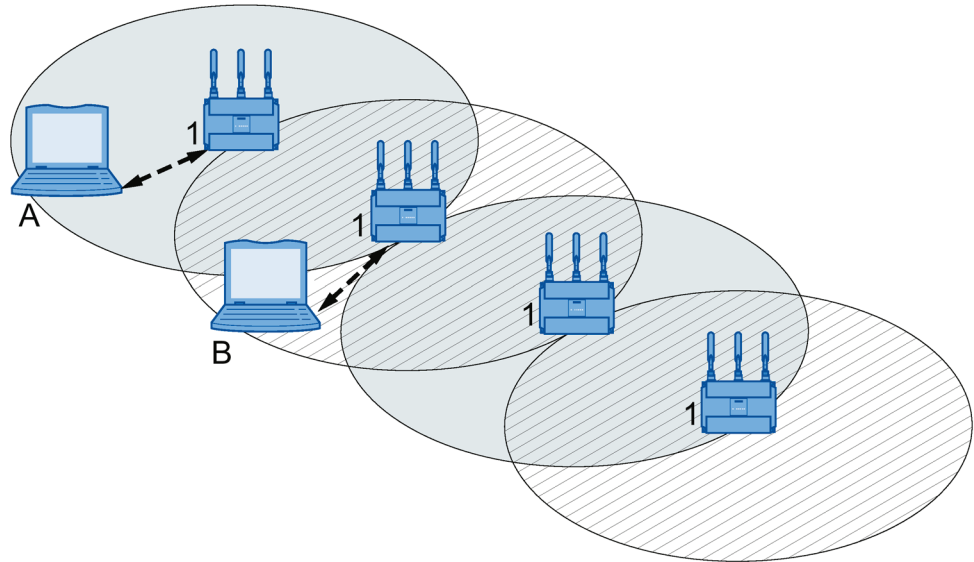
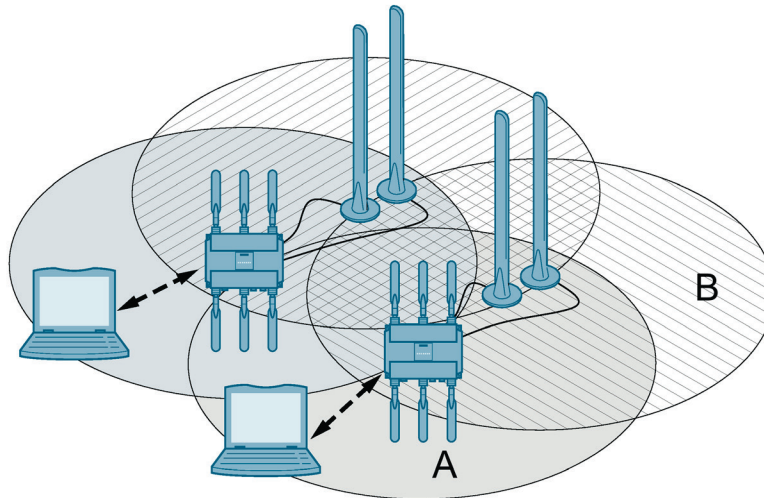


Figure 1-5 Implementation of WDS with four SCALANCE W access points

Redundant Wireless LAN (RWLAN)

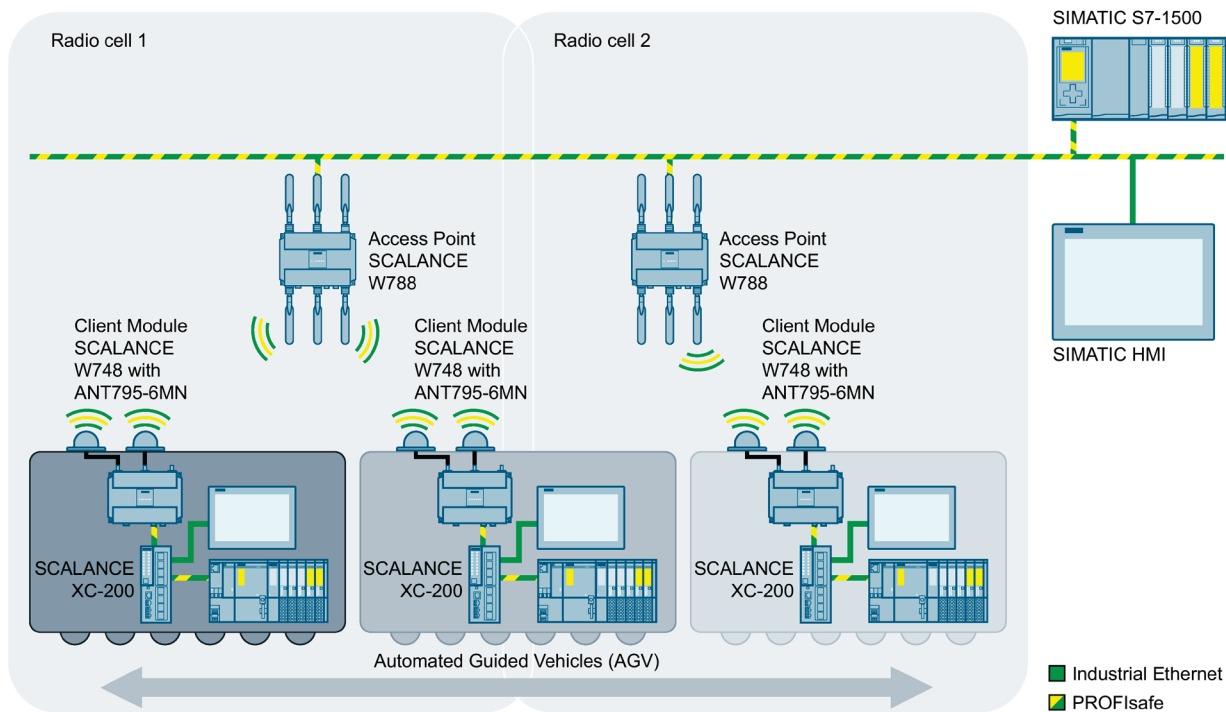
RWLAN allows a redundant, wireless connection between two SCALANCE W access points with at least two WLAN interfaces. This is used to set up a redundant wireless backbone that cannot be implemented as a wired network due to its location but nevertheless has high demands in terms of availability.



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.

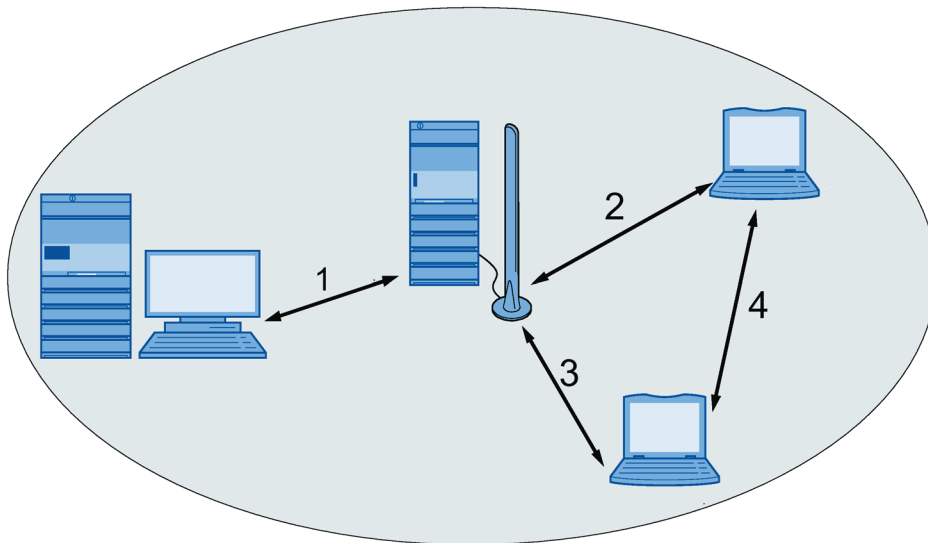
With some devices, the support of the iPCF method is released by the KEY-PLUG "iFeatures" (example: SCALANCE W788-x), the SCALANCE W722-1 RJ45 supports this method already when shipped.

G_IK10_XX_30282

1.5.10.2 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".

1.5.11 Other wireless technologies

Wireless HART

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 a 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.

1.6 Industrial Wireless Control

1.6.1 Mobile wireless standards GSM, UMTS and LTE

Introduction

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.

GSM (2G)

GSM (Global System for Mobile Communication) was the first standard for the digital transmission of languages and short messaging services. Industrial usage is limited to telecontrol and text messaging.

GPRS (2.5G)

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, EDGE (2.75G)

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 (3G)

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. Video surveillance and prompt remote access to machines are relevant applications of this technology in the industrial environment.

LTE (3.9G)

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 and IP-based packet switching allow the transfer of language via TCP/IP ("Voice over IP"). In industrial applications, it facilitates maintenance via smartphone or tablet.

LTE Advanced (4G)

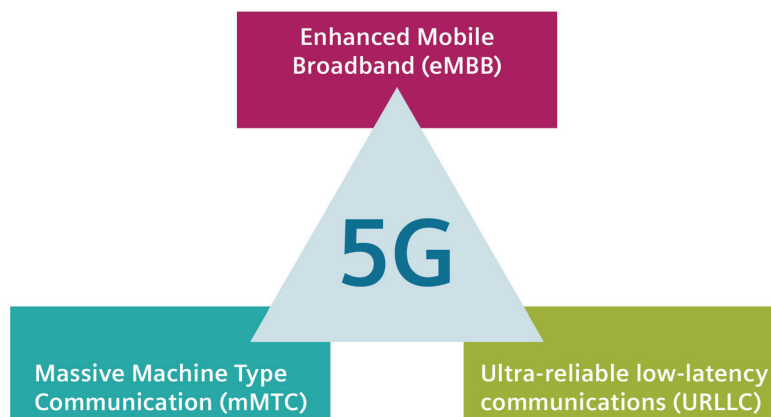
LTE Advanced or also 4G is a protocol extension from LTE. It provides transmission rates up to 1000 Mbps and is downward compatible to LTE. The high data transmission rate allows real-time access. A further advantage is a higher number of users that can be active at the same time.

1.6.2 The mobile wireless standard of the 5th generation

Properties and goals

The new 5G standard offers significant improvements in the following fields compared to the previous standards:

- **Data transmission rates and width of the frequency spectrum**
This property is referred to as Enhanced Mobile Broadband (eMBB).
- **Device density per unit of area**
The scenario Massive Machine-Type Communication (mMTC) is of great importance for industrial applications, both for the Internet of Things and in the process industry.
- **High reliability and low latency**
The designation Ultra-reliable low-latency communications (URLLC) has established itself for this requirement.



The individual 5G functions are being implemented in stages: eMBB is planned for Release 15, mMTC and URLLC for Releases 16 and 17.

Enhanced Mobile Broadband (eMBB)

This 5G function will be available right from the start, because the highest possible data transfer rate is the main demand for public mobile wireless networks. The typical application for this scenario is HD streaming of music and videos. 5G should fulfil the following requirements:

Maximum data rate	20 Gbps (downlink) 10 Gbps (uplink)
Effective data rate across the coverage area	1 Gbps
Total traffic across the coverage area	1000 (Mbps)/m ²
Throughput per wireless bandwidth unit and per wireless cell	3 to 4 x 4G
Sent or received data per energy consumption unit (device or network)	Equal to 4G

Massive Machine-Type Communication (mMTC)

A typical feature of this scenario is the presence of a very high number of units, which do not, however, send or receive continuously. In practice, these are, for example, applications for the Internet. 5G should fulfil the following requirement:

Total number of devices per unit area	10 ⁶ /km ²
---------------------------------------	----------------------------------

Ultra-reliable low-latency communications (URLLC)

The requirement of high reliability and minimum latency times has to be fulfilled for a large number of industrial applications. This applies especially when movements are controlled and coordinated ("Motion Control"): Robot, autonomous logistics, automated guided vehicles (AGV). 5G should fulfil the following requirements:

Maximum delay through the wireless network	1 ms
Maximum speed for rotation and quality of service requirements	500 km/h

Network structures and network configuration

2.1 Integration of a production network in an enterprise network

Introduction

The increasing integration of production networks in enterprise networks requires special measures to ensure network security and system integrity. The communication components used in the industrial environment play an important role in the process. The following section describes which requirements these devices have to fulfil with regard to hardware and functionality.

Example of a configuration

The structure of an industrial network is explained using a bottling plant as an example.

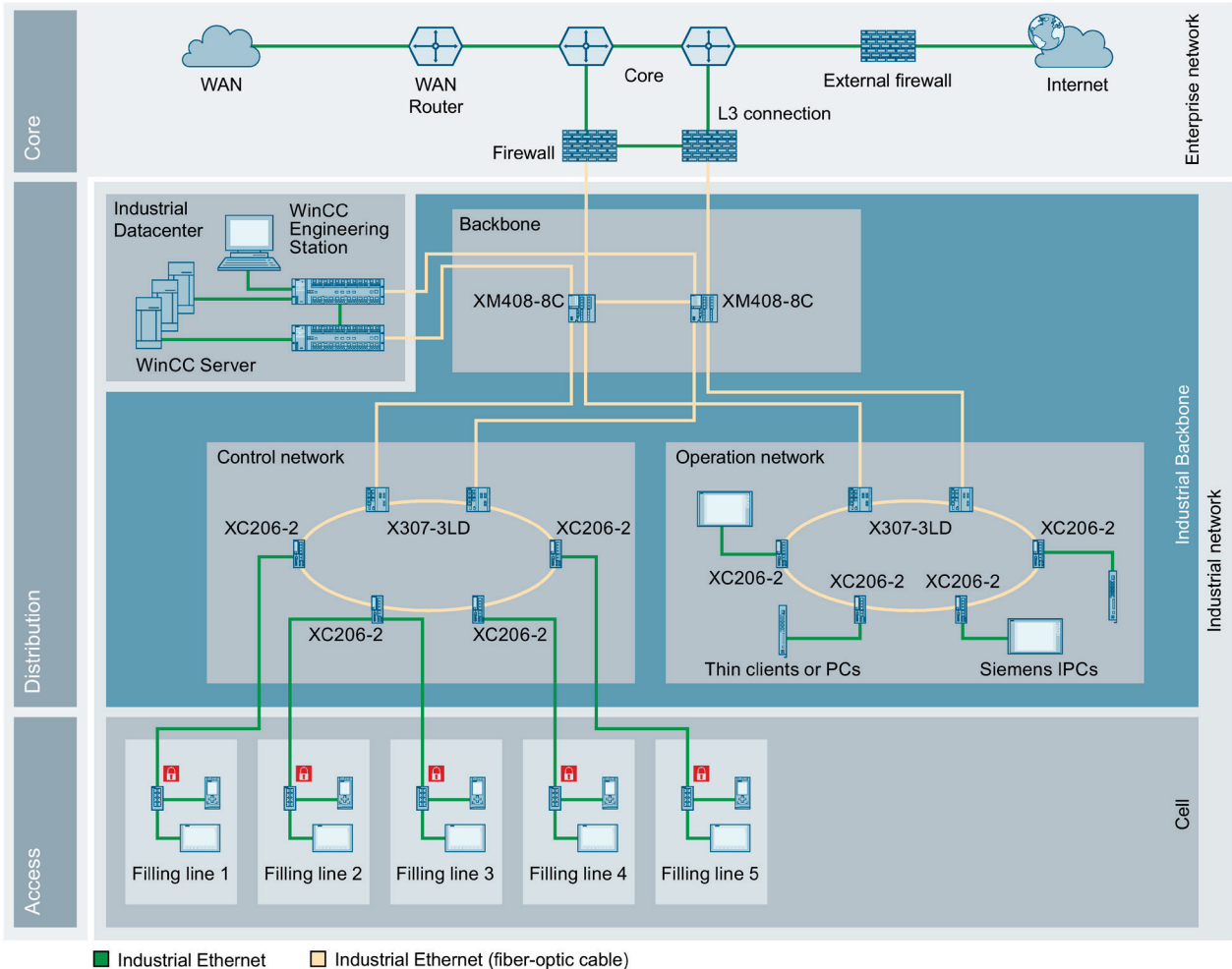


Figure 2-1 Connection of a production network to an enterprise network

- **Enterprise network**

The enterprise network makes available all resources for processing, replacement and storage of the data existing in the company. Both the connections to the Internet and the connections to the industrial network are protected by firewalls.

- **Industrial network**

The industrial network is divided into the backbone level and the cell level. As the name suggests, the cell level consists of the individual automation cells with the corresponding controllers, sensors and actuators.

- **Common data management**

Data are only entered once and are available to the user across the entire factory (on the PLC or computer end, in the visualization system or the distributed I/Os). If the data are required at a different point, the software accesses the shared database. An elaborate consistency check is not required. The "Industrial Datacenter" exists to this purpose. WinCC is typically used here for process visualization.

- **Modular system redundancy R1 in the backbone level**

To achieve the highest possible reliability and availability, all devices and connections are implemented redundantly on the backbone level. The connection to the enterprise network is a redundant Layer 3 coupling via VRRP.

- **Ring redundancy in the control network and in the factory network**

The control and operation network is implemented as a redundant ring topology. Because fiber-optic cables are used, these transmission paths are insensitive to electromagnetic interference.

Requirements for industrial networks

The special demands placed on industrial networks compared to office networks result from the structure of industrial plants and the requirements of manufacturing and process automation that differ fundamentally from those of office applications. To ensure that industrial networks can fulfil their function, the following criteria already have to be taken into account during concept and planning:

- Industrial networks have to fulfil maximum requirements on the availability ("24/7"). Even rare downtimes are not accepted. For this reason, it is often necessary to establish redundant structures. The network components used have to support the corresponding protocols and technologies.
- Depending on the application, the devices must be suitable for extreme ambient conditions, such as shocks and high temperatures. In addition, further requirements for explosion protection, suitability for outdoor conditions or special certifications for various branches may also be necessary.
- The hardware equipment of the devices have to allow flexible adapting to changed boundary conditions. Modular devices of the SCALANCE X series offer a high variability of the port configuration. In addition, some devices can be extended by means of a port extender. In the case of data-intensive applications the devices have to support Gigabit Ethernet or 10 Gigabit Ethernet. Long transmission paths or special ambient conditions require Interfaces for fiber-optic cables. Many SCALANCE devices use the C-PLUG/CLP configuration memory, which simplifies the replacement of devices.
- The spatial extent of the nodes integrated into the network is of great importance. WLAN is often used for mobile units. In addition to common antennas, the RCoax radiating cable is an option for communication along predetermined paths or when radio coverage is not possible or not to a sufficient extent. TeleControl and Teleservice can be used to access distributed stations at remote locations, possibly also via mobile wireless networks with UMTS or LTE.

2.1 Integration of a production network in an enterprise network

- Latency periods during operation can often not be accepted; in some cases, real-time capability is required. Fieldbus systems have been optimized for these special requirements. Office IT components for Ethernet do not fulfil these specific requirements or not to a sufficient extent. The increasing prevalence of Ethernet and IP-based communication in the industrial environment makes devices that are optimized for this application necessary, for example, SCALANCE devices suitable for TSN. In addition, the devices have to be suitable for industry protocols that are often used, such as PROFINET.
- The use of IP-based networks for manufacturing and process automation makes these systems vulnerable because a connection to the Internet or to an office network almost always exists. The damage expected in case of an attack on an automation network is much greater than that of an attack on an office network - up to material damage and danger to persons. To exclude unauthorized accesses, the devices used for this purpose must have fundamental security functions. You can find further information in the section "SCALANCE S Industrial Security Appliance (Page 261)".
- Remote maintenance is a particular problem with regard to network security because in this case external participants have to access devices and plants. Devices of the SCALANCE S and SCALANCE M series allow access for remote maintenance of machines and plants without access to the plant network.
- Because the investment costs are usually higher, industrial plants are used for a notably longer time than office IT components. This means that in the case of industrial IT components, updates for operating systems and application programs have to be available over periods that can be notably longer than ten years.
- The process automation places very specific requirements on components and control engineering. Thanks to their particular suitability for process automation, the devices of the following series fulfil the Siemens classification "PAready":
 - SCALANCE XC-200EEC
 - SCALANCE XF200-2BA
 - SCALANCE XP-200EEC

To fulfil the requirements of the "PAready" classification, a device must support the following technologies or standards:

- Simple S2 system redundancy
- MRP (Media Redundancy Protocol)
- CiR (Configuration in Run)
Configuration in Run is a function that allows plant and configuration changes, such as adding or modifying hardware, to be carried out in run without stopping the plant. The expansion H-CiR is available for applications in which high availability is required.

In addition, the devices of the specified series conform to NAMUR NE 21. These devices are available in a version for extended ambient conditions (conformal coating and an extended temperature range of -40 to +70 °C).

2.2 Network structures

2.2.1 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 cladded glass fibers, such as Polymer Cladded Fiber (PCF), are available.

2.2.2 Linear structure

Linear bus



The linear bus is the simplest network structure. It is characterized by a backbone of the network to which the individual nodes can be connected directly or through individual branches, whereby each branch contains only one node.

- The advantage of the linear bus topology is its simple setup and low hardware investment. It is suitable, for example, for the large-scale interconnection of rigidly coupled machines, such as in a production line.
- 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.

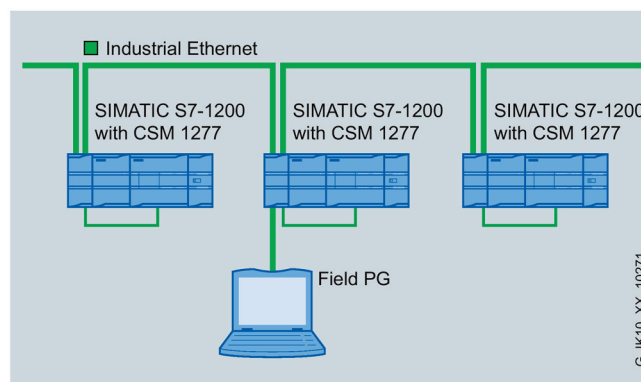


Figure 2-2 Linear network topology with Industrial Ethernet as an example

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

Setup

The line structure can be realized through SCALANCE X switches. Any TP ports can be used to cascade and form a linear bus. The number of SCALANCE X switches that may be cascaded depends on the response times of the applications that are to be operated via this line.

- 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 m
- 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

2.2.3 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.

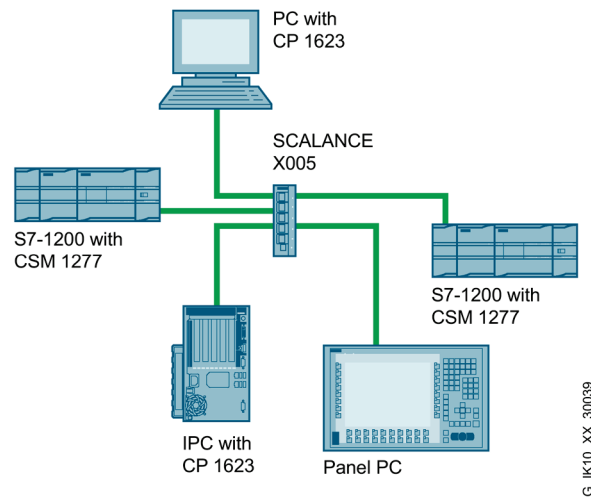


Figure 2-3 Star structure with SCALANCE X005

- 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.

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 of the displayed topology, the SCALANCE X005 can support five 10/100 Mbps cables with RJ45 connectors and no fiber-optic connections.

Typical use cases for star networks are control cabinets, individual machines or manufacturing cells.

Example

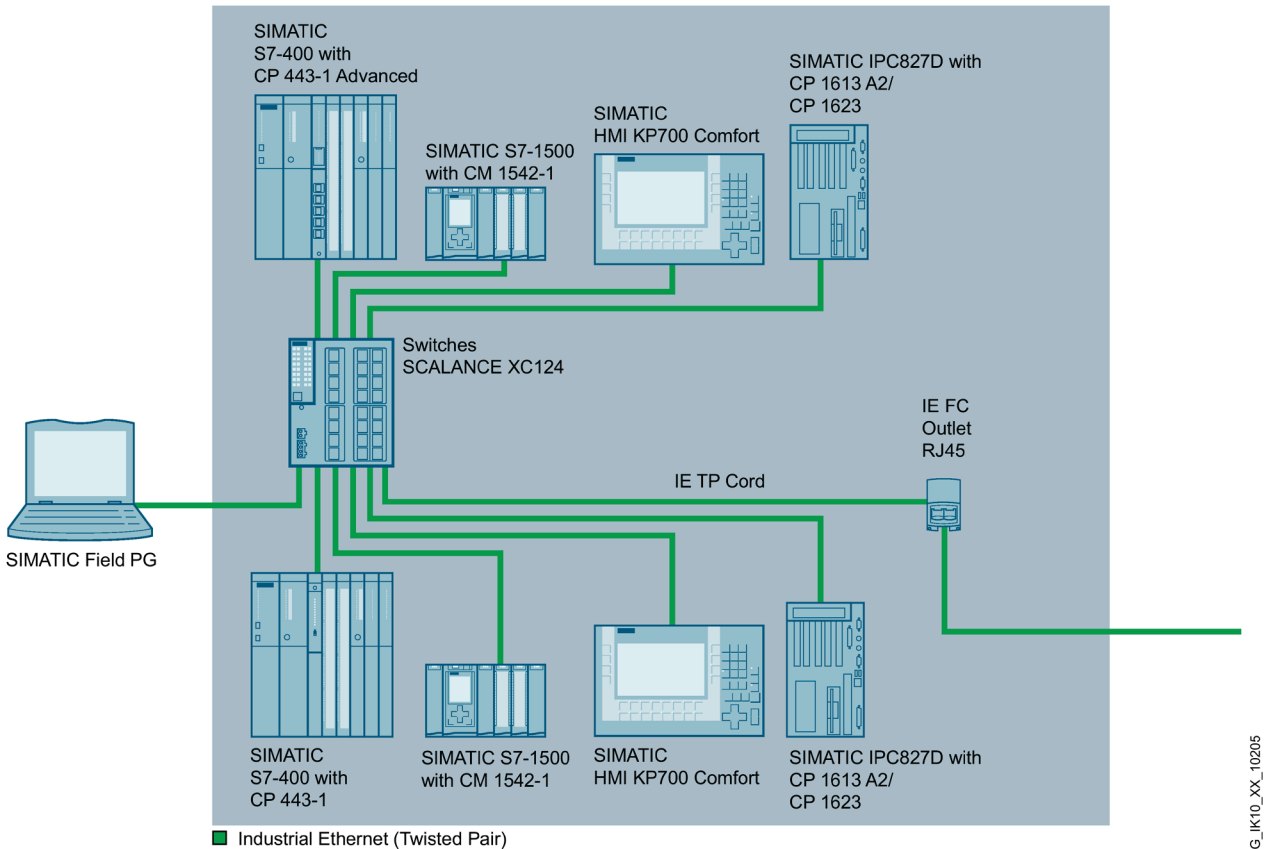


Figure 2-4 Star network structure with SCALANCE XC124

More complex network structures can be set up by using switches with a higher number of ports, in the example above a SCALANCE XC124 device 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 subnetworks makes sense.

See also

SCALANCE X-000 (Page 140)

SCALANCE XC-100 (Page 148)

2.2.4 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 path that is now interrupted and reaches its recipient via this detour. The network does not fall apart into two segments.

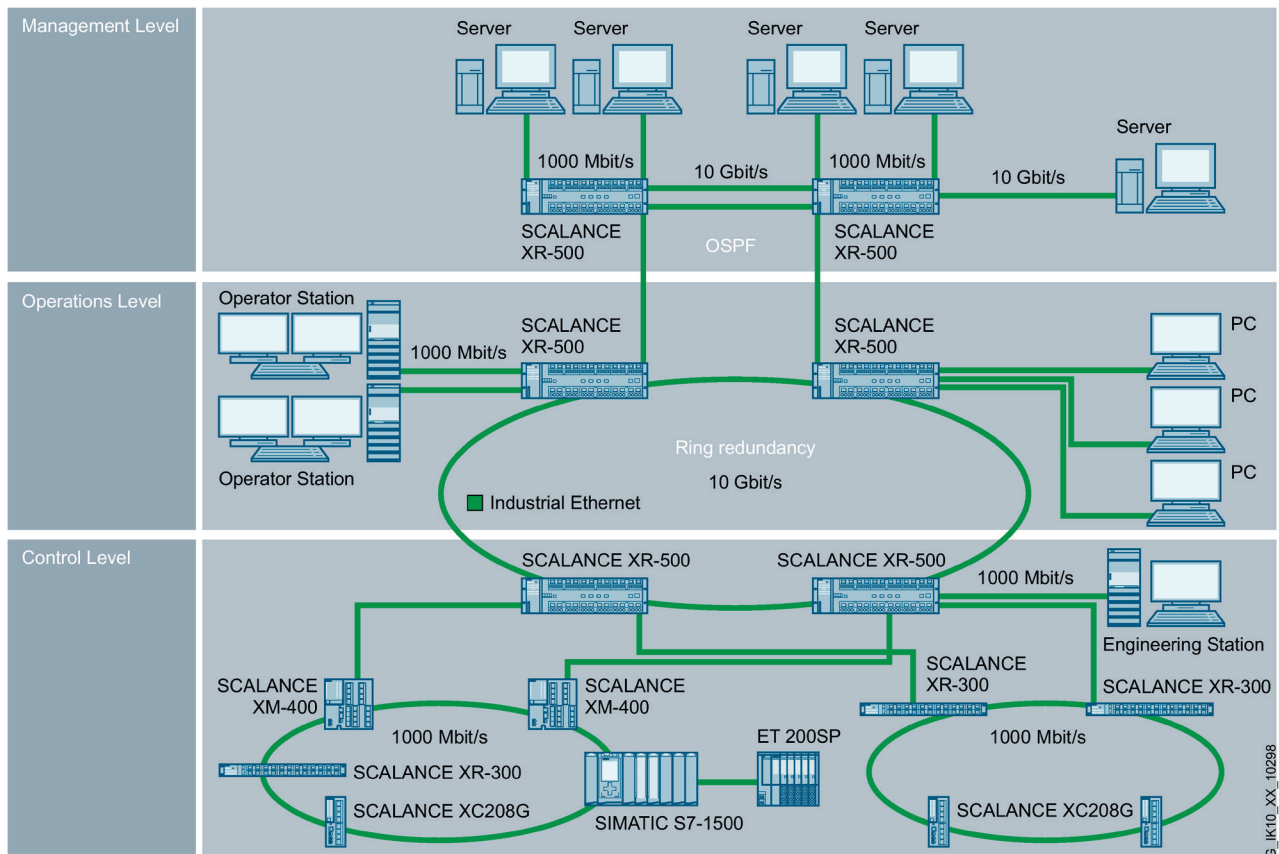


Figure 2-5 Redundant 10 Gbps ring structure and 10 Gbps backbone with SCALANCE XR-500

- The effects of a network component malfunction are thus restricted to the failed component and to the end devices connected to the component. If a ring section is interrupted by a cable break, for example, 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 3 000 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.

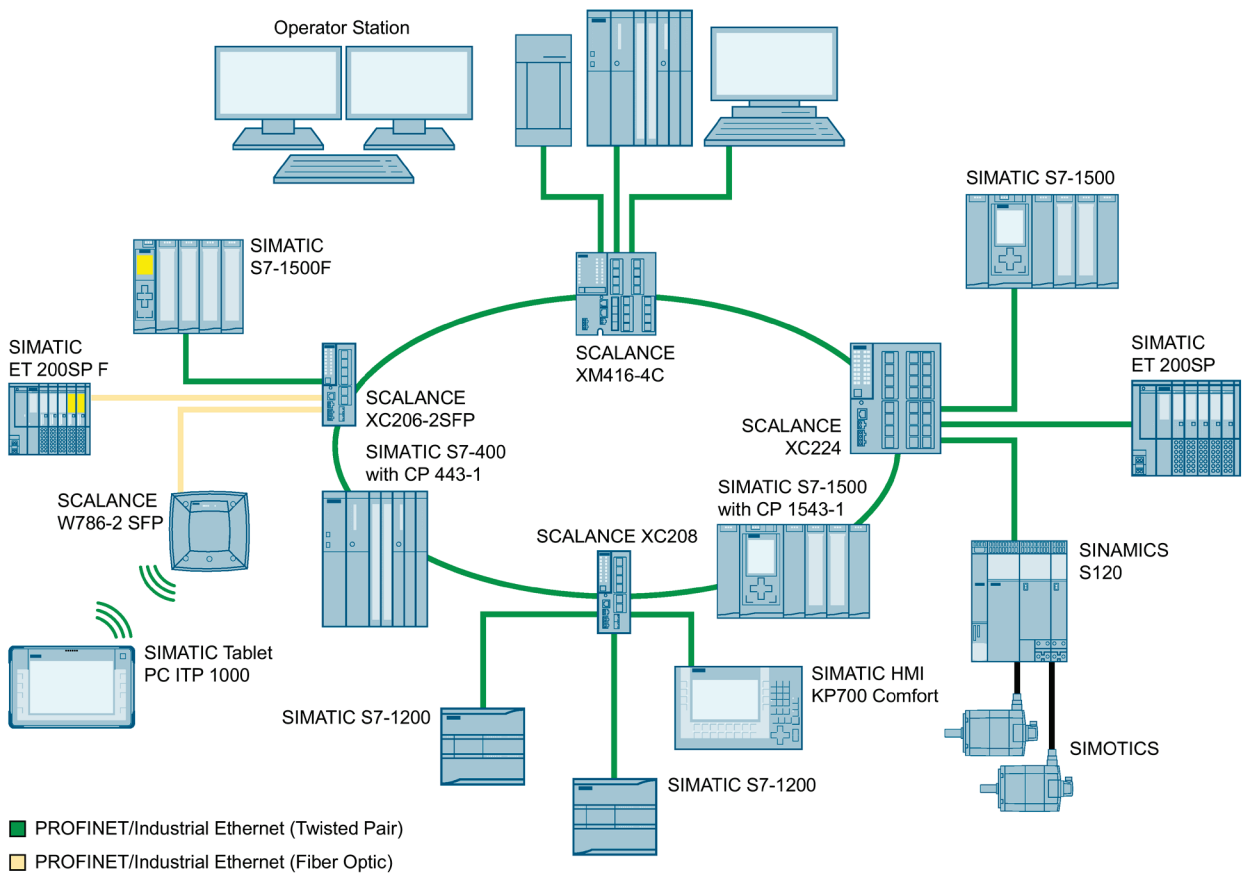


Figure 2-6 SCALANCE X: Redundant setup of an automation network

See also

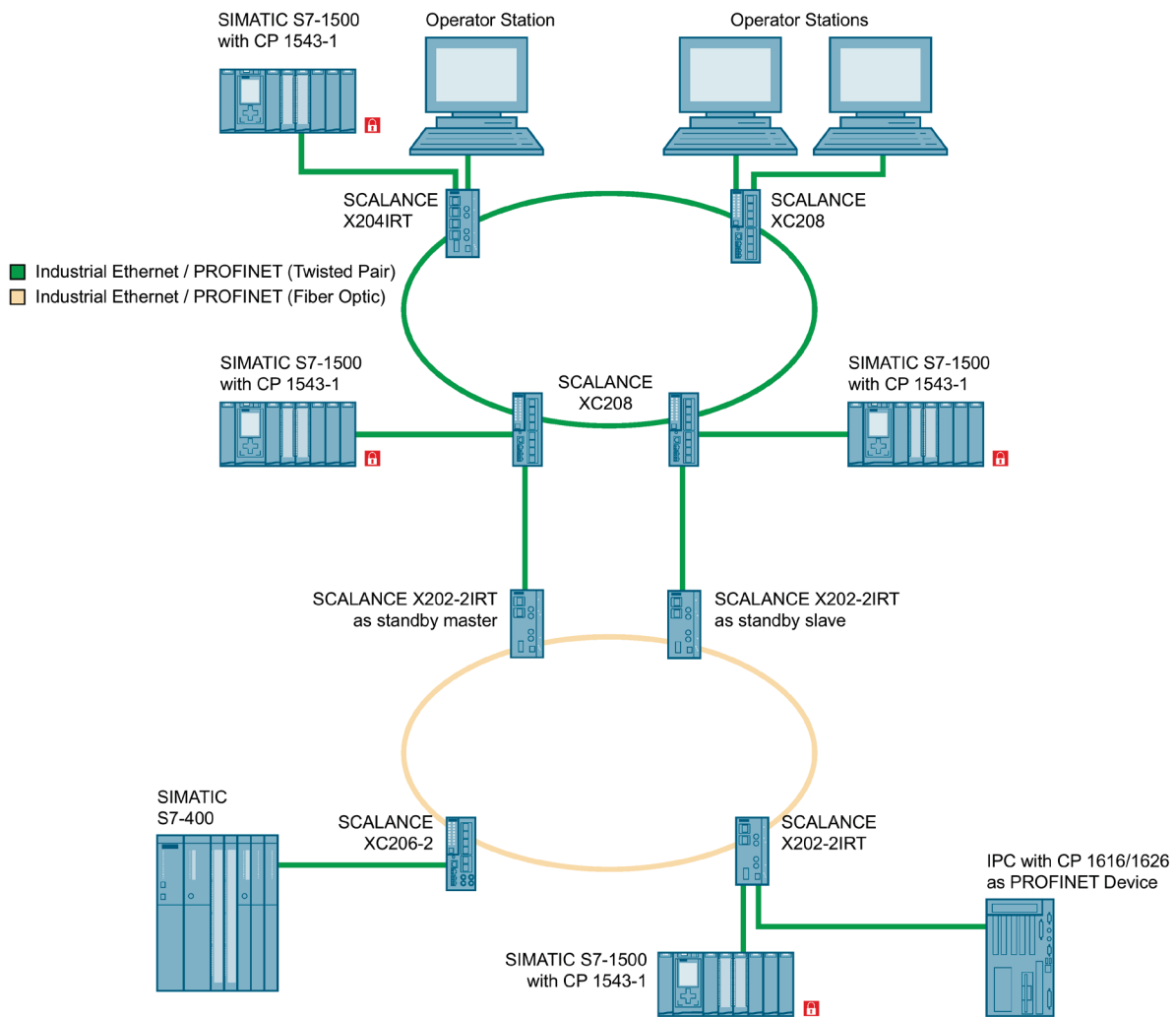
Network topologies (Page 75)

2.2.5 Redundant coupling of network segments with electrical and fiber-optic components

General

SCALANCE X switches support not only ring redundancy within a ring but also redundant coupling of multiple rings or open network segments (linear bus). In the redundant link, two rings are connected together via 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



G_IK10_XX_10173

2.3 Media redundancy

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 becomes the master; the other device becomes the slave). If there are no problems, the link to the other network segment is only active at the master. 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.

2.2.6 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 messages 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 to the data traffic of other nodes any more on 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.

2.3 Media redundancy

2.3.1 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

2.3.2 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.

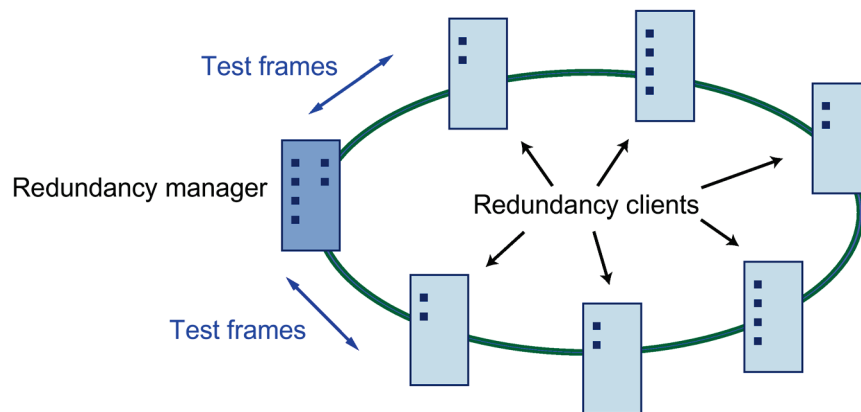


Figure 2-8 Devices in a ring topology with media redundancy

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 around the ring in both directions until they arrive at the other ring port of the redundancy manager.

2.3 Media redundancy

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.

2.3.3 MRP

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

IEC 62439-2:2016 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 200 ms.

Topology

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

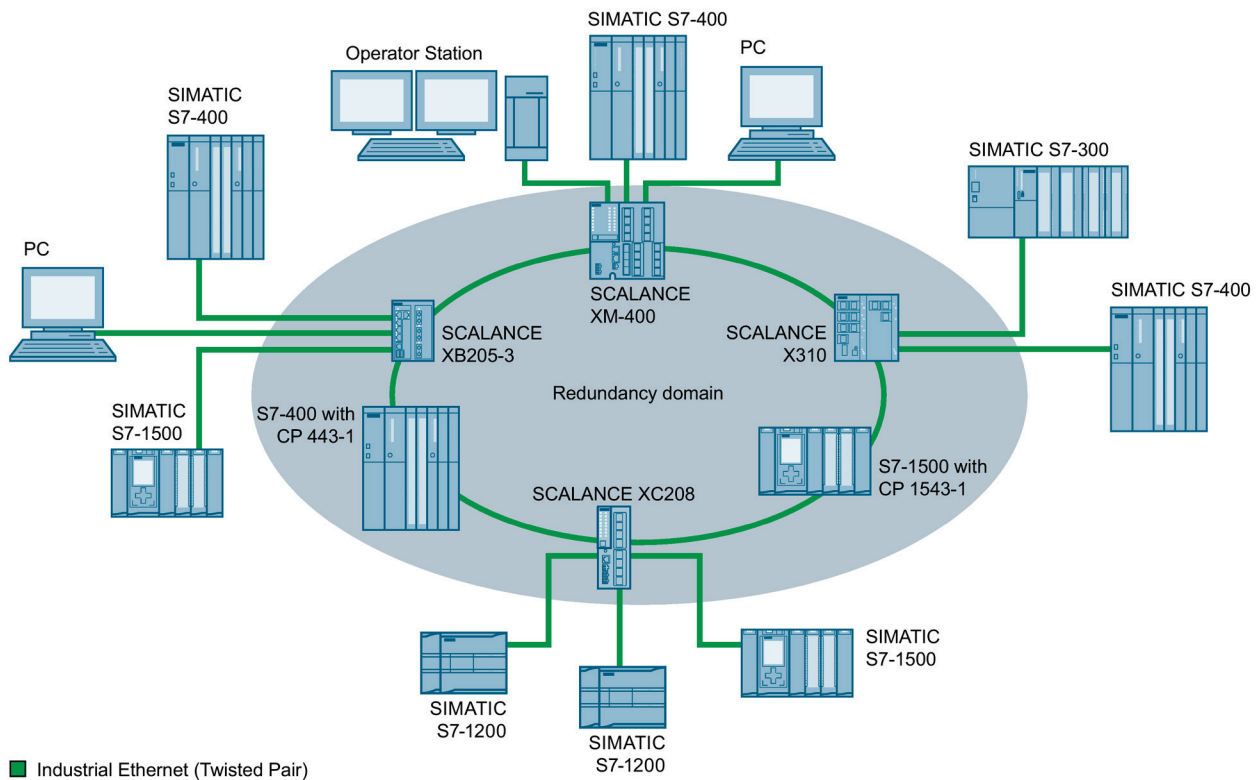


Figure 2-9 Example of a ring topology with the MRP media redundancy protocol

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 capable of MRP.

Requirements

The 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.
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 enabled for all devices in the ring.
- 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.

2.3.4 MRP Interconnection

The MRP Interconnection mode is an extension of MRP and enables redundant linking of two or more MRP rings in networks without real-time capability. Like MRP, MRP Interconnection is specified in the standard IEC 62439-2. MRP Interconnection allows for very fast reconfiguration; the reconfiguration time is typically less than 200 milliseconds.

Topology

The diagram below shows the redundant linking of two MRP rings. In addition, MRP Interconnection also supports additional topologies which are, however, not supported by the current firmware.

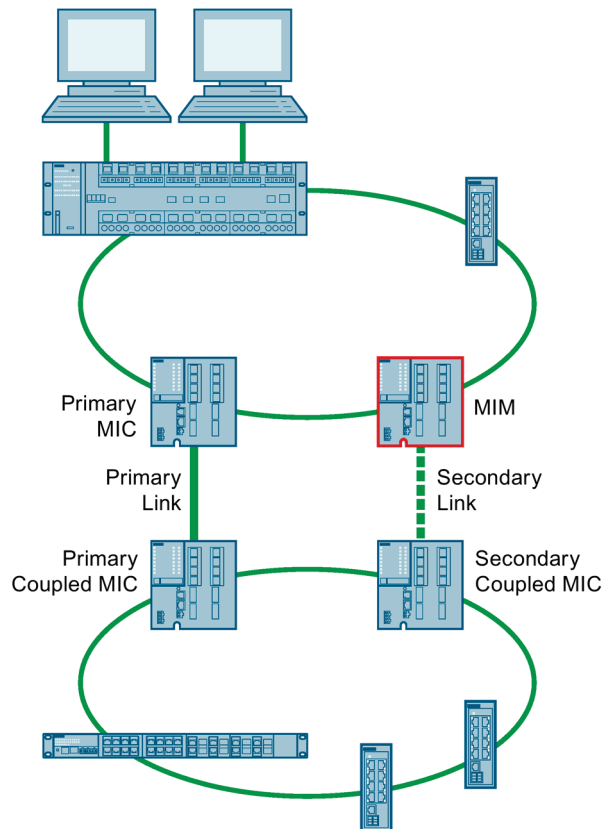


Figure 2-10 Redundant connection of two MRP rings with MRP Interconnection

Operating principle

The requirement for MRP Interconnection is that MRP is used in all rings involved. Four devices are required for the two MRP Interconnection connections:

- One Media Redundancy Interconnection Manager (MIM, shown with a red outline in the diagram)
- Three Media Redundancy Interconnection Clients (Primary MIC, Primary Coupled MIC and Secondary Coupled MIC)

Because each device is part of an MRP ring, each device also takes on one of the roles defined for MRP, i.e. MRC or MRM.

2.3 Media redundancy

Depending on the connection status of the interconnection ports, the MIC sends status messages (Link up or Link down) to the MIM. Interconnection ports are ports that are connected over the primary or secondary connection. This means the MIM is always informed about the connection status between the Primary MIC and the Primary Coupled MIC ("primary connection") as well as its own connection to the Secondary Coupled MIC ("secondary connection"). In regular operation, the data exchange between the two rings is via primary connection and the MIM blocks its interconnection port. If a Link down of the primary connection is signaled to MIM, it switches its interconnection port to the "Forwarding" status, and the data exchange between the two rings is via secondary connection between MIM and Secondary Coupled MIC.

Note

Suitable devices for MRP Interconnection

The Interconnection Manager, the Interconnection Client and all other devices in the rings must support MRP Interconnection. This is the case for the following devices:

- SCALANCE XM-400 as of firmware version V6.2
 - SCALANCE XR-500 as of firmware version V6.2
-

2.3.5 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

2.3.6 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 X-500
 - SCALANCE X-400
 - SCALANCE X-300
 - SCALANCE X-200
- All devices must be interconnected via their ring ports.

2.3.7 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

2.3 Media redundancy

two ports of an interface of the device or via a SCALANCE X-200RNA. 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 with PRP can be maintained 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 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 on LAN A and LAN B are connected correctly. A message 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

2.3.8 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).

2.3.9 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). Through the MAC addresses of the packets passing through, the switches learn the topology of the network by themselves. 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 malfunction 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, in the case of Rapid Spanning Tree, alternatives for many parameters are preconfigured and certain properties of the network structure are 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.

2.3.10 RSTP+

2.3.10.1 Properties and functions of RSTP+

The main application of RSTP+ is the redundant integration of MRP rings into an RSTP network. It is generally possible to manage such a network solely with RSTP. However, in a ring topology, MRP is the more efficient and faster method. The MRP ring redundancy mode is not affected by RSTP+ because both modes work independently of one another.

Another use case is the redundant linking of MRP rings. It is also possible to connect two RSTP networks over one MRP ring with RSTP+. This is not possible without RSTP+ because Spanning Tree is disabled at the ring ports.

Compatibility of devices without RSTP+

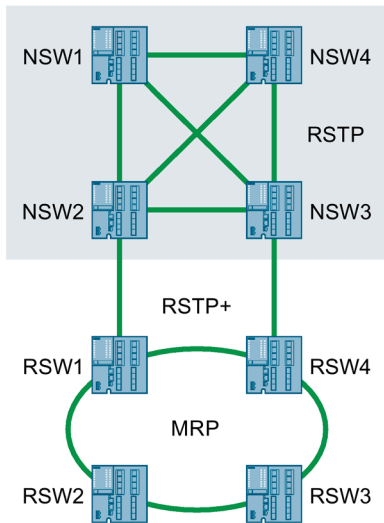
In principle, all devices at the connection points between RSTP network and MRP ring must support the RSTP+ method. All other devices in the MRP ring must forward BPDUs (Bridge Protocol Data Unit).

2.3.10.2 Topology for RSTP+

RSTP network and MRP ring

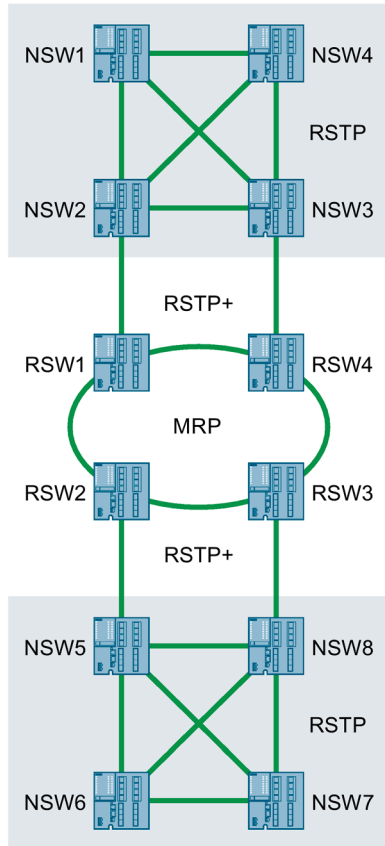
The redundant integration of MRP rings into an RSTP network is not possible without RSTP+ because parallel operation of RSTP and MRP on one port is not permitted. Only the devices of the MRP ring that are connected to the RSTP network must support RSTP+. In the example topology shown, these are the two devices RSW1 and RSW4. The other devices must forward BPDUs.

The identification of the devices in the graphics refers to the respective function of the device. "NSW" is the abbreviation for 'network switch', "RSW" is the abbreviation for 'ring switch'.



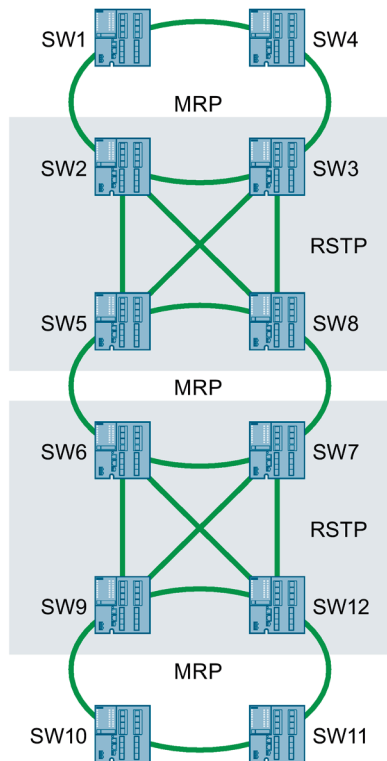
Multiple RSTP network areas and MRP ring

Another use case of RSTP+ is the connection of two or more RSTP network areas over one MRP ring. RSTP+ must be enabled for all devices in the MRP ring that are connected to one of the RSTP networks. In the example shown here, these are the devices RSW1, RSW2, RSW3 and RSW4.



Multiple MRP rings

RSTP+ can also be used to connect multiple MRP rings with each other over RSTP. RSTP+ ensures in this case that MRP still manages the ring redundancy without being affected by RSTP.

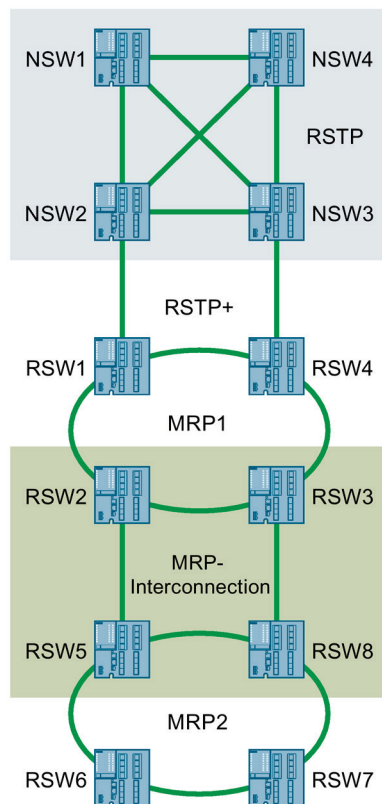


RSTP network and two MRP rings with MRP Interconnection

RSTP+ can also connect an RSTP network to two MRP rings that are linked via MRP Interconnection. In the example topology shown, the two devices RSW1 and RSW4 must support RSTP+. The devices (RSW2, RSW3, RSW5 and RSW8) involved in the connection of the two MRP rings must support MRP Interconnection. In addition, the devices RSW2 and RSW3 must forward BPDUs (Bridge Protocol Data Unit).

The following rules apply to the RSTP+ MRP Interconnection Domain ID in the example shown:

- The same RSTP+ MRP Interconnection Domain ID must be configured for the devices RSW1 and RSW4.
- The same RSTP+ MRP Interconnection Domain ID must be configured for the devices RSW2, RSW3, RSW5 and RSW8.
- The RSTP+ MRP Interconnection Domain ID of the devices RSW1 and RSW4 must differ from the RSTP+ MRP Interconnection Domain ID of the devices RSW2, RSW3, RSW5 and RSW8.



2.3.11 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.

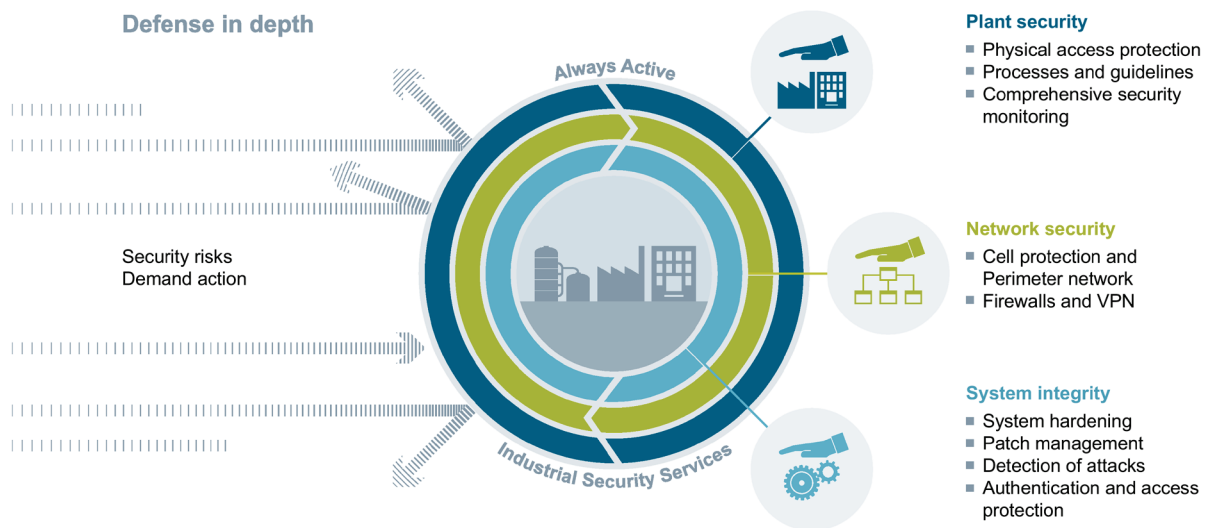
To control and monitor, the Link Aggregation Control Layer (LACL) and the Link Aggregation Control Protocol (LACP) are used.

2.4 Network security

2.4.1 The Industrial Security concept of Siemens

Achieving information security as a complex task

Using the advantages that come along with digitalization has become indispensable for industrial companies. Trends such as cloud-based technologies or the increased usage of Ethernet-based protocols down to the field level offer significant competitive advantages, but also the risk of being subject to cyber attacks. Industrial plants must therefore be thoroughly protected on different levels by means of suitable measures.



IEC 62443

The standard series IEC 62443 ("Industrial communication networks - IT security for networks and systems") is the decisive standard for IT security in the industry and addresses all stakeholders in the life cycle of an automation environment in the various sections. Requirements placed on plant operators or system integrators are also a part of this standards series as well as specific component requirements or principles in the development of automation products ("Security by Design"). The IEC 62443 defines four maturity levels as well as four security levels, from SL-1 (accidental manipulation) to SL-4 (manipulation with specific knowledge and extensive personal and material resources).

Integrated protection of industrial plants

The following procedure can, among other things, be derived from the requirements of statutes and standards:

1. Planning security
 - Evaluation of the existing security levels and application-specific security requirements.
 - Definition of the requirements with regard to standards and legal requirements, such as the law on protecting critical infrastructure, as well as with regard to authentication, user management and access options from external sources (such as remote maintenance).
 - Verification of technical and organizational requirements with regard to a plant-wide security concept.
2. Implementing security
 - Selection of certified and tested products at which security standards were already taken into account during the product development.
 - Inclusion of experts from the field of security and security assessments (for example, Siemens Industrial Security Services).
 - Implementation of the defense in depth concept for the implementation of security-relevant functions on all levels.
3. Always active

Subscribing to Siemens ProductCert Security Advisories to stay informed about product vulnerabilities and security updates.

Defense in Depth

Defense in Depth is a multi-level concept for comprehensive protection of your plant. The concept is based on plant security, network security and system integrity and is based on the recommendations of IEC 62443 - the leading standard for security in industrial automation. The objective is to achieve the highest possible protection at justifiable administrative and economical costs. The following enumeration lists some examples of measures:

- **Plant security**
 - Object protection and definition of processes and guidelines
 - Additional protection of sensitive areas. Personalized access authorizations for machines and plants (for example with SIMATIC RF1060R).
 - Physical network access protection by locking unused ports, for example, by an RJ45 port lock.
- **Network security**
 - Monitoring and protection of all interfaces and zone transitions by firewalls, such as connection to the office network and to the Internet, accesses for remote maintenance.
 - Limitation of IT and OT through a DMZ (demilitarized zone) This term is used for a network that is established to ensure secure data exchange and to safeguard access

between two existing networks. The designation "Perimeter network" is also used for such a structure.

- Implementation of a patch management strategy
- Use of special hardware for firewall and VPN (SCALANCE S) to realize a cell protection concept.
- Use of access points with WLAN-specific security functions (for example SCALANCE W with KEY-PLUG W700 Security for Inter AP-Blocking).
- Use of hardware properties for additional protection (for example, key-operated switch at the digital input for controlled setup of a tunnel connection).
- Use of special software for remote access (SINEMA Remote Connect).
- **System integrity**
 - Authentication and authorization
 - Use of network components with a higher resistance against attacks
 - Malware detection and avoidance
 - Protection of PC-based systems. As a rule, virus scanners can also be used in an OT network. However, performance problems can arise during certain usage scenarios. Whitelisting procedures can be used alternatively or additionally in which permissible processes and programs can be specified explicitly.

2.4.2 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 forms the sole access to the local network from the outside, and the complete data traffic that passes through the network boundaries is routed through 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.

This means that web page packets that are sent from an external server to an internal client can only pass the firewall if the internal client has specifically requested these packets beforehand.

Such techniques are, among other things, relevant for preventing "Denial of Service" attacks ("DoS") in which an external attacker sends simultaneous queries from numerous computers to the attacked target computer with the intention of paralyzing it through network traffic congestion. In the case of Stateful Inspection, these illegitimate queries are already intercepted at the boundary of the local network so that the local traffic continues undisturbed by the DoS attack.

"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.

2.4.3 NAT/NAPT

"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 answers are assigned according to the actual addressees with their IP addresses.

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.

In addition, it provides a certain degree of protection against attackers because only a single address, that of the router, is visible to the outside. A "naive" attack will therefore always target the router directly, instead of the local computers behind the router that have to be protected.

"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.

2.4.4 "Virtual Private Networks" (VPNs)

The function of Virtual Private Networks

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

The participants of the VPN have the impression that they are connected directly to each other. They do not notice the intermediate steps that are introduced during transfer via the public network. This is also called "tunneling" through the public network. For example, two subnetworks of a company that lie very far apart can be connected by means of VPNs in such a manner that they can be addressed as a single unit by the users.

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 58)

2.4.5 Cell protection concept

Basics

In the cell protection concept, a plant network is divided into individual protected cells in which all devices can securely communicate with each other to protect the automation systems. 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 against unauthorized access from the remaining enterprise network through a SCALANCE S Industrial Security Appliance or through further components with firewall and VPN functionality.

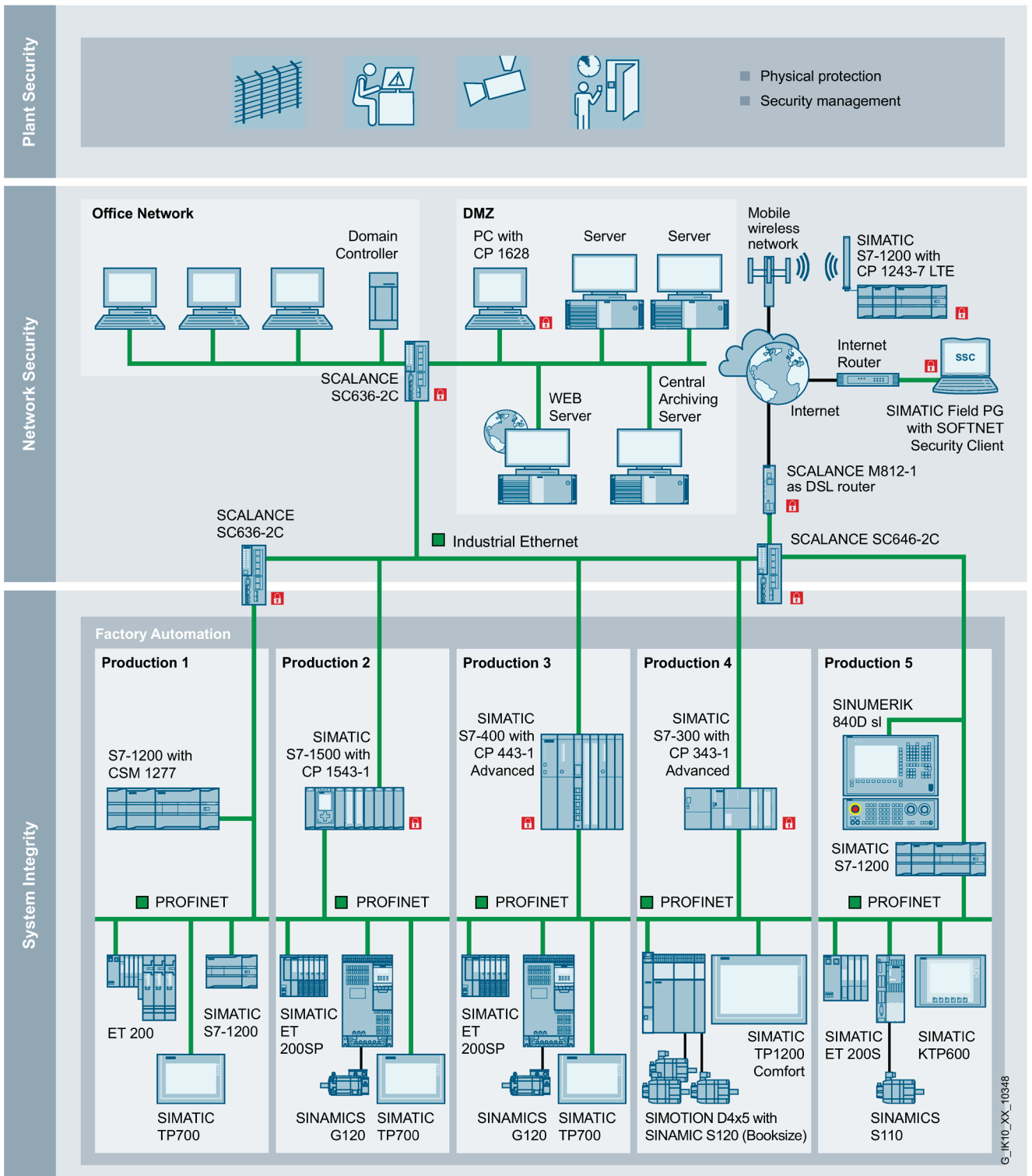


Figure 2-11 Cell protection concept

2.4.6 SIMATIC NET products for network security

SIMATIC NET provides the user with a complete range of high-performance hardware and software components to protect individual devices or an entire network against the following impairments:

- 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 effect on a target system.

If remote access using mobile wireless is part of the infrastructure, it, too, can be protected.

Security functions

The SIMATIC NET products 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 and user-specific firewall rules
- Secure communication with VPN protocols
- 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
- User authentication
- Secure communication protocols such as HTTPS and SSH

SCALANCE S

As a firewall, the Industrial Security Appliances SCALANCE S 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 S615
- SCALANCE SC632-2C
- SCALANCE SC636-2C
- SCALANCE SC642-2C
- SCALANCE SC646-2C

SCALANCE M

The following SCALANCE M industry routers ensure protected remote access via public and private networks and support firewall and VPN functionality:

- SCALANCE M804PB (connection of existing machines and plants via PROFIBUS/MPI)
- SCALANCE M812-1 (ADSL router)
- SCALANCE M816-1 (ADSL router, 4-port switch)
- SCALANCE M826-2 (SHDSL router, 4-port switch)
- SCALANCE M874-2 (2.5G router)
- 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 1243-7
- CP 1243-8
- CP 1543-1
- CP 1542SP-1 IRC
- CP 1543SP-1
- CP 1545-1
- 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.

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).

SINEMA Remote Connect

SINEMA Remote Connect is a server application for convenient and secure maintenance of widely distributed plants and machines. SINEMA Remote Connect uses VPN tunnel connections for protected secure remote access. No special IT know-how is required to operate the SINEMA Remote Client.

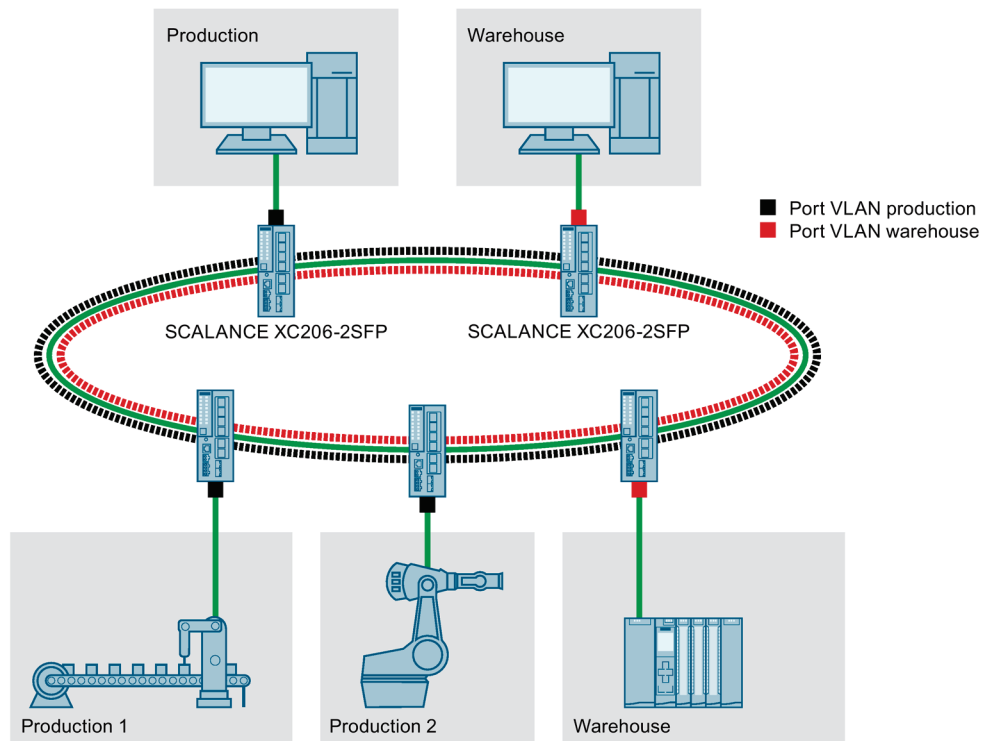
Examples of applications

3.1 Virtual segmentation

Task

Two production areas and an automated warehouse are to use a shared network infrastructure. To reduce the network load and minimize the effects of possible disturbances, only nodes that are assigned to the same area should communicate with each other.

Solution



The two sections of production and storage are separated by virtual segmentation. The SCALANCE XC206-2SFP switches used support port-based VLAN. This makes it possible to assign the nodes of one physical network to different virtual networks. If necessary, data can be exchanged between the individual VLANs by means of Layer 3 switching.

Benefits

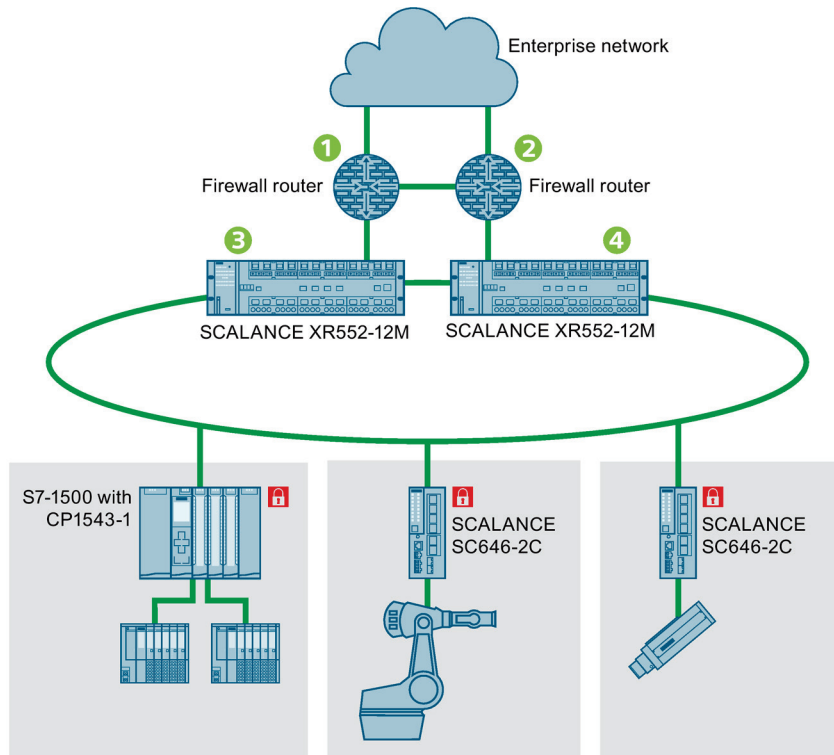
- Lower network loads because broadcast frames are only sent to the nodes of the corresponding VLAN
- The data traffic can be prioritized in accordance with the standard IEEE 802.1Q.
- Segmentation can be a security function when routing between segments is restricted, for example, through firewalls.

3.2 Redundantly coupled networks

Task

In a production company the enterprise network is to be connected reliably with the production network. Faults or the failure of a connecting cable should not have any influence on the data traffic. In addition, the production network is to be protected against unauthorized accesses from the enterprise network.

Solution



To achieve a sufficiently high level of reliability, a redundant Layer 3 coupling is realized. The firewall routers ① and ② are combined with VRRP into a logical router. A virtual IP address and a virtual MAC address are assigned to these two devices. One of the routers is active as a master router. If this device fails, the other router takes over the function of the master

router. Because the virtual addresses are used unchanged, the ARP table must not be updated when the master router is changed.

The two connection paths to the production network between the devices ① and ③ as well as ② and ④ are managed by means of a suitable routing protocol, such as OSPF.

Each automation cell is protected through a security communication processor (for example, SIMATIC CP 1543-1) or an Industrial Security Appliance (for example, SCALANCE SC646-2C).

Benefits

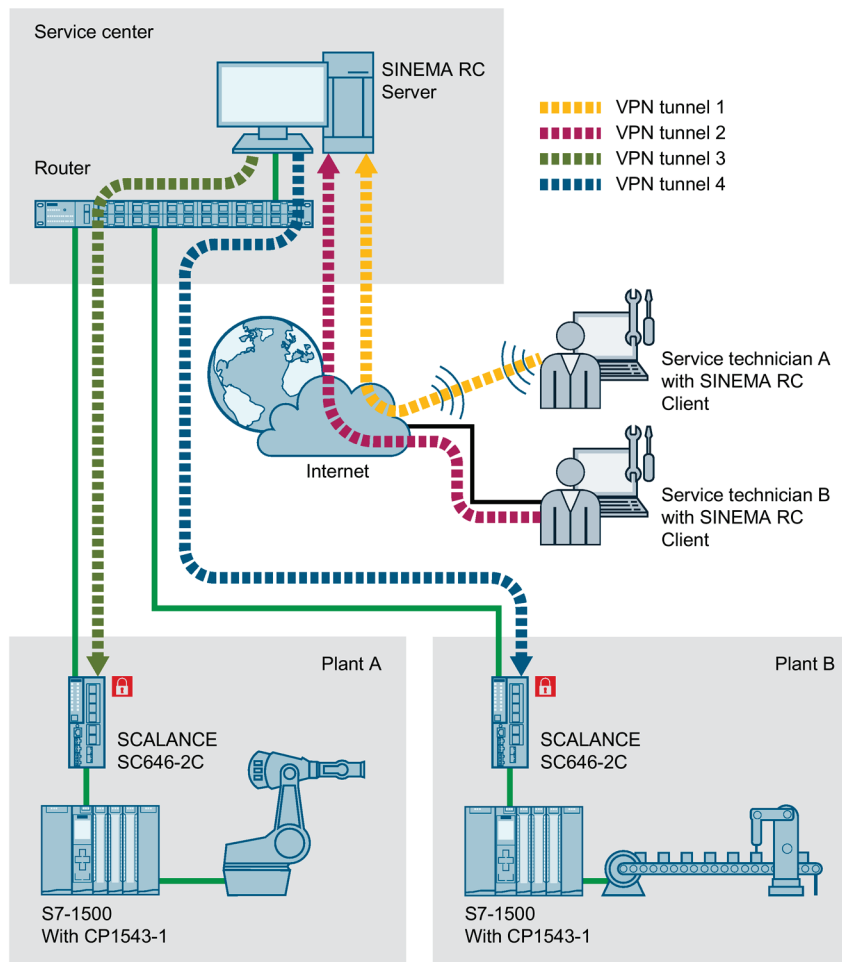
- Extremely high reliability through redundant coupling of the networks
- High data throughput through 10 Gbps technology of the SCALANCE XR552-12M used in the production network
- Separation of networks through a firewall

3.3 Data protection during remote maintenance

Task

Remote access is to be granted to the service technicians of two machine manufacturers for the machines supplied by them. Access should be possible using the wired phone network as well as the mobile wireless network. To ensure security, the company network should not be used for this access.

Solution



SINEMA Remote Connect is used as the management platform for all remote accesses. SINEMA RC Server ensures that only authorized persons have access through multi-factor authentication and manages all VPN connections. The authentication takes place with username and password or PKI smartcard. Each plant is protected against unauthorized access through an Industrial Security Appliance SCALANCE SC646-2C.

Service technician A uses the SINEMA RC Client software to establish VPN tunnel 1 to the SINEMA RC Server via the Internet. Mobile wireless is used for the communication. After successful authentication the SINEMA RC server establishes the VPN Tunnel 3 to Plant A through which the service technician receives access to this plant.

Service technician B uses a wired phone line for the connection to the Internet and to set up VPN tunnel 2 to the SINEMA RC Server. The technician can access plant B using the VPN tunnel 4 established by the SINEMA RC Server.

Benefits

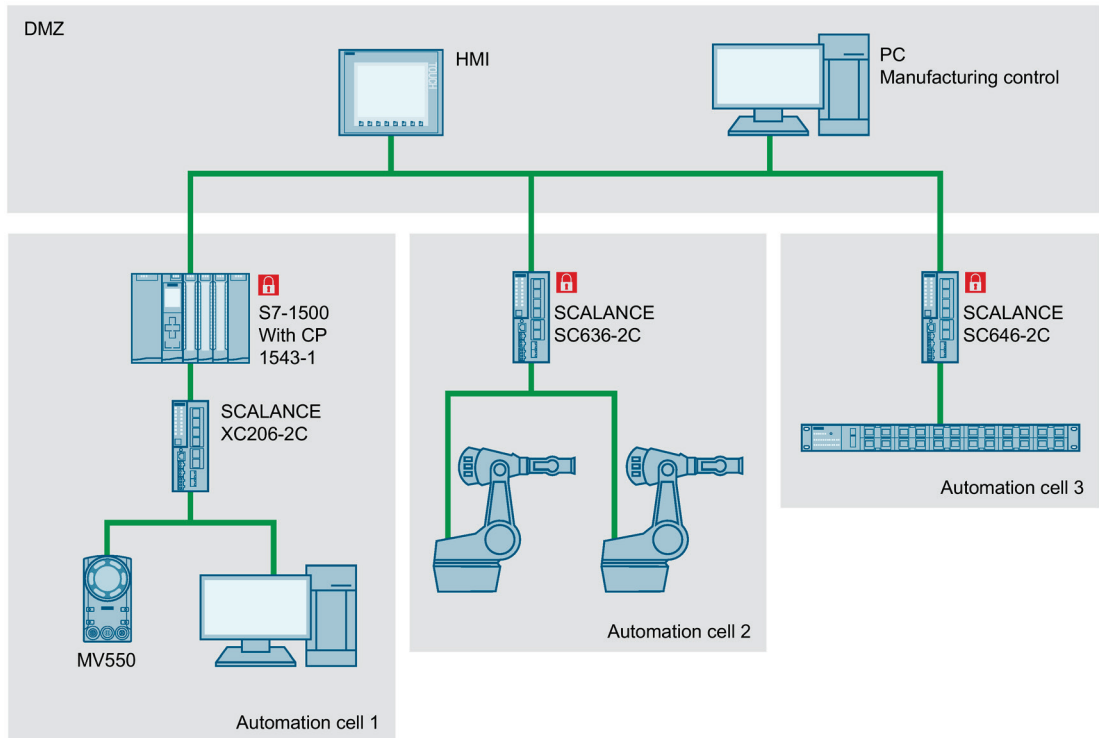
- Central management of all users, access permissions and VPN connections through the SINEMA Remote Connect server
- You only need access to a telephone network (whether landline network or mobile wireless network) for secure and simple connection to the plants.
- Access to the company network is not necessary.
- The service technician only requires the SINEMA RC Client software, which can be operated without any special IT know-how.

3.4 Cell protection concept

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 management 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 carry out since personnel without special training in security will be involved in commissioning and service.

Solution



The devices in each automation cell must communicate with each other unhindered and do not have any security functions. However, each automation cell is connected to the production network via a device with security functions to avoid unauthorized accesses. There are three device categories that can be used for such an application:

- SIMATIC NET communication processors with integrated security functions (for example, SIMATIC CP 1543-1 with firewall and VPN)
- Industrial Security Appliances SCALANCE S with firewall functionality (for example, SCALANCE SC632-2C and SCALANCE SC636-2C)
- Industrial Security Appliances SCALANCE S with firewall functionality and VPN (for example SCALANCE S615, SCALANCE SC642-2C and SCALANCE SC646-2C)

Benefits

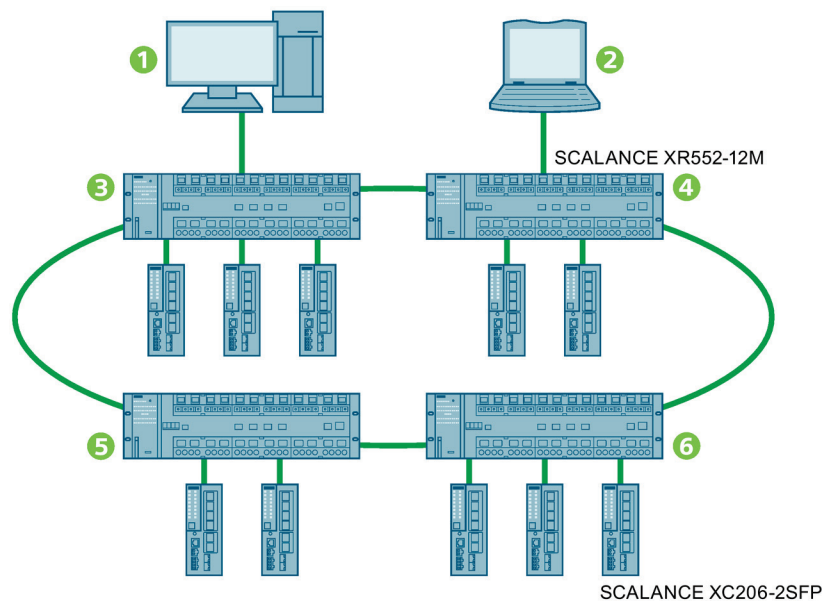
- Effective protection of automation devices from unauthorized access
- Monitoring and logging of accesses from the production network
- Easy configuration of the security functions via Web Based Management

3.5 Network for high data throughput and many nodes

Task

In a production facility, CAE data must be exchanged between many nodes on a large scale. Apart from sufficient band width, comprehensive network management functions are required.

Solution



As a backbone, a redundant ring consisting of four SCALANCE XR552-12M units is set up (position ③ to ⑥). The 10 gigabit ports of these devices are used for a high-performance connection between the switches. A PC (position ①) with the SINEC NMS network management software is connected to one of the backbone computers. SINEC NMS offers various analysis and visualization options as a basis for efficient and optimized operation of the network. If required, the data traffic of a specific port can be analyzed by means of a service programming device (position ②) with port mirroring.

Benefits

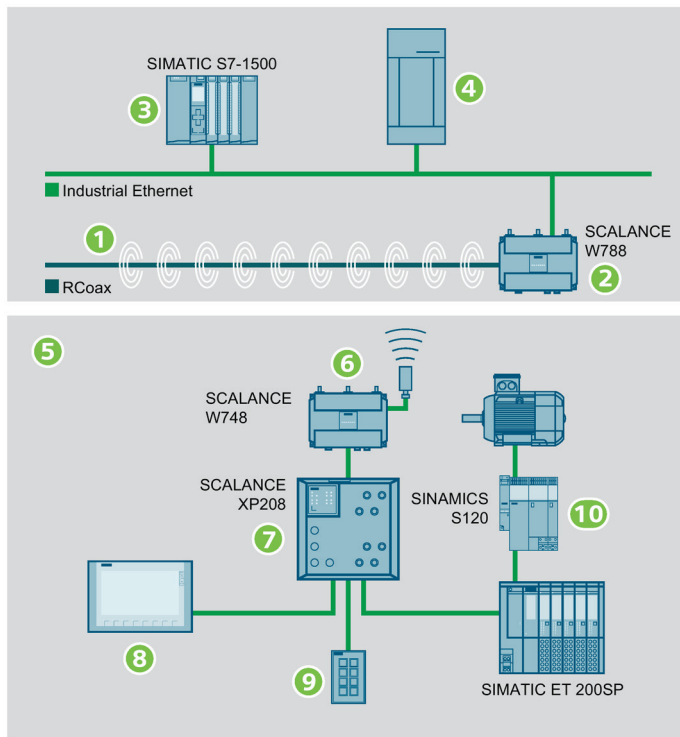
- Sufficient bandwidth through 10 gigabit technology
- Sufficient and efficient network management with SINEC NMS
- Investment protection through modular devices SCALANCE XR552-12M

3.6 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 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.

A SCALANCE W748-1 ⑥ client module is used as the communication partner on the screwdriver stations ⑤.

The data exchange with all components of the mobile station is handled by a SCALANCE XP208 ⑦ switch. Operation of the station takes place via a Panel PC ⑧ and the screwdriver controller ⑨.

The new screwdriver stations are moved by a geared motor connected via the distributed I/O ⑩.

Benefits

- Low investment costs thanks to fewer screwdriver stations.
- Reduction of maintenance costs and downtimes through reliable wireless and therefore wear-free data transmission to mobile communications partners.
- 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, such as 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 W788-1 or W748-1 that are used have a robust metal housing with IP65 degree of protection and are designed especially for industrial use.

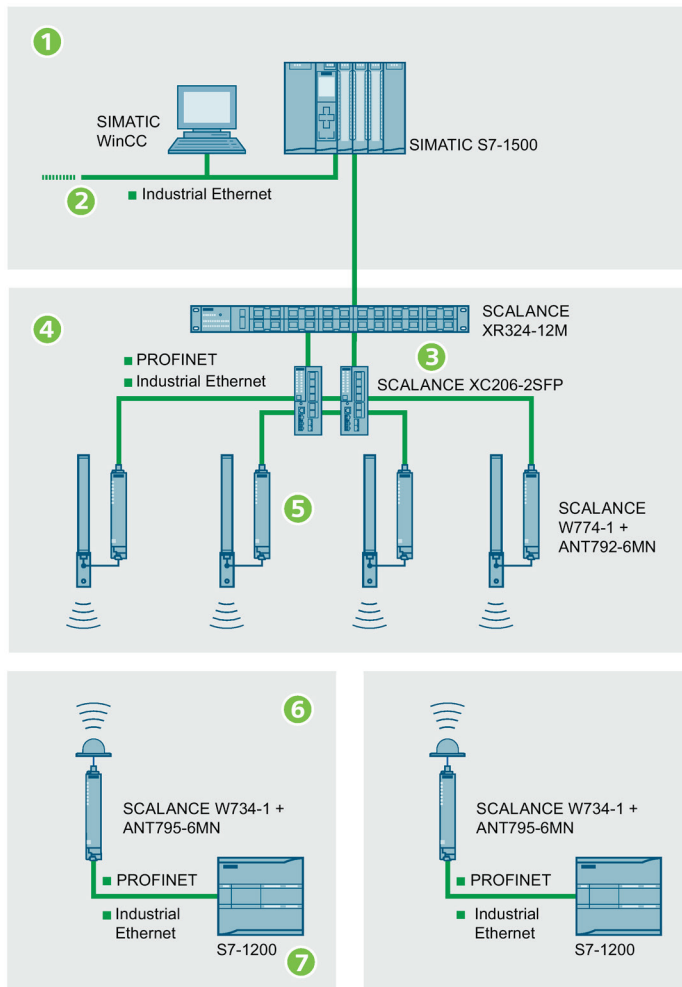
3.7 Controlling material transportation with SCALANCE components

Task

Transportation vehicles in a building need to be controlled using wireless. These vehicles move steel pipes with a weight of several tons. One important aspect is easy scalability if additional vehicles are used. Another requirement is the reliable accessibility of the vehicles in all areas of the hall and high mechanical stability of the devices used on the vehicles in particular with regard to vibration.

Solution

The following graphic shows the topology of the implemented solution and the interfacing to the existing IT structure:



① The plant is controlled via a WinCC system that accepts user input and displays feedback from the individual system components.

② Here, controllers from other operational areas are also connected to allow synchronization of the transportation vehicles with other steps in production.

- ③ The data of the central controller is forwarded to the access points via Industrial Ethernet switches SCALANCE X324-12M and SCALANCE XC206-2SFP.
- 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 S7-1200 controller ⑦.

Benefits

The selected solution has the following advantages for the users:

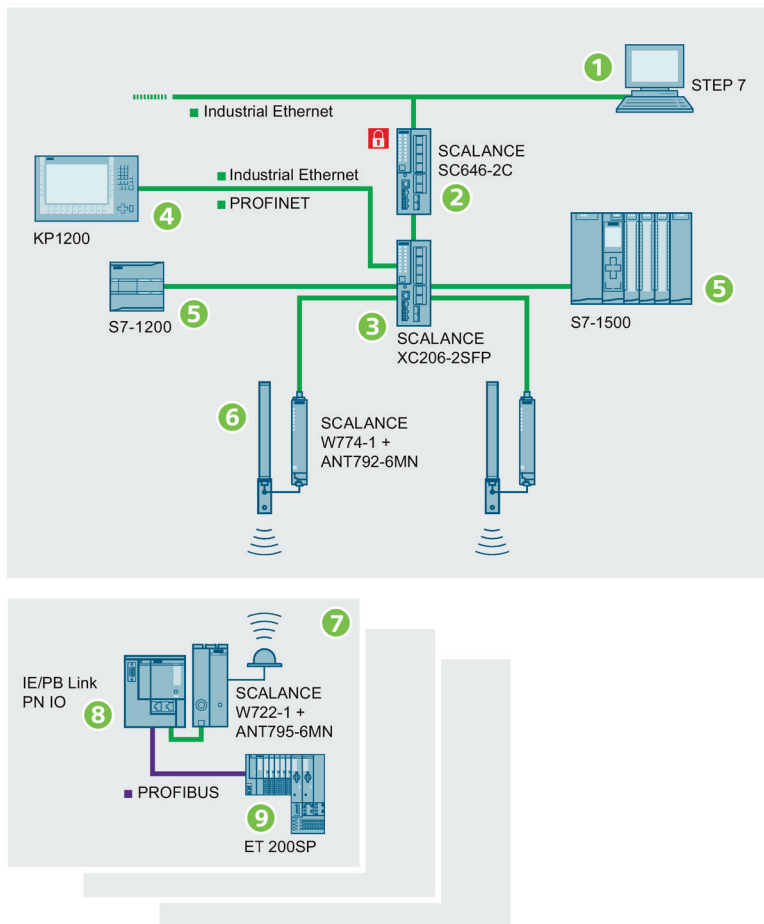
- Wireless LAN suitable for industry that meets all the requirements in terms of reliability and mechanical stability.
- Maximum availability even when changing wireless cells thanks to iPCF
- Easy integration into a WinCC system
- Maintenance-free and problem-free scalability

3.8 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 aims 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.

To protect against unauthorized access, the entire crane system is protected by a SCALANCE SC646-2C ②.

Starting from a SCALANCE XC206-2SFP ③, the individual components form a star topology that includes not only four KP1200 panels as operator control and monitoring stations ④ but also the controllers for the crane carriage ⑤.

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 ⑥ ensure reliable wireless coverage in the area in which the crane carriage moves.

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

Benefits

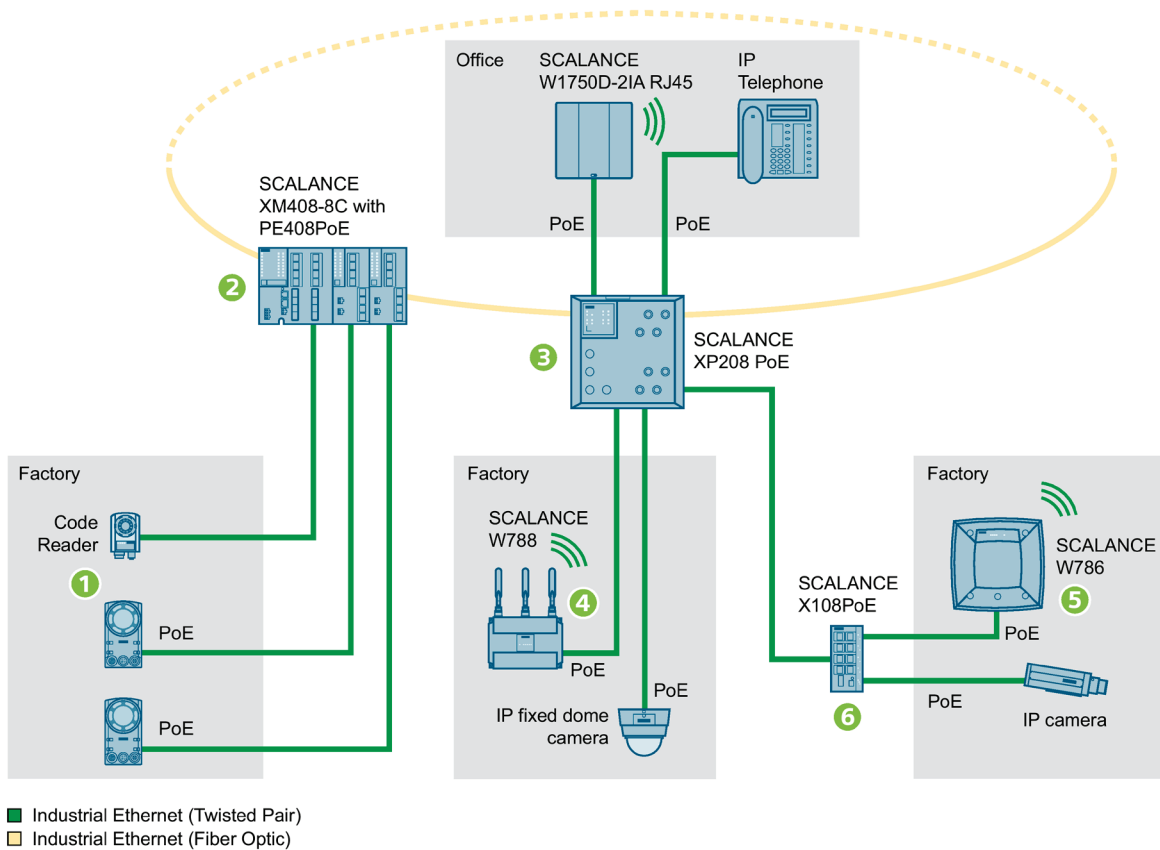
- Reliable and high-speed communication with PROFINET IO and Industrial Wireless LAN with iPCF.
- Protection of investment by using IE/PB Links. The existing PROFIBUS I/O can continue to be used unchanged.
- Through the integration of the absolute value encoders in the distributed ET 200SP, additional cabling is unnecessary
- Absence of maintenance and operational safety thanks to wireless transmission between the stationary system part and the crane carriage.
- Remote access to the system via the factory network is possible, but a SCALANCE SC646-2C protects against unauthorized access.
- If requirements change, the system can easily be expanded or adapted.

3.9 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 into 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_1K10_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 code 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, 16 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 as well as the outside storage area are supplied by a SCALANCE XP208 PoE ③. Both in the production and in the storage area the requirements are the same: An access point has the purpose of making 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 one 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.

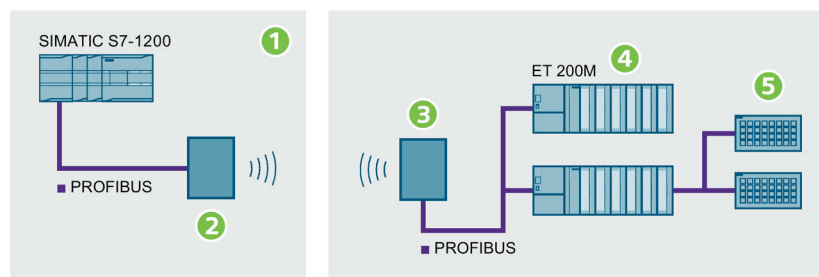
Benefits

- 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 through the high port density of the SCALANCE X devices

3.10 Connecting a PROFIBUS network to a PROFINET installation

Task

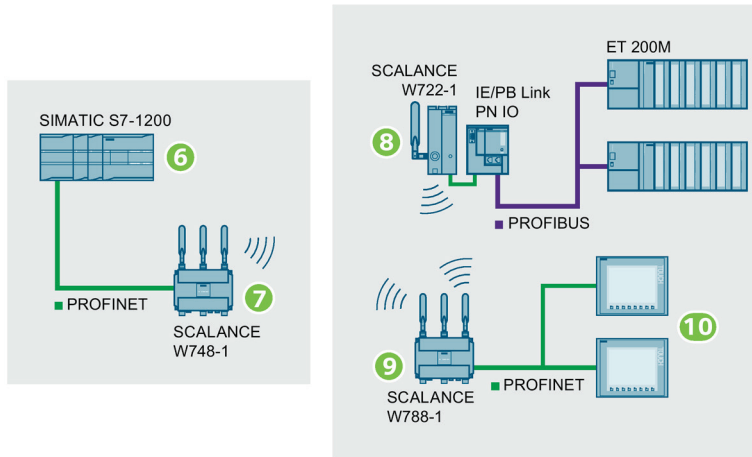
In a brickworks, raw bricks are transported to the drying kiln by a shuttle conveyor ①. The functions of the shuttle conveyor are controlled by an S7-1200 that is equipped with a CM 1243-5 communication module. The movements of the shuttle conveyor are synchronized with the production process in the 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 included a wireless PROFIBUS modem ③ and the ET 200 I/O ④ and operator control stations ⑤ required for production.



This solution alone eliminated 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.



The SIMATIC S7-1200 ⑥ used on the shuttle conveyor has an integrated PROFINET interface. A SCALANCE W748-1 ⑦ client module is connected to this interface for wireless communication. In the stationary part of the system, an IE/PB LINK PN IO ⑧ in conjunction with a SCALANCE W722-1 allows unchanged usage of the ET 200M modules. A SCALANCE W788-1 ⑨ is used as the access point through whose Ethernet interface the operator control stations ⑩ can access the entire system.

Benefits

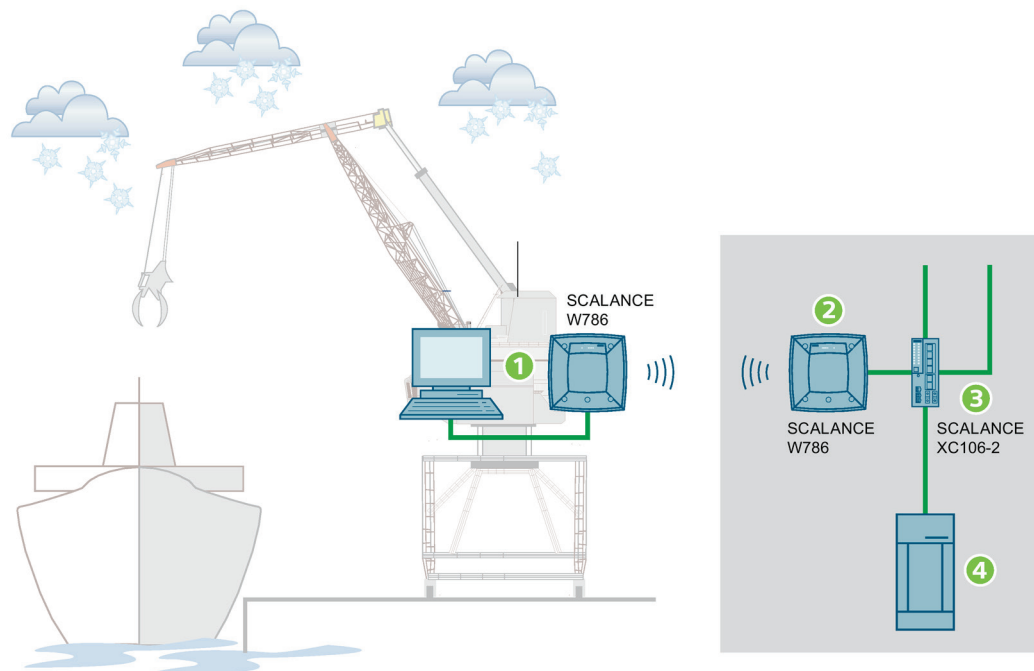
- High data throughput and high reliability in communication with the shuttle conveyor without trailing cables or sliding contacts.
- Transparent network with wireless PROFINET/PROFIBUS gateway
- When necessary, a PC with a WLAN interface can be used for diagnostics and for process visualization.
- Lower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

3.11 Communication components for extreme ambient 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, etc.).

Solution



Communication between the crane and the logistics center takes place 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 XC106-2. 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

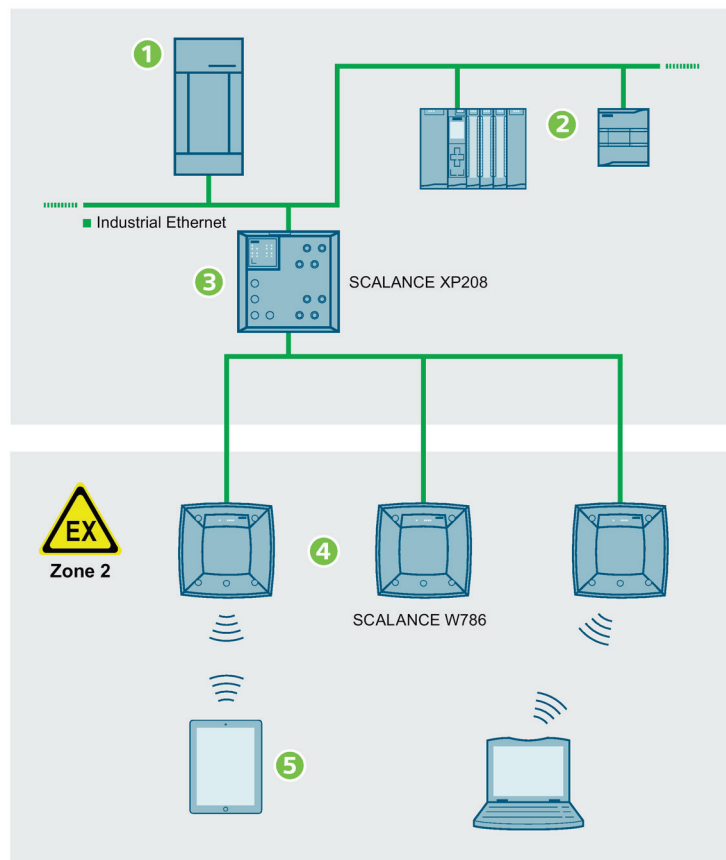
- High availability thanks to maintenance-free components for data transmission
- Unrestricted suitability of the implemented solution for the difficult environmental conditions
- Easy integration into the existing company network
- Access to logistics data regardless of location

3.12 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



All SIMATIC S7-1500 and SIMATIC S7-1200 controllers ② involved in the production process are connected to the SIMATIC PCS 7 server ① via Industrial Ethernet.

A SCALANCE XP208 ③ controls data traffic with the access points.

In the hazardous area, several SCALANCE W786 access points with integrated antennas ④ ensure stable coverage 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.

3.12 Process automation in hazardous areas

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-WW>

With mobile devices ⑤ that are approved for use in hazardous areas, you can retrieve all information of the overall plant at any location.

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.

SCALANCE network components

4.1 Industrial networks with SIMATIC NET

Data communication is the basis for digitalization. Therefore, SIMATIC NET offers all important products and services for industrial communication networks.

Professional Services for Industrial Networks

Consulting during planning and implementation of communication networks. The range of services also includes specialized services, for example, RF field analysis and commissioning as well on-site assistance and support from inventory to maintenance during operation.

You can find further information on the Internet (<https://new.siemens.com/global/en/company/topic-areas/industrial-communication-networks/professional-services.html>).

Services in the area of Industrial Security have become increasingly important. The Industrial Security services offered by Siemens support you during risk analysis, implementation and continuous management of security measures, including an IEC 62443 assessment.

You can find further information on the Internet (<https://www.siemens.com/industrial-security-services>).

Industrial Networks Education

A comprehensive and multilevel training program teaches the skills required for efficient operation of a network (diagnostics, optimization and information security). The training courses offered range from beginner's course through to the expert level and are usually completed with a certification.

You can find further information on the Internet (<https://new.siemens.com/global/en/company/topic-areas/industrial-communication-networks/education.html>).

Solution Partner

To be able to offer matching solutions and services for industry-specific tasks, Siemens works with certified Solution Partners.

You can find further information on the Internet (<https://new.siemens.com/global/en/company/topic-areas/partners/industry.html>).

Worldwide support

Comprehensive services are provided for SIMATIC NET products worldwide. Repair, spare part and maintenance services as well as technical information for all utilization phases of the product are available.

You can find further information on the Internet (<https://support.industry.siemens.com>).

TIA conformity

SIMATIC NET components were developed with regard to the automation concept TIA (Totally Integrated Automation) and tested in a TIA environment.

You can find further information on the Internet (<https://new.siemens.com/global/en/products/automation/topic-areas/tia.html>).

4.2 Product families

The SCALANCE designation stands for SIMATIC NET network components that are tailored to the special requirements of industrial networks. 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 used. 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 industrial wireless local area networks ("IWLANs"). 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 radiating cables (RCoax cables).
- **SCALANCE S** Industrial Security Appliances 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** Industry routers 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

The TIA Selection Tool is available for further information to support you when selecting SCALANCE network components.

TIA Selection Tool (<https://siemens.com/tst>)

4.3 Common properties of all SCALANCE devices

All SCALANCE devices have the following properties. If there are exceptions, these 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 the autonegotiation method 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 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.

The loop detection function detects network loops at the ports monitored by it. Loop Detection is solely an analysis function; detected errors must be eliminated with other measures. Network loops can, for example, be eliminated by changing the topology or by switching off ports.

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.

4.4 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.

The screenshot shows the Siemens WBM interface for a SCALANCE W788-2 RJ45 Access Point. The interface includes a navigation menu on the left with options: Wizards, Information, System, Interfaces, Layer 2, Security, and Features. The main content area displays a photograph of the device and a list of status parameters:

- PNIO Name of Station:
- EtherNet/IP Mode: Off
- System Name: AP_70
- Device Type: SCALANCE W788-2 RJ45
- PNIO AR Status: Offline
- Power Line 1: Up
- Power Line 2: Down
- Power over Ethernet: Down
- PLUG Configuration: ACCEPTED
- PLUG License: ACCEPTED
- Fault Status: No Fault

A Refresh button is located at the bottom left of the status area.

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

Advantages

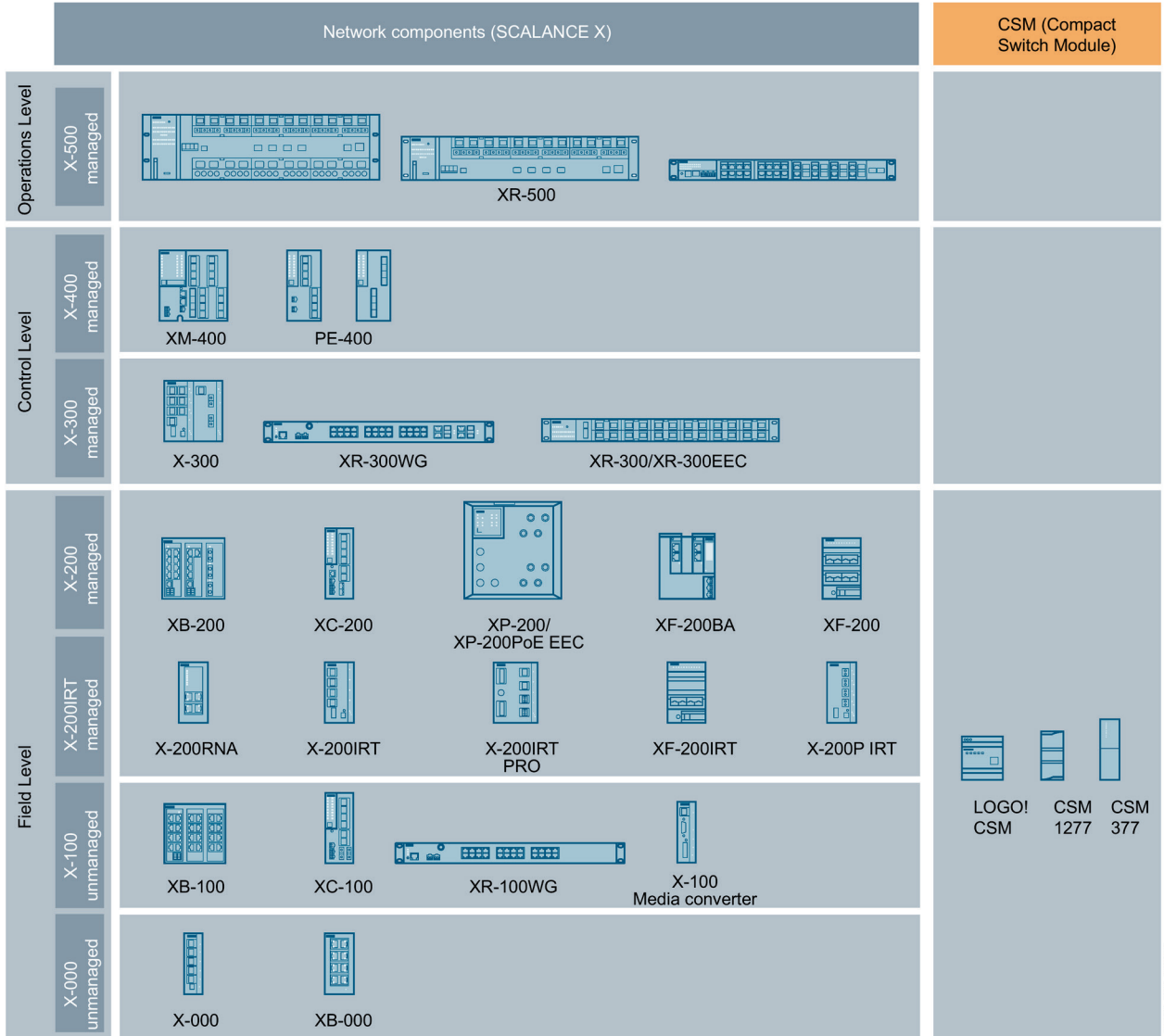
- Access is possible from any PC with a Web browser installed on it and with an Ethernet connection to the target device. With SCALANCE W devices, this connection can also be over a wireless network.
- The installation of special software is not necessary. Operation and navigation through the WBM do not require any special knowledge.
- 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.

4.5 SCALANCE X Industrial Ethernet Switches

4.5.1 Overview of the performance classes

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



G_IK10_XX_10255

Figure 4-2 Overview of IE switches

4.5.2 Type designations

The design and basic properties can be identified based on the following type key.

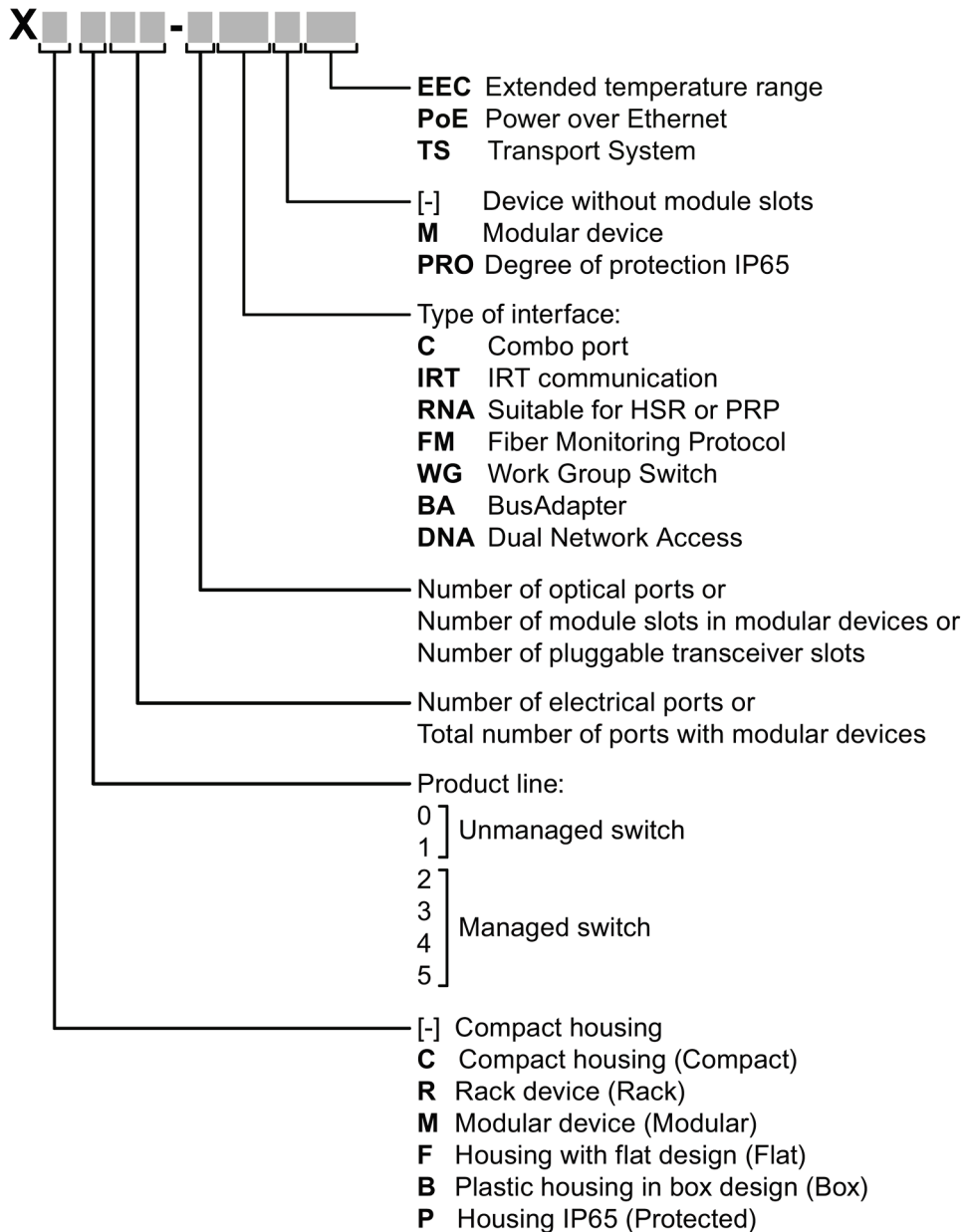


Figure 4-3 Type key SCALANCE X

Basic properties of the SCALANCE X devices

Type of mounting

Apart from a few exceptions, the devices are suitable for wall mounting, DIN rail mounting and S7-300 or S7-1500 standard rail mounting. In individual cases the required type of mounting can be realized by using a mounted adapter.

Devices with the supplement R are either suitable as a desktop device or for installation in a 19" rack.

Management functions

The devices SCALANCE X-000, SCALANCE XB-000, SCALANCE X-100, SCALANCE XB-100 and SCALANCE XC-100 have no management functions. These "unmanaged switches" are therefore cheaper.

The devices SCALANCE X-200, SCALANCE X-300, SCALANCE X-400 and SCALANCE X-500 are equipped with management functions. These devices are also known as "managed switches". The managed switches provide numerous configuration and diagnostics functions for more convenient operation of an Industrial Ethernet network.

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.

Table 4- 2 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.

Table 4- 3 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 1000 Mbps single mode FO cable (up to max. 10 km).
LH	SC port 1000 Mbps single mode FO cable (up to max. 40 km).

Interface	Property
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)

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".

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. For this to work, all devices in an Industrial Ethernet have the same time base. 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.

Modular switches

For applications that require flexibility with regard to interfaces, the use of the modular devices, such as SCALANCE XR324-12M, SCALANCE X308-2M and SCALANCE XR552-12M, is recommended. By making use of media modules, modular switches provide maximum possible variability.

Devices with bus adapters

The switch is equipped with bus adapter interfaces such as SCALANCE XF204-2BA. Through flexible use of different bus adapters, the user can establish electrical and optical line, star and ring structures.

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.

4.5.3 Functions of SCALANCE X devices

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 dropping out of a link at a monitored port.
- The failure of one of the two redundant power supplies.

The connection or disconnection of a communication node at an unmonitored port does not result in 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. This results in several "virtual" networks in the network that exists only once physically. The 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 IEEE 802.1X standard

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 filtered as a result and the load on the network is 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 97)".

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 messages for this address only to ports that have received a registration for this address.

Fast redundancy in the ring

The SCALANCE X-200, X-300, X-400- and X-500 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.

The following redundancy methods are possible:

- MRP in the ring with a maximum reconfiguration time of 200 ms, see section "MRP (Page 84)"
- HSR with a maximum reconfiguration time of 300 ms, see section "HRP (Page 89)"
- MRPD (IE switches with IRT) with 250 μ s reconfiguration time, see section "MRPD (Page 88)"

- Standby redundancy, see section "HRP (Page 89)"
- MRP interconnection, see section "MRP Interconnection (Page 86)"

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 data packets to one recipient whose MAC address is not known to the corresponding switch.

4.5.4 SCALANCE TAP

4.5.4.1 Description



Figure 4-4 SCALANCE TAP104

The unmanaged Industrial Ethernet Test Access Port SCALANCE TAP104 is optimally suitable for frame output in 10/100 Mbps Industrial Ethernet (in particular PROFINET) networks. Output frames can be analyzed for diagnostics of the data communication via standard diagnostics software. The SCALANCE TAP104 can be directly integrated between the connection of two active network nodes. The device is equipped with two electrical RJ45 ports with additional securing collars and two electrical TAP ports. The device has a rugged housing and is designed for installation in control cabinets. It can be installed on the standard DIN rail, SIMATIC S7-300 and S7-1500 standard rail or mounted directly to the wall. The device has LEDs for device diagnostics of the device.

4.5.4.2 Characteristics

SCALANCE TAP104 main features are as follows:

- 2x RJ45 ports with additional securing collar for connecting the IE FC RJ45 Plug 180
- 2x electrical TAP ports
- Device diagnostics at the device via LED: Power and data traffic at TAP port
- Cable length of 100 m between the two active network nodes
- Cable length max. 10 m at TAP ports

4.5.4.3 Interfaces

Device	Twisted pair	
	Network connections 10/100 Mbps	TAP connections
SCALANCE TAP104	2x RJ45	2x RJ45

4.5.4.4 Article numbers

Device	Description	Article number
SCALANCE TAP104	2 x RJ45 ports with securing collars, 10/100 Mbps 2x RJ45 TAP ports	6GK5104-0BA00-1SA2

4.5.5 SCALANCE X-000

4.5.5.1 Description



Figure 4-5 SCALANCE X005

The unmanaged Industrial Ethernet switches of the SCALANCE X-000 product line are suitable for setting up small Industrial Ethernet networks with 10/100 Mbps in linear or star structures with switching functionality in machine or plant islands. The devices have a rugged metal housing in IP30 degree of protection and are designed for installation in the control cabinet. They can be mounted on the standard DIN rail, SIMATIC S7-300 DIN rail or directly on the wall. The device has an LED for diagnostics of the device.

The SCALANCE X-000 is equipped with five RJ45 ports with securing collars for connection of end devices or additional network segments. The EEC and TS variants are suitable for the use under rugged conditions. The TS variant is approved for use in rail and road traffic.

4.5.5.2 Features

	X005	X005EEC
Diagnostics LED	•	•
Railway approval	-	•

- Suitable / available or according to the specified standard

The switch does not support any redundancy functions and cannot be used in redundant networks, with the exception of its usage in two RNA-capable devices. If the connecting network lines are not subject to other redundancy methods, the device becomes neither capable of redundancy nor of RNA.

4.5.5.3 Interfaces

Device	Twisted pair
	10/100 Mbps
SCALANCE X005	5x RJ45
SCALANCE X005EEC	5x RJ45

4.5.5.4 Article numbers

Device	Description	Article number
SCALANCE X005	5x 10/100 Mbps RJ45 ports	6GK5 005-0BA10-1AA3
SCALANCE X005EEC	5x 10/100 Mbps RJ45 ports; extended temperature range -40 °C to +70 °C, approved for use in rail and road traffic	6GK5 005-0BA10-1CA3

4.5.6 SCALANCE XB-000

4.5.6.1 Description



Figure 4-6 SCALANCE XB-000

The unmanaged Industrial Ethernet switches of the SCALANCE XB-000 product line are suitable for setting up small Industrial Ethernet networks in linear or star structures with switching functionality in machine or plant parts. The devices have a rugged plastic housing in IP20 degree of protection and are intended for installation in the control cabinet. They can be installed on the standard rail or directly on a wall. The devices are available with various configurations for copper and fiber-optic cables.

With SCALANCE XB-000 there are variants with transmission rates of 10/100 Mbps and 10/100/1000 Mbps. The devices that support Gigabit Ethernet contain the supplement G in the device designation. Device variants with 24 V AC are suitable for usage in building automation. All devices have LEDs for device diagnostics of the device.

4.5.6.2 Characteristics

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

		XB004-1 XB004-1LD XB005 XB008	XB004-2	XB004-1G XB004-1LDG XB005G XB008G
Gigabit Ethernet		-	-	•
Diagnostics LED		•	•	•
Power supply	24 V DC	•	•	•
	24 V AC (50/60 Hz)	•	-	-

- Suitable / available or according to the specified standard

4.5.6.3 Interfaces

Device	Twisted pair		Fiber-optic cables		
	10/100 Mbps	10/100/1000 Mbps	100 Mbps	1000 Mbps	Max. segment length / km
XB004-1	4x RJ45	-	1x SC, multimode	-	4* / 5**
XB004-1LD	4x RJ45	-	1x SC, single-mode	-	26***
XB004-2	4x RJ45	-	2x SC, multimode	-	5
XB005	5x RJ45	-	-	-	-
XB008	8x RJ45	-	-	-	-
XB004-1G	-	4x RJ45	-	1x SC, multimode	0.75
XB004-1LDG	-	4x RJ45	-	1x SC, single-mode	10
XB005G	-	5x RJ45	-	-	-
XB008G	-	8x RJ45	-	-	-

* With a cable cross-section of 50 µm

** With a cable cross-section of 62.5 µm

*** With a cable cross-section of 9/125 µm; attenuation ≤ 0.5 dB/km at 1310 nm

4.5.6.4 Article numbers

Device	Description	Article number
SCALANCE XB004-1	4x 10/100 Mbps RJ45 ports electrical, 1x 100 Mbps SC port optical (multimode, glass), up to max. 5 km	6GK5004-1BD00-1AB2
SCALANCE XB004-1LD	4x 10/100 Mbps RJ45 ports electrical, 1x 100 Mbps SC port optical (single-mode, glass), up to max. 26 km	6GK5004-1BF00-1AB2

Device	Description	Article number
SCALANCE XB004-2	4x 10/100 Mbps RJ45 ports electrical, 2x 100 Mbps SC port optical (multimode, glass), up to max. 5 km	6GK5004-2BD00-1AB2
SCALANCE XB005	5 x 10/100 Mbps RJ-45 ports electrical	6GK5005-0BA00-1AB2
SCALANCE XB008	8 x 10/100 Mbps RJ-45 ports electrical	6GK5008-0BA00-1AB2
SCALANCE XB004-1G	4x 10/100/1000 Mbps RJ45 ports electrical, 1x 1000 Mbps SC port optical (multimode, glass), up to max. 0.75 km	6GK5004-1GL00-1AB2
SCALANCE XB004-1LDG	4x 10/100/1000 Mbps RJ45 ports electrical, 1x 1000 Mbps SC port optical (single-mode, glass), up to max. 10 km	6GK5004-1GM10-1AB2
SCALANCE XB005G	5 x 10/100/1000 Mbps, RJ-45 ports electrical	6GK5005-0GA00-1AB2
SCALANCE XB008G	8 x 10/100/1000 Mbps, RJ-45 ports electrical	6GK5008-0GA00-1AB2

4.5.7 SCALANCE X-100

4.5.7.1 Description



Figure 4-7 SCALANCE X-100

The Industrial Ethernet Switch SCALANCE X108PoE allows for cost-effective installation of Industrial Ethernet with 10/100 Mbps line and star structures with switching functionality.

The SCALANCE X108PoE is suitable for machine-oriented applications and has a rugged metal enclosure in IP30 degree of protection for space-saving cabinet installation on the standard DIN rail, S7-300 DIN rail or for wall mounting.

The switch offers 8x RJ45 ports, two of which have a Power-over-Ethernet functionality (PoE) in accordance with IEEE 802.3at Type 1 (corresponds to IEEE 802.3af). All ports are equipped with additional securing collars suitable for industrial use for optimum connection of IE FC RJ45 Plug 180. An additional tensile and bending relief is ensured by latching the

plug-in connector into the housing. The transfer of data and energy to Power-over-Ethernet capable end devices via the SCALANCE X108PoE data cable reduces network installation costs.

Secure operation is guaranteed by the redundant power supply and a signaling contact with on-site configuration. The information about supply voltage, port status and data traffic is supplied by an LED.

4.5.7.2 Characteristics

The device has the characteristics shown in the following table:

	X108PoE
PoE Power over Ethernet	•
Diagnostics LED	•
Redundant power supply	•
Signaling contact	•
On site display (Set button)	•
C-PLUG slot	-

- Suitable / available or according to the specified standard

Additional information on the SCALANCE X108PoE:

Over and above the pure Ethernet functionality, ports 1 and 2 can also be used to supply power to Power-over-Ethernet end devices, for example SCALANCE-W, in compliance with 802.3af. The two ports providing PoE are supplied from the same power source. This means that they are electrically interconnected. They are however isolated from ground, from the ports that do not provide PoE and from the power connector (24 V). Their use is therefore subject to the conditions listed in IEEE 802.3af for Environment A. Ports 3 to 8 do not have the PoE function. These ports are all isolated from each other.

Note

Ethernet devices without PoE functionality can also be connected to ports 1 and 2. A voltage is applied only after the SCALANCE X108 PoE has detected a PoE end device complying with the standard at the port.

4.5.7.3 Interfaces

IE Switch	Twisted pair	
	10/100 Mbps	10/100/1000 Mbps with PoE
X108PoE	6x RJ45	2x RJ45

4.5.7.4 Article numbers

Device	Description	Article number
SCALANCE X108PoE	6x 10/100 Mbps RJ45 ports, electrical 2x 10/100 Mbps RJ45 PoE ports, electrical	6GK5108-0PA00-2AA3

4.5.8 SCALANCE XB-100

4.5.8.1 Description



Figure 4-8 SCALANCE XB-100

The devices of the SCALANCE XB-100 product line are unmanaged Industrial Ethernet switches for the setup of small Industrial Ethernet networks with transmission rates of 10/100 Mbps in linear or star structures. The SCALANCE XB-100 devices are suitable for applications in industry and building automation for which management via CLI or WBM is not required.

The space-saving plastic housing in IP20 degree of protection is suitable for DIN rail and wall mounting and is intended for installation in a control cabinet. The redundant power supply and a signaling contact with on-site operation ensure high operational safety. An LED display provides information about supply voltage, port status and data traffic. All versions are PROFINET CC-A compliant and can be used in hazardous areas of Zone 2 (ATEX, IECEx).

Different port configurations with up to 24 RJ45 ports are available. There are also two models available with connections for multimode fiber-optic cables (ST/BFOC or SC interface).

4.5.8.2 Features

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

	XB108-2 XB112 XB116 XB124
Gigabit Ethernet	-
Power supply	24 V DC / 24 V AC
Redundant power supply	•
Diagnostics LED	•

- Suitable / available or according to the specified standard

4.5.8.3 Interfaces

Device	Twisted pair	Fiber-optic cables	
	10/100 Mbps	10/100 Mbps	Max. segment length / km
XB108-2 (SC)	8x RJ45	2x SC, multimode	5*
XB108-2 (ST)	8x RJ45	2x ST/BFOC, multimode	5*
XB112	12x RJ45	-	-
XB116	16x RJ45	-	-
XB124	24x RJ45	-	-

* With a cable cross-section of 50/125 µm or 62.5/125 µm; attenuation ≤ 1 dB/km at 1310 nm; 1200 MHz * km

4.5.8.4 Article numbers

Device	Description	Article number
SCALANCE XB108-2(SC)	8x 10/100 Mbps RJ45 ports, 2x 10/100 Mbps SC ports, multimode fiber-optic cable	6GK5108-2BD00-2AB2
SCALANCE XB108-2(ST)	8x 10/100 Mbps RJ45 ports, 2x 10/100 Mbps ST/BFOC ports, multimode fiber-optic cable	6GK5108-2BB00-2AB2
SCALANCE XB112	12x 10/100 Mbps RJ45 ports	6GK5112-0BA00-2AB2
SCALANCE XB116	16 x 10/100 Mbps RJ-45 ports	6GK5116-0BA00-2AB2
SCALANCE XB124	24 x 10/100 Mbps RJ45 ports	6GK5124-0BA00-2AB2

4.5.9 SCALANCE XC-100

4.5.9.1 Description



Figure 4-9 SCALANCE XC-100

The devices of the SCALANCE XC-100 product line are unmanaged Industrial Ethernet switches for the setup of Industrial Ethernet networks with transmission rates of 10/100 Mbps in linear or star structures. The SCALANCE XC-100 devices are suitable for applications in which a redundancy manager is not required for a ring topology and no Gigabit Ethernet is required.

The rear of the robust enclosure in SIMATIC S7-1500 format with IP20 degree of protection consists of die-cast aluminum and offers all options required for installation in the industrial environment (SIMATIC S7-1500 and S7-300 standard rail, standard DIN rail, wall mounting). The housings have IP20 degree of protection and are designed for installation in a control cabinet. The RJ45 sockets with securing collar provide additional strain and bend relief for the use of FastConnect connectors.

The redundant power supply and a signaling contact with on-site operation ensure high operational safety. An LED display provides information about supply voltage, port status and data traffic.

Different port configurations with up to 24 RJ45 ports are available. There are also two models available with connections for multimode fiber-optic cables (ST/BFOC or SC interface).

4.5.9.2 Features

	XC106-2 XC108 XC116 XC124
Gigabit Ethernet	-
Diagnostics LED	•
Redundant power supply	•

	XC106-2 XC108 XC116 XC124
Signaling contact	•
On site display (Set button)	•

• Suitable / available or according to the specified standard

4.5.9.3 Interfaces

Device	Twisted pair	Fiber-optic cables	
	10/100 Mbps	10/100 Mbps	Max. segment length / km
XC106-2 (SC)	6x RJ45	2x SC, multimode	5*
XC106-2 (ST)	6x RJ45	2x ST/BFOC, multimode	5*
XC108	8x RJ45	-	-
XC116	16x RJ45	-	-
XC124	24x RJ45	-	-

* With a cable cross-section of 50/125 µm or 62.5/125 µm; attenuation ≤ 1 dB/km at 1310 nm; 1200 MHz * km

4.5.9.4 Article numbers

Device	Description	Article number
SCALANCE XC106-2 (SC)	6x 10/100 Mbps RJ45 ports, 2x 10/100 Mbps SC ports, multimode fiber-optic cable	6GK5 106-2BD00-2AC2
SCALANCE XC106-2 (ST/BFOC)	6x 10/100 Mbps RJ45 ports, 2x 10/100 Mbps ST/BFOC ports, multimode fiber-optic cable	6GK5 106-2BB00-2AC2
SCALANCE XC108	8x 10/100 Mbps RJ45 ports	6GK5 108-0BA00-2AC2
SCALANCE XC116	16x 10/100 Mbps RJ45 ports	6GK5 116-0BA00-2AC2
SCALANCE XC124	24x 10/100 Mbps RJ45 ports	6GK5 124-0BA00-2AC2

4.5.10 SCALANCE XR-100WG

4.5.10.1 Description



Figure 4-10 SCALANCE XR124WG

The SCALANCE XR-100WG (Work Group switches) are unmanaged Industrial Ethernet switches for applications in the industry-oriented area. They are suitable for setting up Industrial Ethernet networks with transmission rates of 10/100 Mbps in line and star structure.

The devices have a rugged metal housing in IP30 degree of protection and are intended for installation in 19" control cabinets. The devices offer 24 electrical RJ45 ports. The status information for on-site diagnostics (link status, data traffic) is displayed via LEDs. There are two device versions for a 24 V DC or 100-240 V AC power supply. A redundant voltage supply is possible for devices with a 24 V DC supply voltage.

4.5.10.2 Features

The device has the characteristics shown in the following table:

	XR124WG
Diagnostics LED	•
Redundant power supply	• ¹⁾

• Suitable / available or according to the specified standard

¹⁾ Only for 24 V DC device variants

4.5.10.3 Interfaces

Device	Twisted pair
	10/100 Mbps
XR124WG	24x RJ45

4.5.10.4 Article numbers

Device	Properties	Article number
SCALANCE XR124WG	24 V DC variant 24x 10/100 Mbps RJ45 ports, 2x 24 V DC, connector for the power supply on the front	6GK5124-0BA00-2AR3
	240 V AC variant 24x 10/100 Mbps RJ45 ports, 1x 240 V AC, connector for the power supply on the rear	6GK5124-0BA00-3AR3

4.5.11 SCALANCE X-200IRT

4.5.11.1 Description



Figure 4-11 SCALANCE X-200IRT



Figure 4-12 SCALANCE X-200IRT PRO

The managed Industrial Ethernet switches of the SCALANCE X-200IRT product line are especially designed for the setup of Isochronous Real-Time (IRT) Industrial Ethernet networks in line, star and ring structures with transmission rates of 10/100 Mbps. By using the combination of the switching mechanisms "Cut Through" and "Store and Forward", the

switches meet the real-time requirements of PROFINET. They are used in networks that have special requirements for automation solutions with regard to line topology, hard real time and unrestricted IT openness incorporated in one technology.

The device variant IRT has a compact metal housing in the IP30 degree of protection for installation in control cabinets. The variant IRT PRO has a robust metal housing in IP65/67 degree of protection; its industrial design push-pull connection technology is designed for the setup without cabinet. All device variants can be mounted on the standard DIN rail, on an S7-300 standard rail or directly on the wall. With the optional hat rail adapter, installation is also possible on an S7-1500 standard rail.

The devices are designed for rugged ambient conditions and can also be used in hazardous areas of Zone 2 (ATEX, IECEx). All device variants are compliant with PROFINET CC-C.

Different port configurations with electrical and optical connections (ST/BFOC or SC RJ interface) are available.

The IRT device versions are equipped with RJ45 sockets with securing collars for an additional strain and bend relief; the PRO device variants are equipped with PROFINET-compliant push-pull connectors.

In contrast to the PRO device versions, the IRT device versions have a redundant power supply. A signaling contact with on-site operation provides high operational safety for all device versions. An LED provides information about supply voltage, port status, data traffic, activated redundancy manager as well as POF variants via the POF cable diagnostics.

A remote system diagnostics via signaling contact, PROFINET, SNMP, integrated Web server, SINEMA server or SINEC NMS and an automatic function for sending e-mails for remote diagnostics and signaling via the network are available.

4.5.11.2 Features and functions

Features

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

	X200-4P IRT X201-3P IRT X202-2IRT X202-2P IRT X204IRT	X201-3P IRT PRO X202-2P IRT PRO X204IRT PRO
Diagnostics LED	•	•
Redundant power supply	•	-
Signaling contact	•	•
On site display (Set button)	•	•
IRT communication	•	•
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 use the Primary Setup Tool to assign the IP address, the switches must be accessible via 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
- SNTF
- PROFINET diagnostics
- Topology support (LLDP)
- Ring redundancy including RM functionality
- Passive listening
- Standby redundancy
- IRT capability
- Fast learning

4.5.11.3 Interfaces

Device	Twisted pair	Fiber-optic cables	
	10/100 Mbps	100 Mbps	Max. segment length / km
X200-4P IRT	-	4x SC RJ/ push-pull plug, POF/PCF	0.05 / 0.100 ***
X201-3P IRT	1x RJ45	3x SC RJ/ push-pull plug, POF/PCF	0.05 / 0.100 ***
X201-3P IRT PRO	1x RJ45	3x SC-RJ/ push-pull plug PRO, POF/PCF, multimode	0.05 / 0.100 ***
X202-2IRT	2x RJ45	2x ST/BFOC, multimode	4* / 5**
X202-2P IRT	2x RJ45	2x SC RJ, POF, multimode	0.05 / 0.100 ***
X202-2P IRT PRO	2x IE RJ45 Plug PRO	2x SC RJ/ push-pull plug POF/PCF, multimode	0.05 / 0.100 ***
X204IRT	4x RJ45	-	-
X204 IRT PRO	4x IE RJ45 Plug PRO	-	-

* With a cable cross-section of 50 µm

** With a cable-cross section of 62.5 µm

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

4.5.11.4 Article numbers

Device	Description	Article number
SCALANCE X200-4P IRT	4x 100 Mbps POF/PCF SC RJ ports	6GK5200-4AH00-2BA3
SCALANCE X201-3P IRT	1x 10/100 Mbps RJ45 port, 3x 100 Mbps POF SC RJ ports	6GK5201-3BH00-2BA3
SCALANCE X201-3P IRT PRO	1x 10/100 Mbps RJ45 port, 3x 100 Mbps POF SC RJ ports, degree of protection IP65/67	6GK5201-3JR00-2BA6
SCALANCE X202-2IRT	2x 10/100 Mbps RJ45 ports, 2x 100 Mbps multimode BFOC	6GK5202-2BB00-2BA3
SCALANCE X202-2P IRT	2x 10/100 Mbps RJ45 ports, 2x 100 Mbps POF SC RJ ports	6GK5202-2BH00-2BA3
SCALANCE X202-2P IRT PRO	2x 10/100 Mbps RJ45 push-pull ports, 2x 100 Mbps push-pull SC RJ ports, degree of protection IP65/67	6GK5202-2JR00-2BA6
SCALANCE X204IRT	4x 10/100 Mbps RJ45 ports	6GK5204-0BA00-2BA3
SCALANCE X204IRT PRO	4x 10/100 Mbps RJ45 push-pull ports, degree of protection IP65/67	6GK5204-0JA00-2BA6

4.5.12 SCALANCE X-200RNA

4.5.12.1 Description



Figure 4-13 SCALANCE X-200RNA

With the devices of the SCALANCE X-200RNA product line, fault-tolerant communication structures can be established that also ensure delay-free data transmission in case of a failure. The abbreviation "RNA" stands for "Redundant Network Access". Depending on the required network topology, the redundancy procedures PRP (Parallel Redundancy Protocol, for line and star topology) or HSR (High-availability Seamless Redundancy Protocol, for ring topology) are used. With the PRP redundancy procedure, a SCALANCE X-200RNA enables the connection of up to two end devices or network segments to two parallel networks. The operating principle of the HSR redundancy procedure consists of sending frames in ring networks into two directions. The devices of the SCALANCE X-200RNA series are available in two hardware versions. The X204RNA EEC variant has a metal housing and is suitable for ambient temperatures of -40 °C to 70 °C.

All ECC versions of the device are approved for railway applications according to EN 50155 and EN 50121-4.

4.5.12.2 Features and functions

Features

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

	X204RNA X204RNA EEC
Diagnostics LED	•
Redundant power supply	•
Signaling contact	•
On site display (Set button)	•
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 use the Primary Setup Tool to assign the IP address, the switches must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Web Based Management
- Command Line Interface
- HTTP, HTTPS
- SNMP
- SNTP
- MIB support
- TRAPs via e-mail
- Ring redundancy (not for 6GK5204-0BS00-3PA3/6GK5204-0BS00-3PA3)
- RNA (PRP)

4.5.12.3 Interfaces

Device	Total number of available ports	Twisted pair	Fiber-optic cables		Combo ports
		10/100 Mbps	10/100 Mbps	100/1000 Mbps	
X204RNA	4	4x RJ45 (of which 2x PRP ports)	-	-	-
X204RNA EEC	4 ¹⁾	Max. 4x RJ45 (of which 2x PRP ports)	-	-	2x SFP (100 Mbps) as PRP ports

1) Of which 2 are combo ports

Note

TP connectors of SCALANCE X204RNA EEC

2x RJ45 for connecting two end devices / network structures without PRP-1 capability and optionally 2x RJ45 or 2x SFP modules for connecting network structures capable of PRP. If an SFP module is inserted, the corresponding RJ45 jack is deactivated.

Example: If 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.

4.5.12.4 Article numbers

Device	Description	Supported modes	Article number
SCALANCE X204RNA (PRP)	4x 100 Mbps RJ45 ports	PRP ↔ standard Ethernet PRP ↔ HSR link	6GK5204-0BA00-2KB2
SCALANCE X204RNA (HSR)		HSR ↔ Standard Ethernet; HSR ↔ PRP coupling	6GK5204-0BA00-2MB2
SCALANCE X204RNA EEC (PRP)	2x 100 Mbps RJ45 ports and 2x 100 Mbps combo ports	PRP ↔ standard Ethernet	6GK5204-0BS00-3LA3
SCALANCE X204RNA EEC (HSR)		HSR ↔ Standard Ethernet; HSR ↔ PRP coupling	6GK5204-0BS00-2NA3
SCALANCE X204RNA EEC (PRP/HSR)		PRP ↔ Standard Ethernet; HSR ↔ Standard Ethernet; HSR ↔ PRP link	6GK5204-0BS00-3PA3

4.5.12.5 Accessories SFP transceiver

Pluggable transceiver SFP (100 Mbps)

Type	Property	Article number
SFP991-1	1 x 100 Mbps, LC port optical for glass FO cable (multimode), up to max. 5 km	6GK5991-1AD00-8AA0
SFP991-1 (C)	1 x 100 Mbps, SC port optical, for glass FO cable (multimode), up to max. 5 km, varnished	6GK5991-1AD00-8FA0
SFP991-1LD	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5991-1AF00-8AA0
SFP991-1LD (C)	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km, varnished	6GK5991-1AF00-8FA0
SFP991-1LH+	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5991-1AE00-8AA0
SFP991-1ELH200	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 200 km	6GK5991-1AE30-8AA0

The SFP plug-in transceiver (100 Mbps) cannot be operated in SFP+ slots.

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

SFP991 interfaces (100 Mbps)

Pluggable transceiver	Twisted pair	Fiber-optic cables	
	100 Mbps	100 Mbps	Max. segment length / km
SFP991-1 SFP991-1 (C)	-	1x LC, multimode	5*
SFP991-1LD SFP991-1LD (C)	-	1x LC, single-mode	26**
SFP991-1LH+	-	1x LC, single-mode	70
SFP991-1ELH200	-	1x LC, single-mode	200

* With a cable cross-section of 50/125 µm or 62.5/125 µm; attenuation 1 dB/km at 1310 nm; 1200 MHz * km

** With a cable cross-section of 9/125 µm; attenuation ≤ 0.5 dB/km at 1310 nm

Note

Slots for pluggable transceivers of the product group SFP991

The pluggable transceivers SFP991 with a transmission rate of 100 Mbps cannot be used for devices with the letter "G" in the type designation (Gigabit Ethernet) or in the slots for pluggable transceivers of the product groups SFP992 (1000 Mbps) and SFP993 (10 Gbps). When inserting an SFP991 into the wrong slot, the device detects the incorrect usage and reports the error.

4.5.13 SCALANCE XB-200

4.5.13.1 Description



Figure 4-14 SCALANCE XB-200

The SCALANCE XB-200 series provides devices suitable for industry at a 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 IP20 degree of protection and are intended for installation in the cabinet. They can be installed on a DIN rail without tools. The devices can also be mounted directly on the wall.

They also have a separate console connector and a redundant power supply. There are various port configurations for copper and fiber-optic cables with up to 13x RJ45 ports and 3x ST/BFOS or SC ports. All the designs are available in two variants that differ in the factory settings (EtherNet/IP or PROFINET variant).

Through the integrated redundancy manager, redundant ring structures can also be set up with these devices on the basis of High Speed Redundancy (HRP) or the Media Redundancy Protocol (MRP).

4.5.13.2 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	•

	XB208 XB205-3 (SC) XB205-3LD (SC) XB205-3 XB216 XB213-3 (SC) XB213-3LD (SC) XB213-3
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 use the Primary Setup Tool to assign the IP address, the switches must be accessible via 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)
- 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.

4.5.13.3 Interfaces

Device	Twisted pair	Fiber-optic cables	
	10/100 Mbps	10/100 Mbps	Max. segment length / km
XB208	8x RJ45	-	-
XB205-3 (SC)	5x RJ45	3x SC, multimode	5*
XB205-3LD (SC)	5x RJ45	3x SC, single-mode	26**
XB205-3	5x RJ45	3x ST, multimode	5*
XB216	16x RJ45	-	-
XB213-3 (SC)	13x RJ45	3x SC, multimode	5*
XB213-3LD (SC)	13x RJ45	3x SC, single-mode	26**
XB213-3	13x RJ45	3x ST, multimode	5*

* With a cable cross-section of 50/125 µm or 62.5/125 µm; attenuation 1 dB/km at 1310 nm; 1200 MHz * km

** With a cable cross-section of 9/125 µm; attenuation ≤ 0.5 dB/km at 1310 nm

4.5.13.4 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
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

4.5.14 SCALANCE XC-200

4.5.14.1 Description



Figure 4-15 SCALANCE XC-200

The devices of the SCALANCE XC-200 product line are managed Industrial Ethernet switches for the setup of Industrial Ethernet networks with transmission rates of 10/100/1000 Mbps in linear, star or ring structures.

The rear of the robust enclosure in the SIMATIC S7-1500 format consists of die-cast aluminum and offers all options for the installation that are required in the industrial environment (SIMATIC S7-1500 and S7-300 standard rail standard DIN rail, wall mounting). The housings have IP20 degree of protection and are designed for installation in a control cabinet. The RJ45 sockets with securing collar provide additional strain and bend relief for the use of FastConnect connectors. The redundant power distribution, a signaling contact, a console port for the direct device access as well as the optionally available exchangeable storage medium C-PLUG enable efficient operation of the devices.

Through a wide range of port configurations for copper and fiber-optic cables, all usual deployment scenarios can be covered in the medium-power range. The combo ports available with some devices provide for special flexibility. A combo port is a switch port with two optionally usable hardware interfaces, a combination of an RJ45 socket with a pluggable transceiver slot. If a pluggable transceiver is used, the RJ45 connector switches off and the pluggable transceiver is used for the data transfer. The pluggable transceivers can be used or replaced during operation.

The equipment scope of the SCALANCE XC-200 device allows the setup of networks with the highest reliability and availability. SCALANCE XC-200 devices support the redundancy procedures HRP and MRP as well as standby redundancy between HRP rings. Changes on fiber-optic cable sections or at fiber-optic cable ports can be detected at an early stage with fiber monitoring. All devices are suitable for the industry protocol PROFINET. There are also device variants for EtherNet/IP. SNMP can be used for remote diagnostics. The devices support the S2 system redundancy and H-Sync and can be integrated into the SIMATIC S7-1500 R/H systems.

4.5.14.2 Features and functions

Features

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

	XC206-2 (ST/BFOC) XC206-2 (SC) XC208 XC216 XC224	XC216-4C	XC206-2SFP XC206-2SFP G XC208G	XC216-4C G XC224-4C G
Gigabit Ethernet	-	-	•	•
Combo ports	-	•	-	•
Diagnostics LED	•	•	•	•
Redundant power supply	•	•	•	•
Signaling contact	•	•	•	•
Railway approval	-	-	-	-
On site display (Set button)	•	•	•	•
C-PLUG slot	•	•	•	•

- Suitable / available or according to the specified standard

The individual devices of the EEC variant have the characteristics shown in the following table:

	XC208EEC XC216EEC	XC206-2SFP EEC XC206-2SFP G EEC XC208G EEC	XC216-4C G EEC XC224-4C G EEC
Gigabit Ethernet	-	•	•
Combo ports	-	-	•
Diagnostics LED	•	•	•
Redundant power supply	•	•	•
Signaling contact	•	•	•
Railway approval	•	•	•
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 use the Primary Setup Tool to assign the IP address, the switches must be accessible via Ethernet.
- Configuration of the IP address with DHCP

- Configuration with STEP 7 V 5.3 plus SP 1
- Web Based Management
- Command Line Interface / Telnet
- SNMP / SNMP-supported diagnostics
- SNTF
- Ring redundancy including RM functionality
- MRP interconnection
- Standby redundancy
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol) and RSTP+
- Passive listening
- Topology support (LLDP)
- Link aggregation (IEEE 802.3ad)
- VLAN (Virtual Local Area Network) port based
- IGMP Snooping/Querier (Internet Group Management Protocol)
- IEEE 802.1x (radius)
- PROFINET diagnostics
- 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.

4.5.14.3 Interfaces

Device	Total number of available ports	Twisted pair		Fiber-optic cables	SFP slots	Combo ports
		10/100 Mbps	10/100/1000 Mbps	100 Mbps		
XC206-2 (ST/BFOC)	8	6x RJ45	-	2x ST/BFOC ²⁾ , multimode	-	-
XC206-2 (SC)	8	6x RJ45	-	2x SC ²⁾ , multimode	-	-
XC206-2SFP	8	6x RJ45	-	-	2x SFP991/SFP992	-
XC206-2SFP G	8	-	6x RJ45	-	2x SFP992	-
XC206-2SFP EEC	8	6x RJ45	-	-	2x SFP991/SFP992	-
XC206-2SFP G EEC	8	-	6x RJ45	-	2x SFP992	-
XC208	8	8x RJ45	-	-	-	-
XC208G	8	-	8x RJ45	-	-	-
XC208 EEC	8	8x RJ45	-	-	-	-
XC208G EEC	8	-	8x RJ45	-	-	-

4.5 SCALANCE X Industrial Ethernet Switches

Device	Total number of available ports	Twisted pair		Fiber-optic cables	SFP slots	Combo ports
		10/100 Mbps	10/100/1000 Mbps	100 Mbps		
XC216	16	16x RJ45	-	-	-	-
XC216 EEC	16	16x RJ45	-	-	-	-
XC216-4C	16 ¹⁾	12x RJ45	Max. 4x RJ45	-	-	4x SFP992
XC216-4C G	16 ¹⁾	-	Max. 16x RJ45	-	-	4x SFP992
XC216-4C G EEC	16 ¹⁾	-	Max. 16x RJ45	-	-	4x SFP992
XC224	24	24x RJ45	-	-	-	-
XC224-4C G	24 ¹⁾	-	Max. 24x RJ45	-	-	4x SFP992
XC224-4C G EEC	24 ¹⁾	-	Max. 24x RJ45	-	-	4x SFP992

¹⁾ Of which 4 are combo ports

²⁾ Max. segment length 5 km with a cable cross-section of 50 or 62.5 µm; attenuation ≤ 1 dB/km at 1310 nm

4.5.14.4 Article numbers

Device	Description	Article number (EtherNet/IP)	Article number (PROFINET)
SCALANCE XC206-2 (ST/BFOC)	6x 10/100 Mbps RJ45 ports, 2x 100 Mbps ST/BFOC ports, multimode FO cable	-	6GK5206-2BB00-2AC2
SCALANCE XC206-2 (SC)	6x 10/100 Mbps RJ45 ports, 2x 100 Mbps SC ports, multimode FO cable	-	6GK5206-2BD00-2AC2
SCALANCE XC206-2SFP	6x 10/100 Mbps RJ45 ports, 2x pluggable transceivers with 100/1000 Mbps	-	6GK5206-2BS00-2AC2
SCALANCE XC206-2SFP G	6x 10/100/1000 Mbps RJ45 ports, 2x pluggable transceiver slots with 1000 Mbps	6GK5206-2GS00-2TC2	6GK5206-2GS00-2AC2
SCALANCE XC206-2SFP EEC	6x 10/100 Mbps RJ45 ports, 2x pluggable transceivers with 100/1000 Mbps, coated PCB	-	6GK5206-2BS00-2FC2
SCALANCE XC206-2SFP G EEC	6x 10/100/1000 Mbps RJ45 ports, 2x pluggable transceiver slots with 1000 Mbps, coated PCB	-	6GK5206-2GS00-2FC2
SCALANCE XC208	8x 10/100 Mbps RJ45 ports	-	6GK5208-0BA00-2AC2
SCALANCE XC208G	8x 10/100/1000 Mbps RJ45 ports	6GK5208-0GA00-2TC2	6GK5208-0GA00-2AC2

Device	Description	Article number (EtherNet/IP)	Article number (PROFINET)
SCALANCE XC208EEC	8x 10/100 Mbps RJ45 ports, coated PCB	-	6GK5208-0BA00-2FC2
SCALANCE XC208G EEC	8x 10/100/1000 Mbps RJ45 ports, coated PCB	-	6GK5208-0GA00-2FC2
SCALANCE XC216	16x 10/100 Mbps RJ45 ports	-	6GK5216-0BA00-2AC2
SCALANCE XC216EEC	16x 10/100 Mbps RJ45 ports, coated PCB	-	6GK5216-0BA00-2FC2
SCALANCE XC216-4C	12x 10/100 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver 1000 Mbps or as 10/100/1000 Mbps RJ45 ports)	-	6GK5216-4BS00-2AC2
SCALANCE XC216-4C G	12x 10/100/1000 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver 1000 Mbps or as 10/100/1000 Mbps RJ45 ports)	6GK5216-4GS00-2TC2	6GK5216-4GS00-2AC2
SCALANCE XC216-4C G EEC	12x 10/100/1000 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver 1000 Mbps or as 10/100/1000 Mbps RJ45 ports), coated PCB	-	6GK5216-4GS00-2FC2
SCALANCE XC224	24x 10/100 Mbps RJ45 ports	-	6GK5224-0BA00-2AC2
SCALANCE XC224-4C G	20x 10/100/1000 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver 1000 Mbps or as 10/100/1000 Mbps RJ45 ports)	6GK5224-4GS00-2TC2	6GK5224-4GS00-2AC2
SCALANCE XC224-4C G EEC	20x 10/100/1000 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver 1000 Mbps or as 10/100/1000 Mbps RJ45 ports), coated PCB	-	6GK5224-4GS00-2FC2

4.5.14.5 Accessories SFP transceiver

Pluggable transceiver SFP (100 Mbps)

Type	Property	Article number
SFP991-1	1 x 100 Mbps, LC port optical for glass FO cable (multimode), up to max. 5 km	6GK5991-1AD00-8AA0
SFP991-1 (C)	1 x 100 Mbps, SC port optical, for glass FO cable (multimode), up to max. 5 km, varnished	6GK5991-1AD00-8FA0
SFP991-1LD	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5991-1AF00-8AA0

Type	Property	Article number
SFP991-1LD (C)	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km, varnished	6GK5991-1AF00-8FA0
SFP991-1LH+	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5991-1AE00-8AA0
SFP991-1ELH200	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 200 km	6GK5991-1AE30-8AA0

The SFP plug-in transceiver (100 Mbps) cannot be operated in SFP+ slots.

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Note

You cannot use the plug-in transceiver SFP (100 Mbps) with the following devices:

- Devices with the suffix "G" in the type designation
- Devices with combo ports

SFP991 interfaces (100 Mbps)

Pluggable transceiver	Twisted pair	Fiber-optic cables	
	100 Mbps	100 Mbps	Max. segment length / km
SFP991-1 SFP991-1 (C)	-	1x LC, multimode	5*
SFP991-1LD SFP991-1LD (C)	-	1x LC, single-mode	26**
SFP991-1LH+	-	1x LC, single-mode	70
SFP991-1ELH200	-	1x LC, single-mode	200

* With a cable cross-section of 50/125 µm or 62.5/125 µm; attenuation 1 dB/km at 1310 nm; 1200 MHz * km

** With a cable cross-section of 9/125 µm; attenuation ≤ 0.5 dB/km at 1310 nm

Note

Slots for pluggable transceivers of the product group SFP991

The pluggable transceivers SFP991 with a transmission rate of 100 Mbps cannot be used for devices with the letter "G" in the type designation (Gigabit Ethernet) or in the slots for pluggable transceivers of the product groups SFP992 (1000 Mbps) and SFP993 (10 Gbps). When inserting an SFP991 into the wrong slot, the device detects the incorrect usage and reports the error.

Pluggable transceiver SFP (1000 Mbps)

Type	Property	Article number
SFP992-1	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 750 m	6GK5 992-1AL00-8AA0
SFP992-1+	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 2 km	6GK5 992-1AG00-8AA0
SFP992-1LD	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km	6GK5 992-1AM00-8AA0
SFP992-1LD (C)*	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km, varnished	6GK5 992-1AM00-8FA0
SFP992-1LD+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 30 km	6GK5 992-1AM30-8AA0
SFP992-1LH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 40 km	6GK5 992-1AN00-8AA0
SFP992-1LH+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 992-1AP00-8AA0
SFP992-1ELH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 120 km	6GK5 992-1AQ00-8AA0

* Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Bidirectional plug-in transceiver SFP

Bidirectional plug-in transceivers feature only one fiber connection. They transmit and receive on two different wavelengths. To establish a connection, you need two matching bidirectional SFPs. The connected SFPs must respectively transmit on the wavelength at which the connection partner receives.

Type	Properties	Article number
SFP992-1BXMT	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AL00-8TA0
SFP992-1BXM R	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AL00-8RA0

SFP992 interfaces (1000 Mbps)

Pluggable transceiver	Twisted pair	Fiber-optic cables	
	1000 Mbps	1000 Mbps	Max. segment length / km
SFP992-1	-	1x LC, multimode	0.750
SFP992-1+	-	1x LC, multimode	2
SFP992-1LD	-	1x LC, single-mode	10
SFP992-1LD (C)	-		
SFP992-1LH	-	1x LC, single-mode	40

Pluggable transceiver	Twisted pair	Fiber-optic cables	
	1000 Mbps	1000 Mbps	Max. segment length / km
SFP992-1LH+	-	1x LC, single-mode	70
SFP992-1ELH	-	1x LC, single-mode	120
SFP992-1BXMT	-	1x LC, multimode	0.500
SFP992-1BXM	-	1x LC, multimode	0.500

4.5.15 SCALANCE XF-200/XF-200IRT

4.5.15.1 Description



Figure 4-16 SCALANCE XF-200/XF-200IRT



Figure 4-17 SCALANCE XF-200BA IRT with preassembled BusAdapters

The Managed Industrial Ethernet switches SCALANCE XF-200 product line allows for cost-effective installation of 10/100 Mbps Industrial Ethernet networks with linear (bus), star or ring structures with switching functionality, where high availability of the network or remote diagnostics options are required.

The SCALANCE XF-200 are characterized by an ultra-flat housing in IP30 degree of protection and are suitable for use in small cabinets. They can be mounted on a standard DIN rail without tools. The SCALANCE XF-200 have different port configurations with electrical RJ45 ports with securing collars for connection of an IE FC RJ45 Plug 180 secured by latching as well as optical ST/BFOC ports for glass multimode fiber optic cables. The devices support the fiber monitoring protocol and allow for monitoring of fiber-optic cables. In addition to the LED, a redundant power distribution and a signaling contact are part of the equipment.

The SCALANCE XF-200IRT/XF-200BA IRT form a special class. The switches are especially designed for setup of Industrial Ethernet networks with isochronous/clocked real-time communication and can optimally fulfill the PROFINET real-time requirements through the use of the "Cut Through" switching mechanism. The SCALANCE XF-200BA IRT are available in SIMATIC ET 200SP design with/without pre-installed bus adapters. The SCALANCE XF-200IRT/XF-200BA IRT also have a flat housing in IP20 degree of protection and can also be mounted in small cabinets on the DIN rail.

4.5.15.2 Features and functions

Features

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

	XF204 XF204-2 XF206-1 XF208	XF201-3P IRT XF202-2P IRT XF204IRT XF204-2BA IRT
Diagnostics LED	•	•
Redundant power supply	•	•
Signaling contact	•	•
On site display (Set button)	•	•
IRT communication	-	•
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 use the Primary Setup Tool to assign the IP address, the switches must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7 / Telnet
- Web Based Management
- Command Line Interface

4.5 SCALANCE X Industrial Ethernet Switches

- SNMP / SNMP-supported diagnostics
- SNTP
- Ring redundancy including RM functionality
- Passive Listening
- Topology support (LLDP)
- PROFINET diagnostics

The IRT devices have the following additional functions:

- Standby redundancy
- IRT capability

4.5.15.3 Interfaces

Device	Twisted pair	Fiber-optic cables	
	10/100 Mbps	10/100 Mbps	Max. segment length / km
XF204	4x RJ45	-	-
XF204-2	4x RJ45	2x ST/BFOC, multimode	4* / 5**
XF206-1	6x RJ45	1x ST/BFOC, multimode	4* / 5**
XF208	8x RJ45	-	-
XF201-3P IRT	1x RJ45	3x SC RJ/ push-pull plug, POF	-
XF202-2P IRT	2x RJ45	2x SC RJ/push-pull plug, POF	-
XF204IRT	4x RJ45	-	-
XF204-2BA IRT Basic device without BusAdapter	0x RJ45	-	-

* With a cable cross-section of 50 µm

** With a cable-cross section of 62.5 µm

4.5.15.4 Article numbers

Device	Description	Article number
SCALANCE XF204	4 x 10/100 Mbps RJ-45 ports electrical	6GK5204-0BA00-2AF2
SCALANCE XF204-2	4x 10/100 Mbps RJ45 ports electrical, 2x 100 Mbps BFOC ports optical (multimode, glass), up to max. 5 km	6GK5204-2BC00-2AF2
SCALANCE 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
SCALANCE XF208	8x 10/100 Mbps RJ45 ports electrical	6GK5208-0BA00-2AF2

Device	Description	Article number
SCALANCE XF201-3P IRT	1x 10/100 Mbps RJ45 ports, 3 x 100 Mbps POF SC RJ ports, BusAdapter installed	6GK5201-3BH00-2BD2
SCALANCE XF202-2P IRT	2x 10/100 Mbps RJ45 ports, 2x 100 Mbps POF SC RJ ports, BusAdapter installed	6GK5202-2BH00-2BD2
SCALANCE XF204IRT	4 x 10/100 Mbps RJ-45 ports	6GK5204-0BA00-2BF2
SCALANCE XF204-2BA IRT	4x 10/100 Mbps, 2x BusAdapter interface	6GK5204-2AA00-2BD2

4.5.15.5 Accessories bus adapter

The bus adapters allow you a free choice of the connector technology for SCALANCE XF-200 IRT.

The SCALANCE XF-200 IRTs support the following bus adapters:

Component	Description	Article number
BA 2xRJ45 *)	PROFINET bus adapter with Ethernet socket for standard RJ-45 plugs	6ES7193-6AR00-0AA0
BA 2xFC *)	PROFINET bus adapter with FastConnect Ethernet connector for direct connection of the bus cable)	6ES7193-6AF00-0AA0
BA 2xSCRJ	PROFINET bus adapter with fiber-optic connector POF/PCF	6ES7193-6AP00-0AA0
BA SCRJ/RJ45	Media converter, PROFINET BusAdapter with fiber-optic connector POF/PCF ↔ standard RJ45 plug	6ES7193-6AP20-0AA0
BA SCRJ/FC	Media converter, PROFINET BusAdapter with fiber-optic connector POF/PCF↔ direct connection of the bus cable	6ES7193-6AP40-0AA0
BA 2xLC	SIMATIC BusAdapter with two LC sockets (Lucent Connector)	6ES7193-6AG00-0AA0
BA LC/RJ45	SIMATIC BusAdapter with one LC socket and one RJ45 socket each (media converter)	6ES7193-6AG20-0AA0
BA LC/FC	SIMATIC BusAdapter with an LC socket and a FastConnect connection (media converter)	6ES7193-6AG40-0AA0

*) The approvals for shipbuilding are only valid with the indicated bus adapters

4.5.16 SCALANCE XF-200BA

4.5.16.1 Description



Figure 4-18 SCALANCE XF204-2BA DNA

The SCALANCE XF204-2BA DNA provides a Dual Network Access functionality (DNA or Y-switch functionality). This device connects a redundant PROFINET ring to a fault tolerant PROFINET system (R1 system). This enables the reliable connection of a ring topology to the two redundant cables of the R1 system. The SCALANCE XF204-2BA DNA does not support VLANs.

The SCALANCE XF204-2BA is a managed IE switch for factory and process automation. This device supports VLANs and PROFINET system redundancy (S2) but has no Y functionality. Both switches are NAMUR NE 21-compliant and have coated PCBs as well as an extended temperature range of -40 °C to +70 °C. The maximum set-up altitude is 4000 m.

Due to their flat design, the devices can be mounted in control cabinets in a space-saving way on the standard DIN rail. Two bus adapter interfaces offer the option of individual equipment of the basic device with up to two modular bus adapters with two ports each. This ensures optimum setup of electrical and optical linear, star and ring structure. Thanks to the support of Configuration in Run (CiR/H-CiR), configuration changes defined via PROFINET can be performed at the switch during operation.

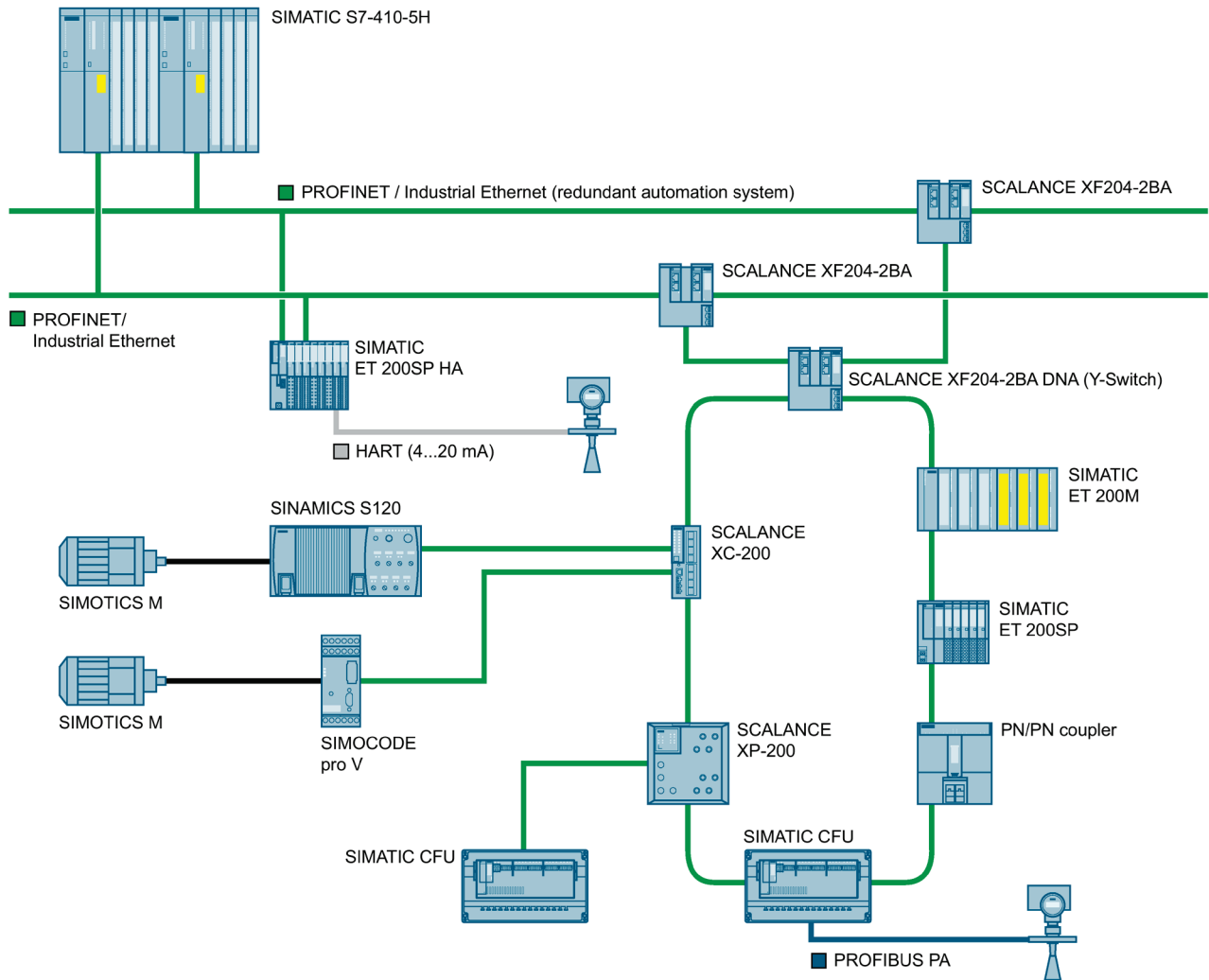


Figure 4-19 Y functionality

4.5.16.2 Features and functions

Features

The devices have the characteristics shown in the following table:

	XF204-2 BA	XF204-2 BA DNA
Diagnostics LED		•
Redundant power supply		•
Signaling contact		•

	XF204-2 BA XF204-2 BA DNA
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 use the Primary Setup Tool to assign the IP address, the switches must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7 / TIA
- Web Based Management
- Command Line Interface / Telnet
- SNMP / SNMP-supported diagnostics
- SNTP
- Ring redundancy including RM functionality
- Standby redundancy
- Passive listening
- DHCP client
- Topology support (LLDP)
- PROFINET diagnostics

4.5.16.3 Interfaces

Device	Twisted pair	Fiber-optic cables		BusAdapter slot
	10/100 Mbps	100 Mbps	1000 Mbps	
XF204-2BA Basic device without BusAdapter	-	-	-	2
XF204-2BA DNA Basic device without BusAdapter	-	-	-	2

4.5.16.4 Article numbers

Device	Description	Article number
SCALANCE XF204-2BA	4x 10/100 Mbps, 2x BusAdapter interface	6GK5204-2AA00-2GF2
SCALANCE XF204-2BA DNA (Y-Switch)	4x 10/100 Mbps, 2x BusAdapter interface	6GK5204-2AA00-2YF2

4.5.17 SCALANCE XP-200

4.5.17.1 Description



Figure 4-20 SCALANCE XP-200

The devices of the SCALANCE XP-200 product line are managed Industrial Ethernet switches for the setup of Industrial Ethernet networks with transmission rates of 10/100/1000 Mbps in linear, star or ring structures. The devices support the redundancy procedures HRP and MRP as well as the redundant coupling of rings via HRP standby and MRP interconnection.

The SCALANCE XP-200 devices are designed for use cases with high mechanical load and extreme ambient conditions (temperature, vibrations, shocks). The metal housing in IP65 degree of protection is suitable for operation outside of control cabinets and can be mounted on an ET 200pro module rack, an ITEM profile or directly on a wall. The 8 or 16 Ethernet ports as well as other interfaces (redundant power supply, fault signaling contact, console port) are designed as M12 connections.

The devices are designed for the extended temperature range of -40 °C to +70 °C and for an installation altitude of up to 4000 meters. The EEC variants are additionally equipped with coated PCBs and are suitable for railway applications (EN 50155, EN 45545). The immunity of the devices corresponds to the NAMUR NE 21 standard. All EEC variants of the products are also available in a version for Power over Ethernet according to IEEE 802.3at Type 2.

4.5 SCALANCE X Industrial Ethernet Switches

The devices support the S2 system redundancy and H-Sync and can be integrated into SIMATIC S7-1500 R/H systems. In addition, the devices support Configuration in Run (CiR/H-CiR). This enables configuration changes defined via PROFINET to be performed at the switch during operation.

The configuration data can also be stored on the optionally available C-PLUG removable data storage medium. This enables quick configuration of a new device during device replacement.

All devices are suitable for the industry protocol PROFINET. The two models XP-208 and XP-216 are also available preassembled ex factory for EtherNet/IP.

4.5.17.2 Features and functions

Features

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

	XP208	XP208 EEC	XP208PoE EEC	XP216	XP216 EEC	XP216PoE EEC
Gigabit Ethernet	-	-	-	•	•	•
PoE Power over Ethernet	-	-	•	-	-	•
Diagnostics LED	•	•	•	•	•	•
Redundant power supply	•	•	•	•	•	•
Signaling contact	•	•	•	•	•	•
Railway approval	-	•	•	-	•	•
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 use the Primary Setup Tool to assign the IP address, the switches must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7
- Web Based Management
- Command Line Interface / Telnet
- SNMP / SNMP-supported diagnostics
- SNTP
- Ring redundancy including RM functionality
- Standby redundancy

- MRP interconnection
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol) as well as RSTP+
- Passive listening
- Topology support (LLDP)
- VLAN (Virtual Local Area Network) port based
- IGMP Snooping/Querier (Internet Group Management Protocol)
- DHCP server / DHCP client / DHCP options 66, 67, 82
- Access Control List (ACL), MAC and IP-based
- IEEE 802.1x (radius)
- Link aggregation
- PROFINET diagnostics
- Some devices exist in two variants: PROFINET and EtherNet/IP However, the mode can be switched over as required for both device variants.
In EtherNet/IP mode, the devices also have EtherNet/IP diagnostics.

4.5.17.3 Interfaces

Device	Twisted pair			
	10/100 Mbps	10/100 Mbps with PoE	10/100/1000 Mbps	10/100/1000 Mbps with PoE
XP208 XP208 EEC	8x M12	-	-	-
XP208PoE EEC	4x M12	4x M12	-	-
XP216 XP216 EEC	12x M12	-	4x M12	-
XP216PoE EEC	6x M12	6x M12	2x M12	2x M12

4.5.17.4 Article numbers

Device	Description	Article number (PROFINET)	Article number (Ethernet/IP)
SCALANCE XP208	8x 10/100 Mbps M12 connector technology electrical	6GK5208-0HA00-2AS6	6GK5208-0HA00-2TS6
SCALANCE XP208 EEC	8x 10/100 Mbps M12 connector technology electrical, coated PCB	6GK5208-0HA00-2ES6	-
SCALANCE XP208PoE EEC	8x 10/100 Mbps M12 connector technology electrical, coated PCB, Power over Ethernet at 4 ports	6GK5208-0UA00-5ES6	-
SCALANCE XP216	12x 10/100 Mbps and 4x 10/100/1000 Mbps M12 connector technology electrical	6GK5216-0HA00-2AS6	6GK5216-0HA00-2TS6

4.5 SCALANCE X Industrial Ethernet Switches

Device	Description	Article number (PROFINET)	Article number (Ethernet/IP)
SCALANCE XP216 EEC	12x 10/100 Mbps and 4x 10/100/1000 Mbps M12 connector technology electrical, coated PCB	6GK5216-0HA00-2ES6	-
SCALANCE XP216PoE EEC	12x 10/100 Mbps und 4x 10/100/1000 Mbps M12 connector technology electrical, coated PCB, Power over Ethernet on 8 ports	6GK5216-0UA00-5ES6	-

4.5.18 SCALANCE X-300

4.5.18.1 Description



Figure 4-21 SCALANCE X308-2M PoE



Figure 4-22 SCALANCE XR324-4M PoE



Figure 4-23 SCALANCE XR324-12M, fully modular device equipped with media modules

The managed Industrial Ethernet switches of the SCALANCE X-300/XR-300 product line are suitable for the setup of electrical and/or optical line, ring or star structures with transmission rates of 10/100/1000 Mbps in high-performance plant networks. The SCALANCE X-300/XR-300 have a wide range of functions for high network security and availability. They support numerous IT standard functions such as VLAN, IGMP Snooping/Querier or STP/RSTP, Quality of Service and allow for seamless integration of automation networks into existing company networks. By establishing virtual networks (VLAN) with the SCALANCE X-300/XR-300, an existing network can be divided into multiple virtual partial networks. The SCALANCE X-300/XR-300 also support the standardized redundancy procedures Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). This allows a subnetwork to be connected redundantly to a higher-level company network with reduced requirements for the reconfiguration time (within seconds). With the support of the Multiple Spanning Tree Protocol (MSTP), a network can be divided into multiple partial segments.

The devices have a rugged metal housing with IP30 degree of protection and are designed for use in switch boxes and control cabinets. The X-300 models are provided for mounting on a DIN rail, an S7-300 standard rail or for wall mounting; the XR-300 models for mounting in the 19" rack.

The devices are equipped with up to 16 fixed electrical RJ45 ports with securing collar for secure connection of IE FC RJ45 Plug 180. The partially or fully modular setup of the devices with 2 to 12 slots offers the possibility of individual equipping of the device with suitable 2-port media modules. These include two device variants with PoE ports IEEE 802.3at Type 1 (corresponding to IEEE 802.3af) for supply of the PoE capable end devices with voltage and data.

The supplied C-PLUG removable data storage medium can be used to store configuration and project engineering data and simply transfer them when replacing a device. The redundant power supply and the ring structures redundantly structured via MRP and HRP ensure high network availability.

The device can be monitored on site with a signaling contact with on-site configuration. Furthermore, the devices provide integrated system diagnostics with PROFINET, SNMP, integrated Web server, SINEMA server or SINEC NMS and an automatic function for sending e-mails for remote diagnostics and signaling via the network.

The TS variants are released according to EN 50155/ and EN 50121-4 for use in railway applications.

The EEC variants are designed for usage in extended temperature ranges of -40 °C to +70 °C. Note the reduced operating temperatures of -40 °C to +70 °C when using media modules or -40 °C to +60 °C when using SFP pluggable transceivers.

4.5.18.2 Features and functions

Features

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

	X308-2M XR324-12M XR324-4M EEC	X308-2M TS XR324-12M TS	X308-2M PoE XR324-4M PoE
Modular design	•	•	•
Gigabit Ethernet	•	•	•
PoE Power over Ethernet	-	-	•
Diagnostics LED	•	•	•
Redundant power supply	• ¹⁾	•	• ¹⁾
Railway applications	-	•	-
On site display (Set button)	•	•	•
C-PLUG slot	•	•	•

• Suitable / available or according to the specified standard

¹⁾ Only for devices variants with 24 V DC

Functions

All devices have the following functions:

- Configuration with the Primary Setup Tool (PST) V3 or higher; to use the Primary Setup Tool to assign the IP address, the switches must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7
- Web Based Management
- Command Line Interface/Telnet
- SNMP / SNMP-supported diagnostics
- Sntp
- Ring redundancy including RM functionality
- Standby redundancy
- MRP interconnection
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol) as well as RSTP+
- Passive Listening
- Topology support (LLDP)
- VLAN (Virtual Local Area Network)
- GVRP (Generic VLAN Registration Protocol)

- IGMP snooping/querier (Internet Group Management Protocol)
- DHCP server / DHCP client / DHCP options 66, 67, 82
- GMRP (Generic Multicast Protocol)
- Broadcast, Multicast, Unicast limiter
- Broadcast blocking
- Access Control List (ACL), MAC and IP-based
- IEEE 802.1x (Radius)
- Link aggregation
- PROFINET diagnostics

4.5.18.3 Interfaces

Device	Total number of available ports	Twisted pair		Fiber-optic cables	Slots for 2 port media modules
		10/100 Mbps	10/100/1000 Mbps	100/1000 Mbps	10/100/1000 Mbps
X308-2M	8	-	4x RJ45	-	2
X308-2M PoE	8	-	4x RJ45 ¹⁾	-	2
X308-2M TS	8	-	4x RJ45	-	2
XR324-12M	24	-	-	-	12
XR324-12M TS	24	-	-	-	12
XR324-4M EEC	24	-	16x RJ45 (of which 8 ¹⁾)	-	4
XR324-4M PoE	24	-	16x RJ45 (of which 8 ¹⁾)	-	4
XR324-4M PoE TS	24	-	16x RJ45 (of which 8 ¹⁾)	-	4

¹⁾ PoE connections

4.5.18.4 Article numbers

Device	Description	Article number
SCALANCE X308-2M	4x 10/100//1000 Mbps RJ45 ports, electrical 2x 10/100/1000 Mbps slots for 2-port media modules, electrical or optical	6GK5308-2GG10-2AA2
SCALANCE X308-2M PoE	4x 10/100/1000 Mbps RJ45 ports with PoE, electrical 2x 10/100/1000 Mbps slots for 2-port media modules, electrical or optical	6GK5308-2QG10-2AA2

4.5 SCALANCE X Industrial Ethernet Switches

Device	Description	Article number
SCALANCE X308-2M TS	4x 10/100//1000 Mbps RJ45 ports, electrical 2x 10/100/1000 Mbps slots for 2 port media modules, electrical or optical, with extended temperature range and approval EN 50155/EN 50121-4 for railway applications	6GK5308-2GG10-2CA2
SCALANCE XR324-12M	Fully modular 19" Industrial Ethernet switch; 12x 10/100/1000 Mbps slots for 2-port media modules, optionally electrically or optically equipped	
	24 VDC power supply	
	Data cable outlet front	6GK5324-0GG10-1AR2
	Data cable outlet rear	6GK5324-0GG10-1HR2
	Power supply 110 to 230 V AC	
	Data cable outlet front	6GK5324-0GG10-3AR2
	Data cable outlet rear	6GK5324-0GG10-3HR2
SCALANCE XR324-12M TS	Fully modular 19" Industrial Ethernet switch; 12x 10/100/1000 Mbps slots for 2-port media modules, optionally electrically or optically equipped Power supply 24 V DC, data cable outlet front with extended temperature range and EN 50155/ EN 50121-4 approval for railway applications	6GK5324-0GG10-1CR2
SCALANCE XR324-4M EEC	Partially modular 19" Industrial Ethernet switch; 8x 10/100/1000 Mbps RJ45 ports with PoE; 8x 10/100/1000 Mbps RJ45 ports without PoE; 4x 10/100/1000 Mbps slots for 2-port media modules, optionally electrically or optically equipped, with extended temperature range	
	Power supply 1x 24 V DC	
	Data cable outlet front	6GK5324-4GG10-1ER2
	Data cable outlet rear	6GK5324-4GG10-1JR2
	Power supply 2x 24 V DC	
	Data cable outlet front	6GK5324-4GG10-2ER2
	Data cable outlet back	6GK5324-4GG10-2JR2
	110 to 230 VAC power supply	
	Data cable outlet front	6GK5324-4GG10-3ER2
	Data cable outlet rear	6GK5324-4GG10-3JR2
	Voltage supply 2x 110 to 230 V AC	
	Data cable outlet front	6GK5324-4GG10-4ER2
	Data cable outlet back	6GK5324-4GG10-4JR2

Device	Description	Article number
SCALANCE XR324-4M PoE	Partially modular 19" Industrial Ethernet switch; 8x 10/100/1000 Mbps RJ45 Ports with PoE 8x 10/100/1000 Mbps RJ45 ports without PoE 4x 10/100/1000 Mbps slots for 2-port media modules, optionally electrically or optically equipped	
	24 VDC power supply	
	Data cable outlet front	6GK5324-4QG10-1AR2
	Data cable outlet back	6GK5324-4QG10-1HR2
	110 to 230 VAC power supply	
	Data cable outlet front	6GK5324-4QG10-3AR2
	Data cable outlet back	6GK5324-4QG10-3HR2
SCALANCE XR324-4M PoE TS	Partially modular 19" Industrial Ethernet switch; 8x 10/100/1000 Mbps RJ45-Ports with PoE 8x 10/100/1000 Mbps RJ45 ports without PoE 4x 10/100/1000 Mbps slots for 2-port media modules, optionally electrically or optically equipped Power supply 24 V DC, data cable outlet front with extended temperature range and EN 50155/ EN 50121-4 approval for railway applications.	6GK5324-4QG10-1CR2

4.5.18.5 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 additional media modules into unused media module slots and allows a change of the cabling technology (for example a change from copper to fiber-optic or from multimode to single mode fiber-optic cable).

Component	Twisted pair		Fiber-optic cables		
	10/100 Mbps	10/100/1000 Mbps	100 Mbps	1000 Mbps	Max. segment length / km
MM991-2	-	-	2x ST, multimode	-	4* / 5**
MM991-2LD	-	-	2x ST, single-mode	-	26
MM991-2	-	-	2x SC, multimode	-	4* / 5**
MM991-2LD	-	-	2x SC, single-mode	-	26
MM991-2LH+	-	-	2x SC, single-mode	-	70
MM992-2CUC	-	2x RJ45	-	-	-

4.5 SCALANCE X Industrial Ethernet Switches

Component	Twisted pair		Fiber-optic cables		
	10/100 Mbps	10/100/1000 Mbps	100 Mbps	1000 Mbps	Max. segment length / km
MM992-2CU	-	2x RJ45	-	-	-
MM992-2SFP	-	2x RJ45	-	-	-
MM992-2	-	-	-	2x SC, multimode	0.75
MM992-2LD	-	-	-	2x SC, single-mode	10
MM992-2LH	-	-	-	2x SC, single-mode	40
MM992-2LH+	-	-	-	2x SC, single-mode	70
MM992-2ELH	-	-	-	2x SC, single-mode	120

* With a cable cross-section of 50 µm

** With a cable cross-section 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.

Component	Twisted pair		Fiber-optic cables		
	10/100 Mbps	10/100/1000 Mbps	100 Mbps	1000 Mbps	Max. segment length / km
SFP991-1 SFP991-1 (C)	-	-	1x LC, multimode	-	4* / 5**
SFP991-1LD SFP991-1LD (C)	-	-	1x LC, single-mode	-	26
SFP991-1LH+	-	-	1x LC, single-mode	-	70
SFP991-1ELH200	-	-	1x LC, single-mode	-	200
SFP992-1	-	-	-	1x LC, multimode	0.75
SFP992-1+	-	-	-	1x LC, multimode	2
SFP992-1LD SFP992-1LD (C)	-	-	-	1x LC, single-mode	10
SFP992-1LH	-	-	-	1x LC, single-mode	40
SFP992-1LH+	-	-	-	1x LC, single-mode	70
SFP992-1ELH	-	-	-	1x LC, single-mode	120
SFP992-1BXMT	-	-	-	1x LC, multimode	0.500
SFP992-1BXMR	-	-	-	1x LC, multimode	0.500

* With a cable cross-section of 50 µm

** With a cable cross-section of 62.5 µm

4.5.19 SCALANCE XR-300WG

4.5.19.1 Description



Figure 4-24 SCALANCE XR-300WG

The devices of the SCALANCE XR-300WG product line are managed Industrial Ethernet switches for the setup of Industrial Ethernet networks with transmission rates of 10/100/1000 Mbps in linear, star or ring structures.

The devices have a robust metal housing in degree of protection IP30 and are intended for installation in 19" cabinets (one 19" height unit). Two device versions with 24 V DC or 100-240 V AC power supply are available. Apart from the 24 integrated RJ45 ports, the device variants XR328-4C WG also have four combo ports. The combo ports can be optionally equipped with pluggable transceivers for optical interfaces (SFP) or used as RJ45 ports. A console port (serial interface) allows for easy on-site parameter assignment and diagnostics.

A redundancy manager for Gigabit Ethernet and Fast Ethernet is integrated. The devices support standardized redundancy procedures (RSTP, MRP) for the redundant integration into higher-level networks.

4.5.19.2 Features and functions

Features

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

	XR324WG	XR328-4C WG
Combo ports	-	•
Gigabit Ethernet	-	•
Diagnostics LED	•	•
Redundant power supply	• ¹⁾	• ¹⁾
Console port (1x RS 232)	•	•

• Suitable / available or according to the specified standard

¹⁾ Only for 24 V DC device variants

Functions

All devices have the following functions:

- Configuration with the Primary Setup Tool (PST) V3 or higher; to assign the IP address using the Primary Setup Tool, the switch must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7
- Web Based Management
- Command Line Interface/Telnet
- SNMP / SNMP-supported diagnostics
- Sntp
- Ring redundancy including RM functionality
- Standby redundancy
- Passive Listening
- Topology support (LLDP)
- VLAN (Virtual Local Area Network)
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol)
- IGMP snooping/querier (Internet Group Management Protocol)
- DHCP server / DHCP client / DHCP options 66, 67, 82
- Unicast Filter
- Broadcast blocking / multicast blocking / unicast blocking
- Management ACL
- IEEE 802.1x (Radius)
- PROFINET diagnostics

4.5.19.3 Interfaces

Device	Total number of available ports	Twisted pair		Fiber-optic cables	Combo ports 1000 Mbps
		10/100 Mbps	10/100/1000 Mbps	1000 Mbps	
XR324WG	24	24x RJ45	-	-	-
XR328-4C WG	28 ¹⁾	24x RJ45	Max. 4x RJ45	-	4x SFP992

¹⁾ Of which 4 are combo ports

4.5.19.4 Article numbers

Device	Properties	Power supply	Article number
SCALANCE XR324WG	24x 10/100 Mbps RJ45 ports	2x 24 V DC Connection for the power supply on the front	6GK5324-0BA00-2AR3
		1x 100 to 240 V AC Connection for the power supply on the rear	6GK5324-0BA00-3AR3
SCALANCE XR328-4C WG	24x 10/100 Mbps RJ45 ports 4x 1000 Mbps combo ports electrical or optical (usable either as 10/100/1000 Mbps RJ45 ports or for plug-in transceiver 1000 Mbps)	2x 24 V DC Connection for the power supply on the front	6GK5328-4FS00-2AR3
		1x 100 to 240 V AC Connection for the power supply on the rear	6GK5328-4FS00-3AR3
		2x 24 V DC Connection for the power supply on the front Reduced approvals (no UL/FM approval)	6GK5328-4FS00-2RR3
		1x 100 to 240 V AC Connection for the power supply on the rear Reduced approvals (no UL/FM approval)	6GK5328-4FS00-3RR3
	24x 10/100/1000 Mbps RJ45 ports 4x 1000 Mbps combo ports electrical or optical (usable either as 10/100/1000 Mbps RJ45 ports or for plug-in transceiver 1000 Mbps)	2x 24 V DC Connection for the power supply on the front	6GK5328-4SS00-2AR3
		1x 100 to 240 V AC Connection for the power supply on the rear	6GK5328-4SS00-3AR3

4.5.19.5 Accessories SFP transceiver

Pluggable transceiver SFP (1000 Mbps)

Type	Property	Article number
SFP992-1	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 750 m	6GK5 992-1AL00-8AA0
SFP992-1+	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 2 km	6GK5 992-1AG00-8AA0
SFP992-1LD	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km	6GK5 992-1AM00-8AA0
SFP992-1LD (C)	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km, varnished	6GK5 992-1AM00-8FA0

Type	Property	Article number
SFP992-1LD+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 30 km	6GK5 992-1AM30-8AA0
SFP992-1LH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 40 km	6GK5 992-1AN00-8AA0
SFP992-1LH+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 992-1AP00-8AA0
SFP992-1ELH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 120 km	6GK5 992-1AQ00-8AA0

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Bidirectional plug-in transceiver SFP

Bidirectional plug-in transceivers feature only one fiber connection. They transmit and receive on two different wavelengths. To establish a connection, you need two matching bidirectional SFPs. The connected SFPs must respectively transmit on the wavelength at which the connection partner receives.

Type	Properties	Article number
SFP992-1BXMT	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AL00-8TA0
SFP992-1BXMR	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AL00-8RA0

SFP992 interfaces (1000 Mbps)

Pluggable transceiver	Twisted pair	Fiber-optic cables	
	1000 Mbps	1000 Mbps	Max. segment length / km
SFP992-1	-	1x LC, multimode	0.750
SFP992-1+	-	1x LC, multimode	2
SFP992-1LD SFP992-1LD (C)	-	1x LC, single-mode	10
SFP992-1LH	-	1x LC, single-mode	40
SFP992-1LH+	-	1x LC, single-mode	70
SFP992-1ELH	-	1x LC, single-mode	120
SFP992-1BXMT	-	1x LC, multimode	0.500
SFP992-1BXMR	-	1x LC, multimode	0.500

4.5.20 SCALANCE XM-400

4.5.20.1 Description



Figure 4-25 SCALANCE XM-400

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.

4.5.20.2 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 (2x 24 V DC)	•	•	•
Signaling contact	•	•	•
On site display (Set button)	•	•	•
Console port (1x RS 232)	•	•	•
Out-of-band port for on-site parameterization (1 x RJ45)	•	•	•
C-PLUG slot	•	•	•
Maximum number of port extenders	2	2	1
Maximum number of network interfaces	24	24	24

- 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 assign the IP address using the Primary Setup Tool, the switch must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7
- Command Line Interface / Telnet
- Web Based Management
- SNMP / SNMP-supported diagnostics
- SNTP
- Ring redundancy including RM functionality
- Standby redundancy
- MRP interconnection
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol) as well as RSTP+
- Passive Listening
- Topology support (LLDP)
- VLAN (Virtual Local Area Network)
- GVRP (Generic VLAN Registration Protocol)
- IGMP snooping/querier (Internet Group Management Protocol)
- GMRP (Generic Multicast Protocol)
- Broadcast, Multicast, Unicast limiter
- Broadcast blocking
- DHCP server / DHCP client / DHCP options 66, 67, 82
- Access control list (MAC)
- IEEE 802.1x (Radius)
- Link aggregation
- PROFINET diagnostics

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)

- Multicast routing (PIM-SM, PIM-SSM, PIM-BiDir, MSDP)
- IPv6:
 - Management
 - RIPng
 - OPSFv3
 - VRRPv3

4.5.20.3 Interfaces

Device	Total number of available ports	Twisted pair	Fiber-optic cables	Combo ports 100/1000 Mbps
		10/100/1000 Mbps	1000 Mbps	
XM408-4C	8 ¹⁾	Max. 8x RJ45	-	4x STP/SCP
XM408-8C	8 ²⁾	Max. 8x RJ45	-	8x SFP
XM416-4C	16 ¹⁾	Max. 16x RJ45	-	4x SFP

¹⁾ Of which 4 are combo ports

²⁾ Of which 8 are combo ports

4.5.20.4 Article numbers

Device	Description	Article number
SCALANCE XM408-4C	4x 10/100/1000 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver STP/SCP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); Up to 2 port extenders, Layer 3 integrated via KEY-PLUG	6GK5408-4GP00-2AM2
	4x 10/100/1000 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver STP/SCP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); Up to 2 port extenders, Layer 3 integrated	6GK5408-4GQ00-2AM2
SCALANCE XM408-8C	8x combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); Up to 2 port extenders, Layer 3 via KEY-PLUG	6GK5408-8GS00-2AM2
	8x combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); up to 2 port extenders, Layer 3 integrated	6GK5408-8GR00-2AM2

Device	Description	Article number
SCALANCE XM416-4C	12x 10/100/1000 Mbps RJ45 ports, 4x combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); Max. 1 Port Extender, Layer 3 with KEY-PLUG	6GK5416-4GS00-2AM2
	12x 10/100/1000 Mbps RJ45 ports, 4x combo ports (either usable for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); Max. 1 Port Extender, Layer 3 integrated	6GK5416-4GR00-2AM2

4.5.20.5 Accessories SFP transceiver

Pluggable transceiver SFP (100 Mbps)

Type	Property	Article number
SFP991-1	1 x 100 Mbps, LC port optical for glass FO cable (multimode), up to max. 5 km	6GK5991-1AD00-8AA0
SFP991-1 (C)	1 x 100 Mbps, SC port optical, for glass FO cable (multimode), up to max. 5 km, varnished	6GK5991-1AD00-8FA0
SFP991-1LD	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5991-1AF00-8AA0
SFP991-1LD (C)	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km, varnished	6GK5991-1AF00-8FA0
SFP991-1LH+	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5991-1AE00-8AA0
SFP991-1ELH200	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 200 km	6GK5991-1AE30-8AA0

The SFP plug-in transceiver (100 Mbps) cannot be operated in SFP+ slots.

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Pluggable transceiver SFP (1000 Mbps)

Type	Property	Article number
SFP992-1	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 750 m	6GK5 992-1AL00-8AA0
SFP992-1+	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 2 km	6GK5 992-1AG00-8AA0
SFP992-1LD	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km	6GK5 992-1AM00-8AA0
SFP992-1LD (C)	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km, varnished	6GK5 992-1AM00-8FA0

Type	Property	Article number
SFP992-1LD+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 30 km	6GK5 992-1AM30-8AA0
SFP992-1LH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 40 km	6GK5 992-1AN00-8AA0
SFP992-1LH+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 992-1AP00-8AA0
SFP992-1ELH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 120 km	6GK5 992-1AQ00-8AA0

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Bidirectional plug-in transceiver SFP

Bidirectional plug-in transceivers feature only one fiber connection. They transmit and receive on two different wavelengths. To establish a connection, you need two matching bidirectional SFPs. The connected SFPs must respectively transmit on the wavelength at which the connection partner receives.

Type	Properties	Article number
SFP992-1BXMT	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AL00-8TA0
SFP992-1BXM R	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AL00-8RA0

SFP991 interfaces (100 Mbps)

Pluggable transceiver	Twisted pair	Fiber-optic cables	
	100 Mbps	100 Mbps	Max. segment length / km
SFP991-1 SFP991-1 (C)	-	1x LC, multimode	5*
SFP991-1LD SFP991-1LD (C)	-	1x LC, single-mode	26**
SFP991-1LH+	-	1x LC, single-mode	70
SFP991-1ELH200	-	1x LC, single-mode	200

* With a cable cross-section of 50/125 µm or 62.5/125 µm; attenuation 1 dB/km at 1310 nm; 1200 MHz * km

** With a cable cross-section of 9/125 µm; attenuation ≤ 0.5 dB/km at 1310 nm

Note

Slots for pluggable transceivers of the product group SFP991

The pluggable transceivers SFP991 with a transmission rate of 100 Mbps cannot be used for devices with the letter "G" in the type designation (Gigabit Ethernet) or in the slots for pluggable transceivers of the product groups SFP992 (1000 Mbps) and SFP993 (10 Gbps). When inserting an SFP991 into the wrong slot, the device detects the incorrect usage and reports the error.

SFP992 interfaces (1000 Mbps)

Pluggable transceiver	Twisted pair	Fiber-optic cables	
	1000 Mbps	1000 Mbps	Max. segment length / km
SFP992-1	-	1x LC, multimode	0.750
SFP992-1+	-	1x LC, multimode	2
SFP992-1LD	-	1x LC, single-mode	10
SFP992-1LD (C)	-	1x LC, single-mode	10
SFP992-1LH	-	1x LC, single-mode	40
SFP992-1LH+	-	1x LC, single-mode	70
SFP992-1ELH	-	1x LC, single-mode	120
SFP992-1BXMT	-	1x LC, multimode	0.500
SFP992-1BXMR	-	1x LC, multimode	0.500

4.5.20.6 Extender modules SCALANCE PE-400

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 4-26 Port Extender SCALANCE PE-400

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

Device	Twisted pair	Fiber-optic cables	SFP slots 100/1000 Mbps
	10/100/1000 Mbps	1000 Mbps	
PE408	8x RJ45	-	-
PE408PoE	8x RJ45 ¹⁾	-	-
PE400-8SFP	-	-	8x SFP

1) PoE connections; separate supply of PoE voltage via two PoE input ports required

Article numbers

Device	Description	Article number
SCALANCE PE408	8 x 10/100/1000 Mbps RJ-45 ports	6GK5408-0GA00-8AP2
SCALANCE PE408PoE	8 x 10/100/1000 Mbps, RJ-45 ports with PoE	6GK5408-0PA00-8AP2
SCALANCE PE400-8SFP	8 x 100/1000 Mbps, SFP ports	6GK5400-8AS00-8AP2

4.5.20.7 External power supply units SCALANCE PS-900PoE



Figure 4-27 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

4.5 SCALANCE X Industrial Ethernet Switches

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.

Features

	SCALANCE PS9230 PoE	SCALANCE PS924 PoE
Input voltage	85 ... 264 VAC at 47 ... 63 Hz	19.2 ... 28.8 VDC
Output voltage	48 ... 54 VDC, can be set	
Output effective power	86 W	
Effective power loss	14 W	
Diagnostics LED	•	•
Signaling contact	•	•

Interfaces

Electrical connectors		SCALANCE PS9230 PoE	SCALANCE PS924 PoE
Power supply	At the input	FE / + / - screw terminals 0.5 - 2.5 mm ²	IEC plug
	At the input	2x + / 2x -, screw terminals 0.5 - 2.5 mm ²	2x + / 2x -, screw terminals 0.5 - 2.5 mm ²
Signaling contact		2 screw terminals 0.5-2.5 mm ²	

Article numbers

Device	Description	Article number
SCALANCE PS9230 PoE	PoE power supply for SCALANCE PE408PoE with 230 V AC input voltage	6GK5923-0PS00-3AA2
SCALANCE PS924 PoE	PoE power supply for SCALANCE PE408PoE with 24 V DC input voltage	6GK5924-0PS00-1AA2

4.5.21 SCALANCE XR-500

4.5.21.1 Description



Figure 4-28 SCALANCE XR-500

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.

4.5.21.2 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:

- Configuration with the Primary Setup Tool (PST) V3 or higher; to use the Primary Setup Tool to assign the IP address, the switches must be accessible via Ethernet.
- Configuration of the IP address with DHCP
- Configuration with STEP 7
- Command Line Interface
- Web Based Management
- SNMP / SNMP-supported diagnostics
- SNTP
- Ring redundancy including RM functionality
- Standby redundancy
- MRP interconnection
- STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol) as well as RSTP+
- Passive Listening
- Topology support (LLDP)
- VLAN (Virtual Local Area Network)
- GVRP (Generic VLAN Registration Protocol)
- IGMP snooping/querier (Internet Group Management Protocol)

- GMRP (Generic Multicast Protocol)
- Broadcast, Multicast, Unicast limiter
- Broadcast blocking
- DHCP server / DHCP client / DHCP options 66, 67, 82
- 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)
- PROFINET diagnostics
- Multicast routing (PIM-SM, PIM-SSM, PIM-BiDir, MSDP)
- IPv6:
 - Management
 - RIPv6
 - OPSFv3
 - VRRPv3

4.5.21.3 Interfaces

Device	Total number of available ports	Twisted pair	Fiber-optic cables	Combo ports	SFP slots	Slots for 4-port media modules
		10/100/1000 Mbps	1000 Mbps	100/1000 Mbps	1/10 Gbps	100/1000 Mbps
XR524-8C	24 ¹⁾	Max. 24x RJ45	-	8x SFP	-	-
XR526-8C	26 ¹⁾	Max. 24x RJ45	-	8x SFP	2x SFP+	-
XR528-6M	28	-	-	-	4x SFP+	6
XR552-12M	52	-	-	-	4x SFP+	12

¹⁾ of which 8 are combo ports

4.5.21.4 Article numbers

Device	Properties	Layer 3	Power supply	Article number
SCALANCE XR524-8C	1 height unit; 16x 10/100/1000 Mbps RJ45 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

4.5 SCALANCE X Industrial Ethernet Switches

Device	Properties	Layer 3	Power supply	Article number
	8x combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports)	Integrated	2 x 100 to 240 VAC Connectors on rear	6GK5524-8GS00-4AR2
			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
SCALANCE XR526-8C	1 height unit; 16x 10/100/1000 Mbps RJ45 ports, 8x combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports) 2x 10 Gbps SFP+ transceiver	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
SCALANCE XR528-6M	2 height units; 4x 1/10 Gbps SFP+slots, 6x 100/1000 Mbps slots for 4-port media modules (depending on the plugged media module: electrical, electrical PoE or optical)	KEY-PLUG	Front	6GK5528-0AA00-2AR2
			Back	6GK5528-0AA00-2HR2
		Integrated	Front	6GK5528-0AR00-2AR2
			Back	6GK5528-0AR00-2HR2
SCALANCE XR552-12M	3 height units; 4x 1/10 Gbps SFP+slots, 12x 100/1000 Mbps slots for 4 port media modules (depending on the plugged media module: electrical, electrical PoE or optical)	KEY-PLUG	Front	6GK5552-0AA00-2AR2
			Back	6GK5552-0AA00-2HR2
		Integrated	Front	6GK5552-0AR00-2AR2
			Back	6GK5552-0AR00-2HR2

4.5.21.5 Media modules and SFP transceivers

Media modules

Component	Twisted pair	Fiber-optic cables			1 port SFP slots
	10/100/1000 Mbps	100 Mbps	1000 Mbps	Max. segment length / km	100/1000 Mbps
MM991-4	-	4x BFOC, multimode	-	4* / 5**	-
MM991-4LD	-	4x BFOC, single-mode	-	26	-
MM992-4	-	-	4x SC, multimode	0.75	-
MM992-4LD	-	-	4x SC, single-mode	10	-
MM992-4SFP	-	-	-	-	4x LC
MM992-4CUC	4x RJ45 ¹⁾	-	-	-	-
MM992-4CU	4x RJ45	-	-	-	-
MM992-4PoEC	4x RJ45 ^{1) 2)}	-	-	-	-
MM992-4PoE	4x RJ45 ²⁾	-	-	-	-

* With a cable cross-section of 50 µm

** With a cable-cross section of 62.5 µm

¹⁾ Securing collar

²⁾ PoE connections

SFP transceiver

The SFP transceiver (Small Form-factor Pluggable) can be used only in conjunction with the SFP media module MM992-4SFP.

Component	Fiber-optic cables			
	100 Mbps	1000 Mbps	10 000 Mbps	Max. segment length / km
SFP991-1 ¹⁾ SFP991-1 (C) ¹⁾	1x LC, multimode	-	-	4* / 5**
SFP991-1LD ¹⁾ SFP991-1LD (C) ¹⁾	1x LC, single-mode	-	-	26
SFP991-1LH+ ^{1) 2)}	1x LC, single-mode	-	-	70
SFP991-1ELH200 ¹⁾	1x LC, single-mode	-	-	200
SFP992-1BXM	-	1x LC, multimode	-	0.500
SFP992-1BXT	-	1x LC, multimode	-	0.500
SFP992-1 ^{1) 2)}	-	1x LC, multimode	-	0.750
SFP992-1+ ^{1) 2)}	-	1x LC, multimode	-	2
SFP992-1LD ^{1) 2)} SFP992-1LD (C) ^{1) 2)}	-	1x LC, single-mode	-	10
SFP992-1LH ^{1) 2)}	-	1x LC, single-mode	-	40
SFP992-1LH+ ^{1) 2)}	-	1x LC, single-mode	-	70

Component	Fiber-optic cables			
	100 Mbps	1000 Mbps	10 000 Mbps	Max. segment length / km
SFP992-1ELH ^{1) 2)}		1x LC, single-mode	-	120
SFP993-1 ²⁾	-	-	1x LC, multimode	0.300
SFP993-1LD ²⁾		-	1x LC, single-mode	10
SFP993-1LH ²⁾	-	-	1x LC, single-mode	40

* With a cable cross-section of 50 µm

** With a cable-cross section of 62.5 µm

1) Only pluggable in combination with SFP shaft module MM992-4SFP

2) Only pluggable in integrated XR-500 SFP+ slots

4.5.21.6 External power supply unit SCALANCE PS598-1

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 4-29 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 pad use the material Viledon P 15/150 G2 EN 779. The dimensions of the filter pad are 38 x 135 x 8 mm (H x W x D).

Article numbers

Device	Description	Article number
SCALANCE PS598-1	Power supply 300 W input: 85 to 264 V AC cold-device connector; output: 24 V DC terminals or for direct connection to SCALANCE XR-500	6GK5598-1AA00-3AA0

4.6 SCALANCE W components for the Industrial Wireless LAN

4.6.1 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), KEY-PLUG and CLP (Configuration License 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 or CLP iFeatures activates further device properties (known as "iFeatures").

4.6 SCALANCE W components for the Industrial Wireless LAN

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

- 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 with the 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 their functionality is restricted to that of a client.

- Direct Access Points

The direct access points have integrated controller functions and allow for centralized management of up to 128 access points. They are designed according to the IWLAN standard IEEE 802.11ac Wave 2 and are used wherever only very high data rates are required.

- 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 can also be configured as client modules.

Overview of the performance classes of the SCALANCE W devices

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

	Client Modules				Access Points				Access Points with integrated Management
					also configurable as Client Modules				
	SCALANCE								
	W720	W730	W740	W1740	W760	W770	W780	W1780	W1750D
For enhanced environmental conditions									
For outdoor use									
For production hall mounting									
For use in control cabinet									
For moderate environment									
iFeatures (optional)	•	•	•	•*		•	•	•*	

G_IK10_XX_30311
* iPRP available

Figure 4-30 SCALANCE W access points and clients according to IEEE 802.11n/ac

Example of a topology

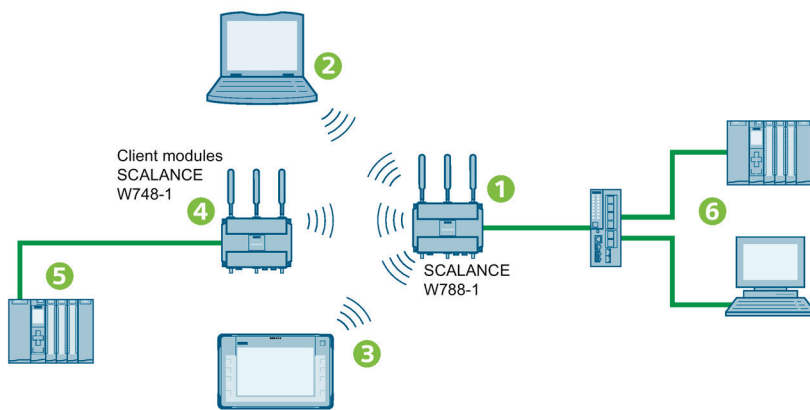


Figure 4-31 Example of an infrastructure network:
A SCALANCE W788 ① adopts the function of the access point. Mobile nodes such as PC/PG with IWLAN card ②, IWLAN control panels ③ or WLAN clients ④ and their nodes ⑤ can communicate with each other or exchange data with stationary nodes ⑥.

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.

4.6.2 Type designations

The design and basic properties of a SCALANCE W device can be identified based on the following type key:

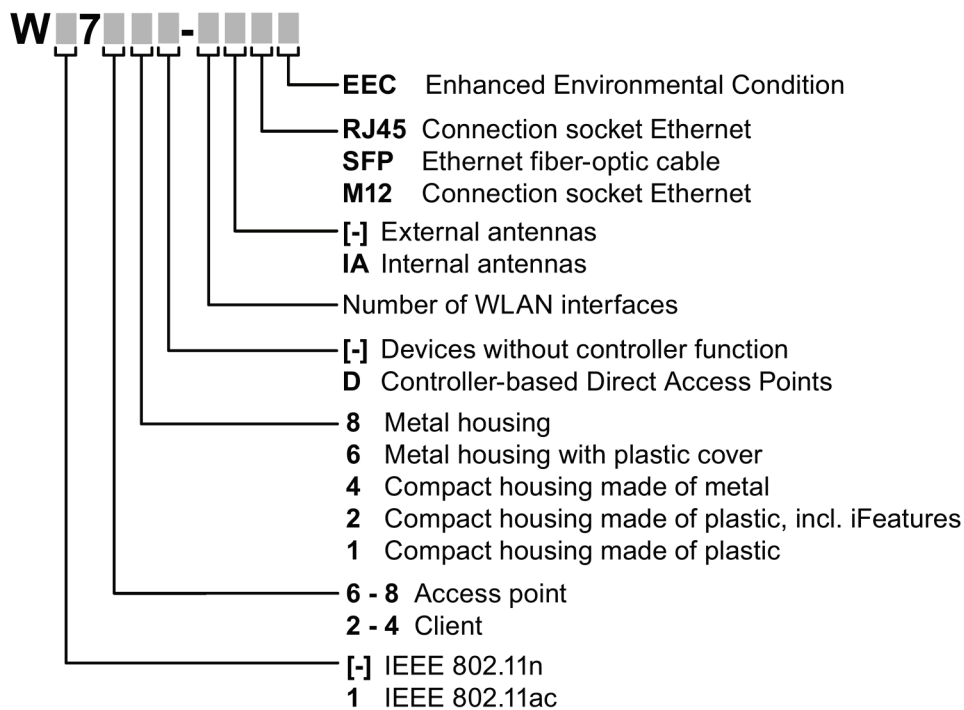


Figure 4-32 Type designations of the SCALANCE W devices complying with IEEE 802.11n/ac

4.6.3 IEEE 802.11r

During roaming, the WLAN client roams from one access point to the next. A delay time of several 100 ms can come about at the connection transition.

The following steps can be executed during this time:

- Client searches for a new access point (scanning)
- Logon at a new access point (authentication and association)
- Allow a data connection via the new access point

Shorter delay times are required for time-critical applications, for example, Voice over IP. The standard IEEE 802.11r contains amendments which optimize roaming and therefore is also referred to as Fast BSS Transition (FT).

With FT, the WLAN client must not authenticate every time the access point changes. For this purpose, the access points are grouped into a mobility domain. The WLAN client receives the mobility domain ID from the first access point to which it logs on. The log-on information is buffered within the mobility domain. This logon is valid for all members of the mobility domain.

Based on the ID, the WLAN client recognizes whether the access point is a member of the same mobility domain and can therefore log on without delay. Only WLAN clients with IEEE 802.11r support can use the improved roaming or handover functions.

Requirement

- The access points are members of the same mobility domain
- Only possible with WPA2 encryption (WPA2-PSK and WPA2 RADIUS)

See also

Web Based Management for configuring networks (Page 131)

4.6.4 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 W configuration manuals and in the section "Encryption and data security (Page 58)".

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. Detailed information is available in the section "IEEE 802.11n/ac". These devices also support the following functions:

- Single-User MIMO
- Spatial multiplexing
- Reduced guard interval

- Frame aggregation
- Channel bonding

Support of IEEE 802.11ac

The SCALANCE W1700 devices support the IEEE 802.11ac standard. The data throughput for these devices is up to 1733 Mbps. Detailed information is available in the section "IEEE 802.11n/ac (Page 209)". These devices also support the following functions:

- Multi-User MIMO
- Spatial multiplexing
- Shortened guard interval
- Frame aggregation
- Channel bonding
- Channel width up to 160 MHz

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 and are available, depending on the version, for the SCALANCE W devices via the KEY-PLUG or CLP.

- **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. In addition, wireless and security-related PROFINET IO communication via PROFISAFE is supported.

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

The IPCF-MC function 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. Unlike with IPCF, with IPCF-MC the time for a roaming procedure does not increase with multiple used WLAN channels.

- **IPCF-HT: IPCF High Throughput**

The IPCF-HT function must be used for a higher data throughput for IPCF. With this you can, for example, also transfer video data in addition to PROFINET. Individual data packets for the same receiver station (client) with the same prioritization are bundled into a large data packet and transferred via frame bursting (A-MPDU). Prerequisite is an optimal HF environment such as in a slotted hollow conductor.

- **iPRP: industrial Parallel Redundancy Protocol**

iPRP ensures high availability of the wireless communication through the setup of redundant structures.

- **iREF: industrial Range Extension Function (only for access points)**

iREF ensures that the data traffic from the access point to each individual client is handled via the most suitable antenna. The access point determines the suitable antenna on the basis of the RSSI values of received packets.

- **AeroScout (only for access points)**

The devices support tags of the AeroScout company. Tags are battery-operated RFID sensors that send their data cyclically as multicast frames. For more detailed information, refer to the documentation of the AeroScout company (www.aeroscout.com).

- **Inter AP blocking (only for access points)**

With Inter AP-Blocking the access point restricts the communication of the clients connected to it.

- **PROFINET Transparent mode**

Even if NAT is used, you can make individual PROFINET nodes visible again to the outside. Frames are also forwarded transparently. The exceptions are made by means of the PROFINET device names.

4.6.5 IEEE 802.11n/ac

Overview

The IEEE 802.11ac standard is a further development of the IEEE 802.11n standard and is downward compatible with the standards IEEE 802.11a, IEEE 802.11h and IEEE 802.11n. The mechanisms of the PHY and MAC layer implemented in the IEEE 802.11n standard have been improved.

The following table contains the most important differences.

	IEEE 802.11n	IEEE 802.11ac
Frequency band	2.4 GHz and 5 GHz	5 GHz
Channel bandwidth	20 MHz, 40 MHz	20 MHz, 40 MHz, 80 MHz Optional: 160 MHz
Spatial streams (data streams)	1 to 4	1 to 8 Up to 4 per client
MIMO	Single-User MIMO	Multi-User MIMO
Modulation scheme	OFDM (BPSK, QPSK, 16-QAM, 64-QAM)	OFDM (BPSK, QPSK, 16-QAM, 64-QAM, 128-QAM, optional 256-QAM)

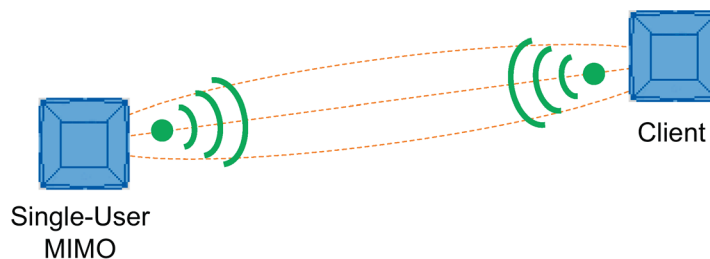
MIMO antenna technology

MIMO (Multiple Input - Multiple Output) is based on an intelligent multiple antenna system. The transmitter and the receiver have several spatially separate antennas. These separated antennas transmit the data streams (spatial streams) at the same time. Up to four data streams are possible with IEEE 802.11n and up to eight data streams with IEEE 802.11ac.

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. The specific characteristics of each sender enable the recipient to separate several signals from each other.

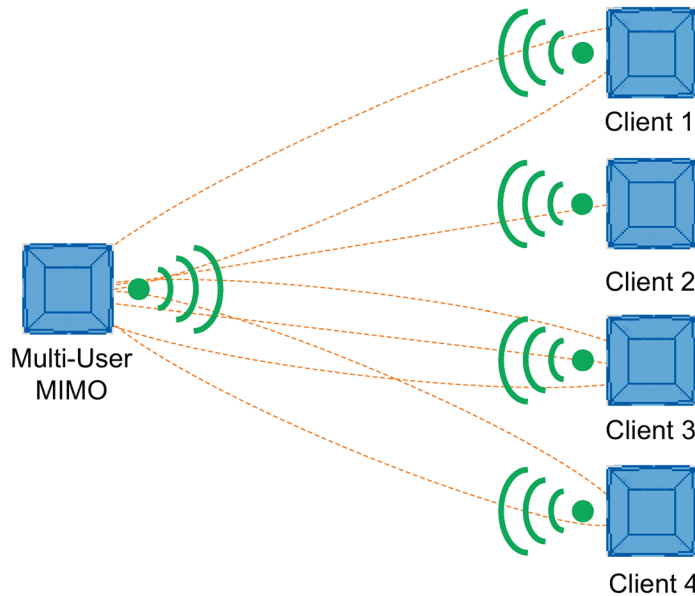
Single-User MIMO

With Single-User MIMO, the same frame is sent over multiple data streams to a single WLAN client. A single-user MIMO can operate up to four devices alternately, but only one device at a time.



Multi-User MIMO

With multi-user MIMO, multiple frames are sent simultaneously to different multi-user MIMO clients over the same frequency range. A multi-user MIMO therefore supplies up to four multi-user MIMO clients with data simultaneously.



Spatial mutliplexing

With spatial multiplexing, different information is sent using the same frequency. The data stream is distributed over n transmitting antennas; in other words, each antenna sends only $1/n$ of the data stream. The division of the data stream is restricted by the number of antennas. The signal is reconstructed at the receiver end. Due to the spatial multiplexing, there is a higher signal-to-noise ratio and a higher data throughput.

Accelerated guard interval

The guard interval prevents different transmissions being mixed together. In telecommunications, this mixing is also known as intersymbol interference (ISI). When the send time has elapsed, a send pause (guard interval) must be kept to before the next transmission begins.

The guard interval of IEEE 802.11a /b/g is 800 ns. IEEE 802.11n/ac can use the reduced guard interval of 400 ns. You specify the guard interval on the WBM page "AP 802.11n/ac (Page 131)".

Frame aggregation

With IEEE 802.11n/ac, it is possible to bundle together individual frames to form one larger frame, a process referred to as frame aggregation. There are two types of frame aggregation:

- Aggregated MAC Service Data Unit (A-MSDU)

Multiple MSDU frames with the same destination address are bundled and sent as one A-MSDU. This reduces the network load. Due to their shorter maximum length, A-MSDUs are mainly suitable for bundling several shorter frames.

- Aggregated MAC Protocol Data Unit (A-MPDU)

Multiple MPDU frames with the same destination address are bundled and sent as one large A-MPDU. This allows the total throughput to be increased.

The SCALANCE W devices support both types of frame aggregation. You make the settings on the WBM page "AP 802.11n/ac".

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.

4.6.6 SCALANCE W760/W720

4.6.6.1 Description



Figure 4-33 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

4.6.6.2 Features and functions

Features

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

Functionality	W761-1 RJ45 W722-1 RJ45 W721-1 RJ45
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

4.6 SCALANCE W components for the Industrial Wireless LAN

- 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
- iPCF-HT
- iPRP

4.6.6.3 Interfaces

Functionality	W761-1 RJ45 W721-1 RJ45 W722-1 RJ45
Number of wireless interfaces	1
Connectors for external antennas	1x R-SMA connector female
Number and type of the Ethernet interfaces	1x RJ45

4.6.6.4 Article numbers

Access points

Device	Description	Article number
SCALANCE W761-1 RJ45	Ethernet interface RJ45, 1x R-SMA antenna connections	6GK5761-1FC00-0AA0 6GK5761-1FC00-0AB0 ¹⁾

¹⁾ US variant

Clients

Device	Description	Article number
SCALANCE W721-1 RJ45	Ethernet interface RJ45, 1x R-SMA antenna connections	6GK5721-1FC00-0AA0 6GK5721-1FC00-0AB0 ¹⁾
SCALANCE W722-1 RJ45	Ethernet interface RJ45, 1x R-SMA antenna connections	6GK5722-1FC00-0AA0 6GK5722-1FC00-0AB0 ¹⁾ 6GK5722-1FC00-0AC0 ²⁾

¹⁾ US variant

²⁾ Israel variant

4.6.7 SCALANCE W774/W734**4.6.7.1 Description**

Figure 4-34 SCALANCE W774-1 M12 EEC

The SCALANCE W774/W734 devices have a metal housing in SIMATIC S7-1500 and ET 200MP design and are designed 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 RJ45 Client module

4.6.7.2 Features and functions

Features

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

Functionality	W774-1 RJ45 W734-1 RJ45	W774-1 M12 EEC
PoE (Power over Ethernet) according to 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	-30 °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 (only in client mode)
- iPCF-HT
- iPRP
- iREF (only in access point mode)
- AeroScout (only in Access Point mode)
For more detailed information on this, please refer to the documentation of the AeroScout company (www.aeroscout.com).

4.6.7.3 Interfaces

Functionality	W774-1 RJ45 W734-1 RJ45	W774-1 M12 EEC
Number of wireless interfaces	1	1
Connectors for external antennas	2x R-SMA connector female	2x R-SMA connector female
Number and type of Ethernet interface	2x RJ45	2x M12

4.6.7.4 Article numbers

Access points

Device	Description	Article number
SCALANCE W774-1 RJ45	Ethernet interface RJ45, 2x R-SMA antenna connections	6GK5774-1FX00-0AA0 6GK5774-1FX00-0AB0 ¹⁾ 6GK5774-1FX00-0AC0 ²⁾
SCALANCE W774-1 M12 EEC	Ethernet interface M12, 2x R-SMA antenna connections	6GK5774-1FY00-0TA0 6GK5774-1FY00-0TB0 ¹⁾

- ¹⁾ US variant
²⁾ Israel variant

Clients

Device	Description	Article number
SCALANCE W734-1 RJ45	Ethernet interface RJ45, 2x R-SMA antenna connections	6GK5734-1FX00-0AA0 6GK5734-1FX00-0AB0 ¹⁾

- ¹⁾ US variant

4.6.8 SCALANCE W778/W738

4.6.8.1 Description



Figure 4-35 SCALANCE W778/W738

The access point and client devices of the SCALANCE W778/W738 product group are designed for easy and cost-effective wireless machine networking. They support the IEEE 802.11n standard and use the 2 x 2 Single-User MIMO antenna technology that reaches a data transmission speed of up to 300 Mbps. A redundant power supply and the PoE connection is part of the standard equipment of the devices. The devices are therefore suitable for applications with high requirements on reliability. iFeatures can be added with the optionally available KEY-PLUG; real-time data transfer will then also be possible.

All devices have a shock- and vibration-resistant aluminum housing with screwed connections. The devices can therefore be used in areas of application with high requirements on mechanical stability.

The devices are designed in IP65 degree of protection for the installation without cabinets and can be directly mounted on a standard DIN rail or directly on the wall.

The EEC variants have coated PCBs and can be used in extended temperature ranges as well as in railway applications.

The following variants exist:

- SCALANCE W778-1 M12
Access Point
- SCALANCE W778-1 M12 EEC
Access point with coated PCBs
- SCALANCE W738-1 M12
Client

4.6.8.2 Features and functions

Features

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

Table 4- 4

Functionality	W778-1 M12 W738-1 M12	W778-1 M12 EEC
PoE (Power over Ethernet) according to IEEE 802.3at Type 1, previously IEEE 802.3af	•	•
Redundant power supply	•	•
Digital input / digital output	-	-
PLUG slot	•	•
IP degree of protection	IP65	IP65
Operating temperature minimum	-20 °C	-30 °C
Operating temperature maximum	+60 °C	+75 °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 manageable IP addresses in the client	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)

4.6 SCALANCE W components for the Industrial Wireless LAN

- VLANs (Multi-SSID)
- PROFINET IO diagnostics
- SNMP
- Syslog

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

- iPCF
- iPCF-MC (only in client mode)
- iPCF-HT
- iPRP
- iREF (only in access point mode)
- AeroScout (only in access point mode)

For more detailed information on this, please refer to the documentation of the AeroScout company (www.aeroscout.com).

4.6.8.3 Interfaces

Functionality	W778-1 M12 W778-1 M12 EEC W738-1 M12
Number of wireless interfaces	1
Connectors for external antennas	2x N-Connect socket
Number and type of Ethernet interface	2x M12

4.6.8.4 Article numbers

Access points

Device	Description	Article number
SCALANCE W778-1 M12	Ethernet interface M12, 2x N-Connect antenna connections	6GK5778-1GY00-0AA0 6GK5778-1GY00-0AB0 ¹⁾
SCALANCE W778-1 M12 EEC	Ethernet interface M12, 2x N-Connect antenna connections	6GK5778-1GY00-0TA0 6GK5778-1GY00-0TB0 ¹⁾

¹⁾ US variant

Clients

Device	Description	Article number
SCALANCE W738-1 M12	Ethernet interface M12, 2x N-Connect antenna connections	6GK5738-1GY00-0AA0 6GK5738-1GY00-0AB0 ¹⁾

¹⁾ US variant

4.6.9 SCALANCE W786

4.6.9.1 Description



Figure 4-36 SCALANCE W786 access point

The SCALANCE W786 devices 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.

4.6.9.2 Features and functions

Features

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

	W786-1 RJ45 W786-2 RJ45 W786-2IA RJ45	W786-2 SFP
PoE (Power-over-Ethernet) according to 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

	W786-1 RJ45 W786-2 RJ45 W786-2IA RJ45	W786-2 SFP
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⁾ Observe 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
- iPRP

- iREF (only in access point mode)
- AeroScout (only in access point mode)
For more detailed information on this, please refer to the documentation of the AeroScout company (www.aeroscout.com).

4.6.9.3 Interfaces

	W786-1 RJ45	W786-2 RJ45	W786-2 SFP	W786-2IA RJ45
Number of wireless interfaces	1	2	2	2
Connectors for external antennas	3	6	6	-
Internal antennas	-	-	-	6
Type and number of Ethernet interfaces	1x RJ45	1x RJ45	2x SFP	1x RJ45

4.6.9.4 Article numbers

Access points

Device	Description	Article number
SCALANCE W786-1 RJ45	Ethernet interface RJ45, 3x external antennas	6GK5786-1FC00-0AA0 6GK5786-1FC00-0AB0 ¹⁾
SCALANCE W786-2 RJ45	Ethernet interface RJ45, 6x external antennas	6GK5786-2FC00-0AA0 6GK5786-2FC00-0AB0 ¹⁾ 6GK5786-2FC00-0AC0 ²⁾
SCALANCE W786-2IA RJ45	Ethernet interface RJ45, 6x internal antennas	6GK5786-2HC00-0AA0 6GK5786-2HC00-0AB0 ¹⁾
SCALANCE W786-2 SFP	SFP slot, 6x external antennas	6GK5786-2FE00-0AA0 6GK5786-2FE00-0AB0 ¹⁾

¹⁾ US variant

²⁾ Israel variant

4.6.10 SCALANCE W788/W748

4.6.10.1 Description



Figure 4-37 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/ac (Page 209) 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.

4.6.10.2 Features and functions

Features

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

	W788-1 RJ45 W788-2 RJ45 W748-1 RJ45	W788-1 M12 W788-2 M12 W748-1 M12	W788-2 M12 EEC
PoE (Power-over-Ethernet) according to IEEE 802.3at Type 1, previously IEEE 802.3af.	•	•	•
Redundant power supply	•	•	•
Digital input / digital output (DI/DO)	•	-	-
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)

4.6 SCALANCE W components for the Industrial Wireless LAN

- 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
- iPRP
- iREF (only in access point mode)
- AeroScout (only in access point mode)

For more detailed information on this, please refer to the documentation of the AeroScout company (www.aeroscout.com).

4.6.10.3 Interfaces

	W788-1 RJ45 W748-1 RJ45	W788-2 RJ45	W788-1 M12 W748-1 M12	W788-2 M12 W788-2 M12 EEC
WLAN interface	1x RJ45	2x RJ45	1x M12	2x M12
Internal antennas	-	-	-	-
Connectors for external antennas	3x R-SMA female	6x R-SMA female	3x N-Connect female	6x N-Connect female
Connector for 10/100/1000 Mbps Ethernet with PoE according to IEEE 802.3at	1x RJ45	1x RJ45	1x M12 (X-coded)	1x M12 (X-coded)

4.6.10.4 Article numbers

Access points

Device	Description	Article number
SCALANCE W788-1 RJ45	Ethernet interface 1x RJ45 max. 1 Gbps, PoE 1x integral wireless card 3x R-SMA antenna connections	6GK5788-1FC00-0AA0 6GK5788-1FC00-0AB0 ¹⁾
SCALANCE W788-2 RJ45	Ethernet interface RJ45 max. 1 Gbps, PoE 2x integral wireless cards 6x R-SMA antenna connections	6GK5788-2FC00-0AA0 6GK5788-2FC00-0AB0 ¹⁾ 6GK5788-2FC00-0AC0 ²⁾
SCALANCE W788-1 M12	Ethernet interface 1x M12 max. 1 Gbps, PoE 1x integral wireless card 3x N-Connect female	6GK5788-1GD00-0AA0 6GK5788-1GD00-0AB0 ¹⁾

4.6 SCALANCE W components for the Industrial Wireless LAN

Device	Description	Article number
SCALANCE W788-2 M12	Ethernet interface 1x M12 max. 1 Gbps, PoE 2x integral wireless cards 6x N-Connect female, antenna connections	6GK5788-2GD00-0AA0 6GK5788-2GD00-0AB0 ¹⁾
SCALANCE W788-2 M12 EEC	Ethernet interface 1x M12 max. 1 Gbps, PoE 2x integral wireless cards 6x N-Connect female, antenna connections	6GK5788-2GD00-0TA0 6GK5788-2GD00-0TB0 ¹⁾

¹⁾ US variant

²⁾ Israel variant

Clients

Device	Description	Article number
SCALANCE W748-1 RJ45	Ethernet interface 1x RJ45 max. 1 Gbps, PoE 3x R-SMA antenna connections	6GK5748-1FC00-0AA0 6GK5748-1FC00-0AB0 ¹⁾
SCALANCE W748-1 M12	Ethernet interface 1x M12 max. 1 Gbps, PoE 3x N-Connect female	6GK5748-1GD00-0AA0 6GK5748-1GD00-0AB0 ¹⁾

¹⁾ US variant

4.6.11 SCALANCE W1788/W1748

4.6.11.1 Description



Figure 4-38 SCALANCE W1700

4.6 SCALANCE W components for the Industrial Wireless LAN

The access points and client devices of the SCALANCE W1700 product line support the IEEE 802.11ac standard. These devices are intended to set up Industrial Wireless LAN (IWLAN) wireless networks for 5 GHz. You use the 4 x 4 Multi-User MIMO technology (Multiple Input Multiple Output) and Wave 2 that let you reach transmission speeds of up to 1733 Mbps (gross). The access points are equipped with two M12 ports for Gigabit Ethernet; one of them can be used as a PoE port according to IEEE 802.3at Type 2.

The devices are suitable for installation outside the control cabinet. The following types of installation are possible: Installation on standard DIN rail, on the S7-300 and S7-1500 standard rail or directly on the wall. The devices have a rugged metal enclosure in IP65 degree of protection with connection jacks for bolted or locked plug-in connectors and thus fulfil the requirements when it comes to mechanical stability through shock and vibration. The EEC variant of the device has coated PCBs (conformal coating) and is suitable for use at ambient temperatures of -40 °C to +75 °C and in the railway environment.

The devices with connections to external antennas are equipped with 4 or 8 N-Connect jacks for directly mounted and detached antennas. For SCALANCE W1788-2IA, the 8 MIMO antennas are inside the housing.

All devices have a slot for the optional CLP with which additional functions can be enabled.

4.6.11.2 Features and functions

Features

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

	W1788-1 M12 W1788-2 M12 W1788-2IA W1748-1 M12	W1788-2 M12 EEC
PoE (Power-over-Ethernet) according to IEEE 802.3at Type 1, previously IEEE 802.3af.	•	•
Redundant power supply	•	•
Digital input / digital output	-	-
CLP / KEY-PLUG slot	•	•
IP degree of protection	IP65	IP65
Operating temperature minimum	-20 °C	-40 °C
Operating temperature maximum	+70 °C	+75 °C
Resistant to condensation	-	•
Resistant to salt water spray	-	-
UV resistant	-	-
Conformal coating	-	•
Railway approval	-	•
Use in EX Zone 2 ¹⁾	•	•

	W1788-1 M12 W1788-2 M12 W1788-2IA W1748-1 M12	W1788-2 M12 EEC
IEEE 802.11ac	•	•
IEEE 802.11ac MU-MIMO (Input x Output Streams)	4 x 4	4 x 4

- Suitable / available or according to the specified standard
¹⁾ Observe 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
- Support of forced roaming
- VLANs (Multi-SSID)

The access points also have the following functions:

- IEEE 802.11e (QoS/WMM)
- STP / RSTP (IEEE 802.1d/w)
- WDS (Wireless Distribution System)
- Operation possible as IWLAN client

With the optionally available CLP, the following function can be used:

- iPRP

4.6.11.3 Interfaces

	W1788-1 M12	W1788-2 M12 W1788-2 M12 EEC	W1788-2IA M12	W1748-1 M12
WLAN interface	1x M12	2x M12	2x M12	1x M12
Internal antennas	-	-	8x	-

4.6 SCALANCE W components for the Industrial Wireless LAN

	W1788-1 M12	W1788-2 M12 W1788-2 M12 EEC	W1788-2IA M12	W1748-1 M12
Connectors for external antennas	4x N-Connect female	8x N-Connect female	-	4x N-Connect female
Connector for 10/100/1000 Mbps Ethernet with PoE according to IEEE 802.3at	2x M12 (X-coded)	2x M12 (X-coded)	2x M12 (X-coded)	2x M12 (X-coded)

4.6.11.4 Article numbers

Access points

Device	Description	Article number
SCALANCE W1788-1 M12	2x M12 Ethernet interfaces, max. 1 Gbps, PoE 1x integral wireless card 4x N-Connect female antenna connections	6GK5788-1GY01-0AA0 6GK5788-1GY01-0AB0 ¹⁾
SCALANCE W1788-2 M12	2x M12 Ethernet interfaces, max. 1 Gbps, PoE 2x integral wireless cards 8x N-Connect female antenna connections	6GK5788-2GY01-0AA0 6GK5788-2GY01-0AB0 ¹⁾
SCALANCE W1788-2 M12 EEC	2x M12 Ethernet interfaces, max. 1 Gbps, PoE 2x integral wireless cards 8x N-Connect female antenna connections	6GK5788-2GY01-0TA0 6GK5788-2GY01-0TB0 ¹⁾
SCALANCE W1788-2IA M12	2x M12 Ethernet interfaces, max. 1 Gbps, PoE 2x integral wireless cards 8x internal antennas	6GK5788-2HY01-0AA0 6GK5788-2HY01-0AB0 ¹⁾

¹⁾ US variant

Clients

Device	Description	Article number
SCALANCE W1748-1 M12	2x M12 Ethernet interfaces, max. 1 Gbps, PoE 1x integral wireless card 4x N-Connect female antenna connections	6GK5748-1GY01-0AA0 6GK5748-1GY01-0AB0 ¹⁾

¹⁾ US variant

4.6.12 SCALANCE W1750D

4.6.12.1 Description



Figure 4-39 SCALANCE W1750D

The controller-based SCALANCE W1750D Direct Access Point supports the IEEE 802.11ac Wave 2 standard. The device includes a virtual controller and is suitable for centralized management of up to 128 access points. The device uses the 4 x 4 Multi-User MIMO antenna technology that allows data transmission at speeds of up to 1733 Mbps (gross).

The device has two installed wireless cards and 8 internal antennas. It offers two Gigabit Ethernet interfaces, one of them can be used with PoE.

The device can be installed to the wall or ceiling without any problems by using the included bracket. Thanks to its discreet and unobtrusive design it can be optimally integrated into any room concept.

4.6.12.2 Features and functions

Features

The device has the characteristics shown in the following table:

	W1750D-2IA RJ45
Number of supported access points	128
PoE (Power-over-Ethernet) according to IEEE 802.3at Type 1, previously IEEE 802.3af.	•
Redundant power supply	-
Digital input / digital output	-
C-PLUG/KEY-PLUG slot	-
USB 2.0 Type A	•
IP degree of protection	IP20
Operating temperature minimum	0 °C

	W1750D-2IA RJ45
Operating temperature maximum	+50 °C
Resistant to condensation	-
Resistant to salt water spray	-
UV resistant	-
Conformal coating	-
Railway approval	-
Use in EX Zone 2 ¹⁾	-
IEEE 802.11ac	●
IEEE 802.11ac MIMO (Input x Output Streams)	4 x 4

- Suitable / available or according to the specified standard

Functions

The device has the following functions:

- CLI
- SSH / HTTPS / admin password
- WEP / WPA / WPA2
- IEEE 802.11i, Hidden SSID
- IEEE 802.1x (radius)
- EAP-TLS, EAP-TTLS, PEAP
- VLANs (Multi-SSID)
- SNMP
- Syslog
- DHCP client
- Spanning Tree Protocol (STP)
- LLDP
- IGMP Snooping/Querier (Internet Group Management Protocol)
- Broadcast / Multicast
- Access Control List (ACL), MAC and IP-based
- Link aggregation
- Support of Fast Roaming
- IEEE 802.11e (QoS/WMM)

4.6.12.3 Interfaces

	W1750D-2IA RJ45
WLAN interface	2
Internal antennas	8
Connections for external antennas	-
Ethernet interface 10/100/1000 Mbps	2x RJ45
Connection PoE according to IEEE 802.3af / 802.3at for Type 1	1x 48 V DC
Power supply connection	DC connector 2.1/5.5 mm
USB 2.0 Type A	1

Article numbers

Device	Description	Article number
SCALANCE W1750D-2IA RJ45	2x RJ45 Ethernet interfaces, max. 1 Gbps, PoE 2x integral wireless cards 8x integrated omnidirectional antennas	6GK5750-2HX01-1AA0 6GK5750-2HX01-1AB0 ¹⁾ 6GK5750-2HX01-1AD0 ²⁾

¹⁾ US variant

²⁾ Japan variant

4.6.13 Antennas

4.6.13.1 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 detached and directly mounted or 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. A cable connects the detached antenna and access point or client. The antennas operated directly on the device allow compact, low-maintenance installation.

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** (omnidirectional antennas)

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

- **Directional** (directional antennas)

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. The reach of the wireless signal increases through a narrower angle. The disadvantage of directional antennas is that they need to be exactly oriented towards the partner.

- **Sectoral** (sector antennas)

Sector antennas are directional antennas with a larger opening angle. It lies between 30 and 120 degrees horizontally and 5 and 10 degrees vertically. As a rule several sector antennas are positioned at a location to ensure full 360° coverage.

- **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 it difficult to use wireless or when the node only moves along predefined rails, it is sometimes preferable to replace 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, transfer paths, tunnels or suspended monorails
- Generation of a cone-shaped limited RF field
- Cost savings due to direct substitution of sliding contacts and trailing cables
- Highly flexible application

4.6.13.2 Product overview

Table 4- 5 Omnidirectional antennas



Device type	Horizontal radiation angle/ characteristics	Antenna gain at 2.4 GHz	Antenna gain 5 GHz	Connection	Mounting		Degree of protection
					Direct	Detached	
 ANT795-4MA	360°	3 dBi	5 dBi	1 x R-SMA male	•	-	IP30
 ANT795-4MB	360°	2 dBi	3 dBi	1 x R-SMA male	•	-	IP65
 ANT795-4MC	360°	3 dBi	5 dBi	1x N-Connect male	•	-	IP65
 ANT795-4MD	360°	3 dBi	5 dBi	1x N-Connect female	•	-	IP65
 ANT795-4MX	360°	2 dBi	2.5 dBi	1x N-Connect male	•	-	IP68/69 K
 ANT795-6MP	360°	5 dBi	7 dBi	1x N-Connect female	-	•	IP67

4.6 SCALANCE W components for the Industrial Wireless LAN

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

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


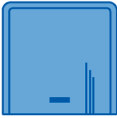



Table 4- 6 Antennas with directionality

Device type	Horizontal radiation angle/ characteristics	Antenna gain 2.4 GHz / dBi	Antenna gain 5 GHz / dBi	Connection	Mounting		Degree of protection
					Direct	Detached	
 ANT795-6DC	75° ¹⁾ 55° ²⁾	9 dBi	9 dBi	1x N-Connect female	-	•	IP67
 ANT793-6DG	70° ²⁾	-	9 dBi	2x N-Connect female	-	•	IP67

1) In the 2.4 GHz frequency band




2) In the 5 GHz frequency band

Table 4- 7 Antennas with strong directionality

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

¹⁾ In the 5 GHz frequency band

Table 4- 8 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	Connection	Mounting		Degree of protection
					Direct	Detached	
 ANT792-4DN	90° ¹⁾	4 dBi	-	1x N-Connect female	-	•	IP65
 ANT793-4MN	360° ²⁾	-	6 dBi	1x N-Connect female	-	•	IP65
 RCoax cable	-	-	-	-	-	•	IP65

1) In the 2.4 GHz frequency band

2) In the 5 GHz frequency band

Article numbers

Omnidirectional antennas

Designation	Description	Article number
ANT795-4MA ¹⁾	Antenna gain incl. connector 3 / 5 dBi for 2.4 GHz / 5 GHz, IP30, radially rotatable, with extra joint, R-SMA male	6GK5795-4MA00-0AA3
ANT795-4MB ¹⁾	Antenna gain incl. connectors: 2 / 3 dBi for 2.4 GHz / 5 GHz, IP65, radially rotatable, with extra joint, R-SMA male	6GK5795-4MB00-0AA0
ANT795-4MC ¹⁾	Antenna gain incl. plug 3 / 5 dBi for 2.4 GHz / 5 GHz, IP65 (-20 °C to +65 °C), straight connection, N-Connect male	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), connection with fixed 90° angle, N-Connect male	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)	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), incl. installation fittings	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 TI795-1R; incl. installation fittings	6GK5792-6MN00-0AA6
ANT795-6MN	Antenna gain incl. plug 6/8 dBi for 2.4 GHz / 5 GHz, IP65 (-40 °C to +80 °C); with terminating resistor 1 x TI795-1R	6GK5795-6MN10-0AA6

4.6 SCALANCE W components for the Industrial Wireless LAN

Designation	Description	Article number
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 jacks, antenna gain 6 dBi, for 2.4 GHz / 5 GHz, IP65 (-40 °C to +80 °C), incl. mounting bracket	6GK5795-6MT00-0AA0

1) Mounting directly on SCALANCE W

Antennas with weak directionality

Designation	Description	Article number
ANT795-6DC	Wide-angle antenna with light 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 wide-angle antenna with slight directivity; antenna gain incl. N-Connect plug 2 / 9 dBi for 5 GHz, IP67 (-40 °C to +80 °C)	6GK5793-6DG00-0AA0

Antennas with strong directionality

Designation	Description	Article number
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 1x 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, incl. installation material	6GK5793-8DL00-0AA0
ANT793-8DJ	Vertical-horizontal polarized antenna with strong directivity; antenna gain incl. 2 N-Connect plugs 18 dBi, for 5 GHz, IP67 (-45 °C to +70 °C)	6GK5793-8DJ00-0AA0
ANT793-8DK	Vertical-horizontal polarized antenna with strong directivity; antenna gain incl. 2 N-Connect plugs 23 dBi, for 5 GHz, IP67 (-45 °C to +70 °C)	6GK5793-8DK00-0AA0

RCoax antennas

Designation	Description	Article number
ANT792-4DN	RCoax helical antenna circular, polarized for RCoax systems; N-Connect female connection; antenna gain at 2.4 GHz 1 dBi, IP65	6GK5792-4DN00-0AA6
ANT793-4MN	RCoax λ 5 / 8 vertically polarized for RCoax systems; Connection N-Connect female; Antenna gain at 5.2 GHz/ 5.7 GHz 6/ 5 dB; 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.

Link: (<https://support.industry.siemens.com/cs/us/en/view/109480868>)

4.7 SCALANCE M industry router

4.7.1 Overview

Areas of application for SCALANCE M

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

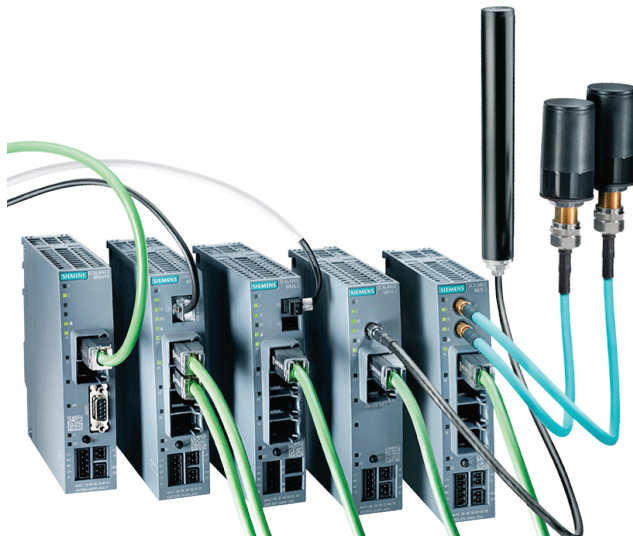


Figure 4-40 SCALANCE M product family

GPRS / UMTS / LTE for complex stations with increased security requirements

GPRS, UMTS and LTE packet oriented mobile communications services. With their 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 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. An Industrial Security Appliance SCALANCE S615, SCALANCE SC642-2C or SCALANCE SC646-2C 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 by means of the configuration tool Security Configuration Tool (SCT) and allows configuration without special IT experience. The IP address of the master station should ideally be fixed; the IP address of the stations can be assigned dynamically.

Wired communication using public or internal company networks

The devices 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 and VPN).

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

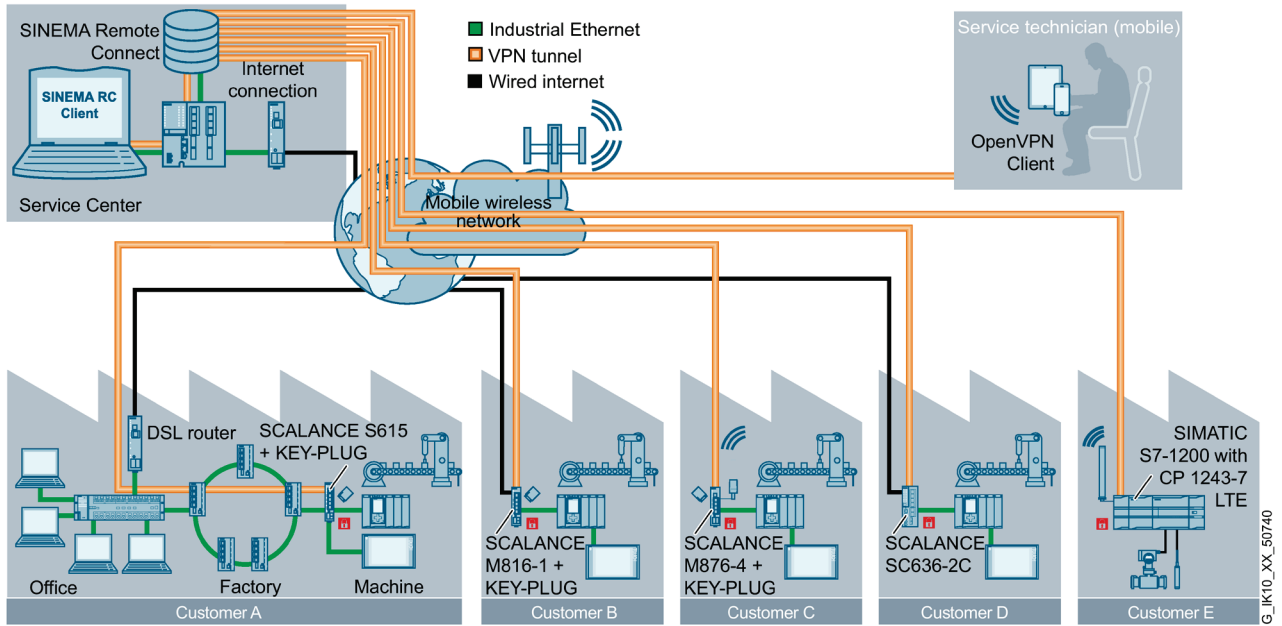


Figure 4-41 Example of a topology for the TeleControl network: Industrial Remote Communication

4.7.2 SCALANCE M812-1, M816-1 and M826-2

4.7.2.1 Description



Figure 4-42 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 IP20 degree of protection 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.

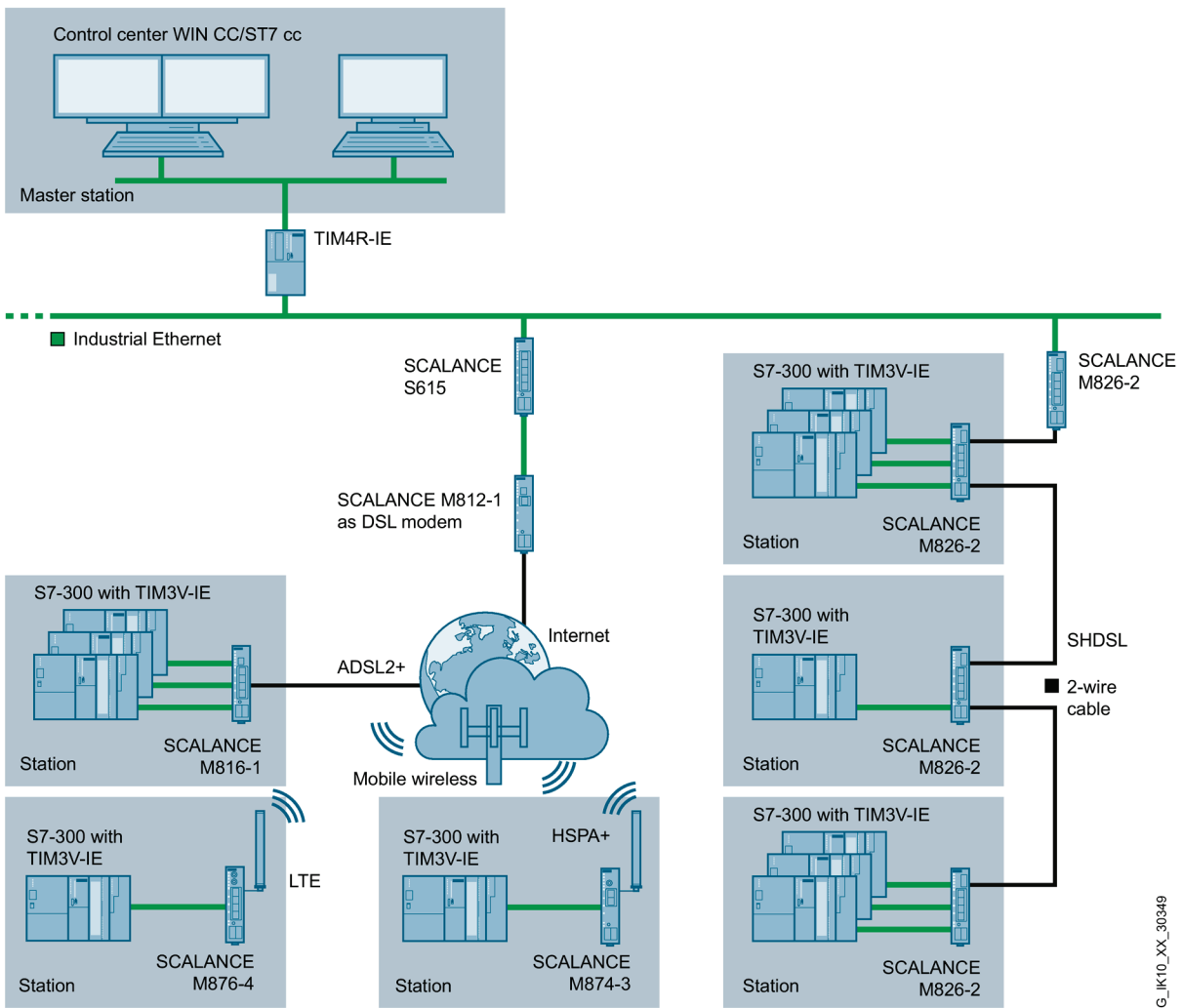


Figure 4-43 Example of a topology for using the devices SCALANCE M816-1 and M826-2

4.7.2.2 Features and functions

Features

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

	M812-1	M816-1	M826-2
Diagnostics LED	•	•	•
On site display (Set button)	•	•	•
Connectors	ADSL ADSL2 ADSL2+	ADSL ADSL2 ADSL2+	SHDSL
Ethernet interface	1x RJ45	4x RJ45	4x RJ45
Transmission rate	10/100 Mbps	10/100 Mbps	10/100 Mbps

4.7 SCALANCE M industry router

	M812-1	M816-1	M826-2
DSL interface	1x RJ45	1x RJ45	Terminal strip for 2-wire/4-wire cable
Digital input/output	1/1	1/1	1/1
Power supply 24 V DC	•	•	•
Redundant power supply	•	•	•
C-PLUG slot	-	•	•

- Suitable / available or according to the specified standard

Functions

- Industrial Ethernet interface 10/100 Mbps, TP, autocrossover
- 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
- NTP
- SNTP

4.7.2.3 Article numbers

Device	Description	Article number
SCALANCE M812-1	ADSL router with connector for the internal network	
	ADSL2+ (Annex A)	6GK5812-1AA00-2AA2
	ADSL2+ (Annex B)	6GK5812-1BA00-2AA2
SCALANCE M816-1	ADSL router 4-port switch	
	ADSL2+ (Annex A)	6GK5816-1AA00-2AA2
	ADSL2+ (Annex B)	6GK5816-1BA00-2AA2
SCALANCE M826-2	SHDSL router with 4-port switch.	6GK5826-2AB00-2AB2

4.7.3 SCALANCE M874-3 and M-876-4

4.7.3.1 Description



Figure 4-44 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 IP20 degree of protection 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.

4.7 SCALANCE M industry router

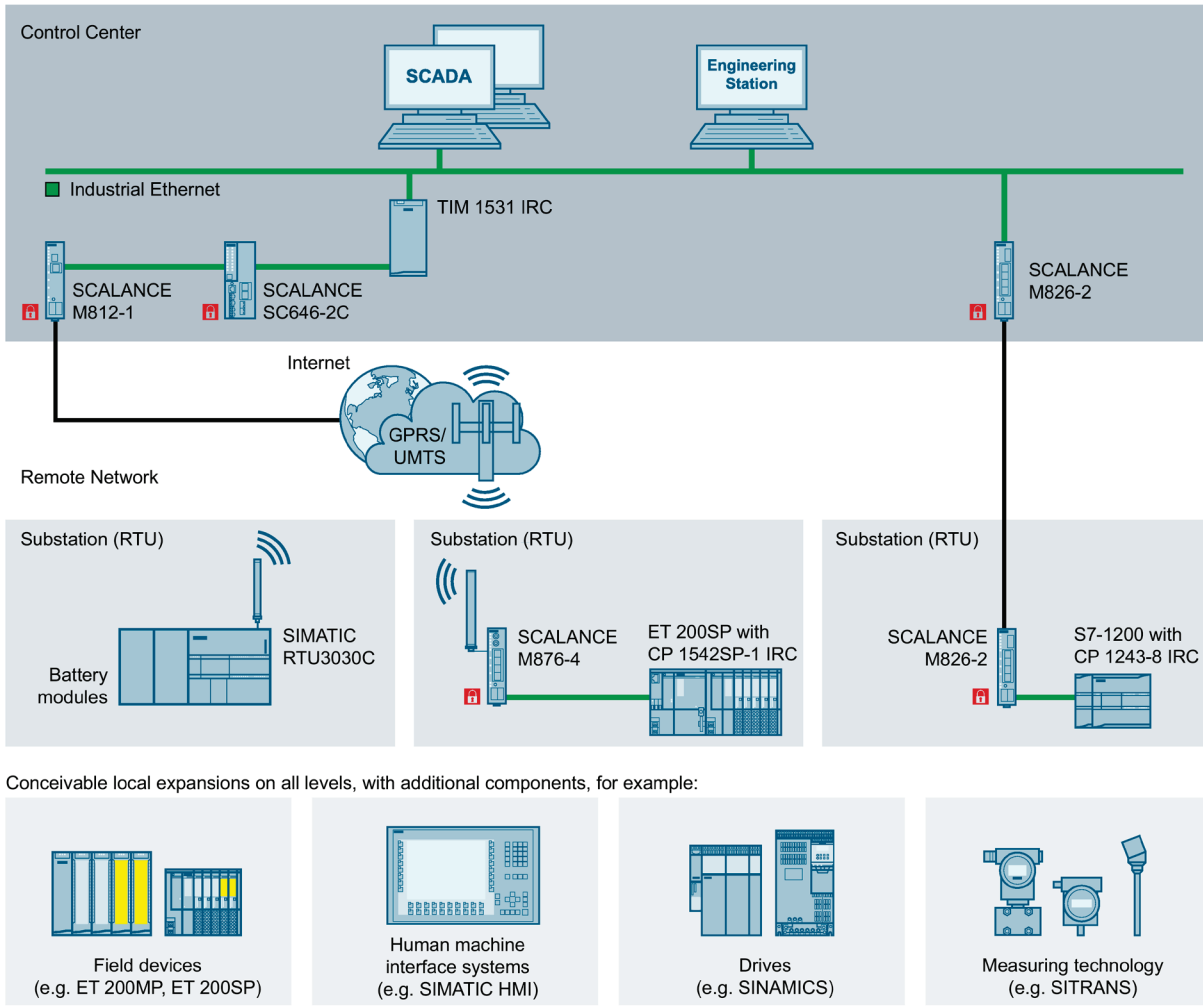


Figure 4-45 Example of a topology for using the SCALANCE M-800

4.7.3.2 Features and functions

Features

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

	M874-2 2.5G	M874-3 3G	M876-3 3G M876-3 3G (ROK)	M876-4 LTE (EU) M876-4 LTE (NAM)
Supported wireless networks	GSM	GSM UMTS	GSM UMTS CDMA * EV-DO *	GSM UMTS LTE
Supported mobile wireless services	GPRS eGPRS	GPRS eGPRS HSPA+	GPRS eGPRS HSPA+	GPRS eGPRS HSPA+ LTE Cat. 3
Ethernet interface	2x RJ45	2x RJ45	4x RJ45	4x RJ45
Transmission rate 10/100 Mbps	•	•	•	•
Number of SMA antenna sockets	1	1	2	2
Power supply 24 V DC	•	•	•	•
Redundant power supply	•	•	•	•
C-PLUG slot	•	•	•	•
Digital input/output	1/1	1/1	1/1	1/1

• Suitable / available or according to the specified standard

* Not for ROK product variant

Functions

- Industrial Ethernet interface 10/100 Mbps, TP, autocrossover
- 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

4.7.3.3 Article numbers

Device	Description	Article number
SCALANCE M874-2	Mobile wireless router for GSM with 2-port switch	6GK5874-2AA00-2AA2
SCALANCE M874-3	Mobile wireless router for GSM and UMTS with 2-port switch	6GK5874-3AA00-2AA2
SCALANCE M876-3	Mobile wireless router for GSM, UMTS, CDMA and EV-DO with 4-port switch	6GK5876-3AA02-2BA2 6GK5876-3AA02-2EA2
SCALANCE M876-3 (ROK)	Mobile wireless router for GSM, UMTS, CDMA and EV-DO with 4-port switch. Version for Korea	6GK5876-3AA02-2EA2
SCALANCE M876-4 LTE (EU)	Mobile wireless router for LTE with 4-port switch. Version for Europe	6GK5876-4AA00-2BA2
SCALANCE M876-4 LTE (NAM)	Mobile wireless router for LTE with 4-port switch. Version for North America	6GK5876-4AA00-2DA2

4.7.4 SCALANCE M804PB

4.7.4.1 Description



Figure 4-46 SCALANCE M804PB

The SCALANCE M804PB enables secure remote connection of PROFIBUS / MPI plants to Ethernet networks. The connection is secured via VPN connection and a firewall. The device is equipped with an RS485 interface for the connection to PROFIBUS and two RJ45 interfaces for the connection to the internal network. An RJ45 interface is available for the connection to the external network.

There is an auto configuration interface for the connection to SINEMA RC that is enabled with the KEY-PLUG SINEMA RC. SINEMA RC then allows fast and efficient connection configuration. The devices can also be connected via the TIA Portal or SIMATIC STEP7.

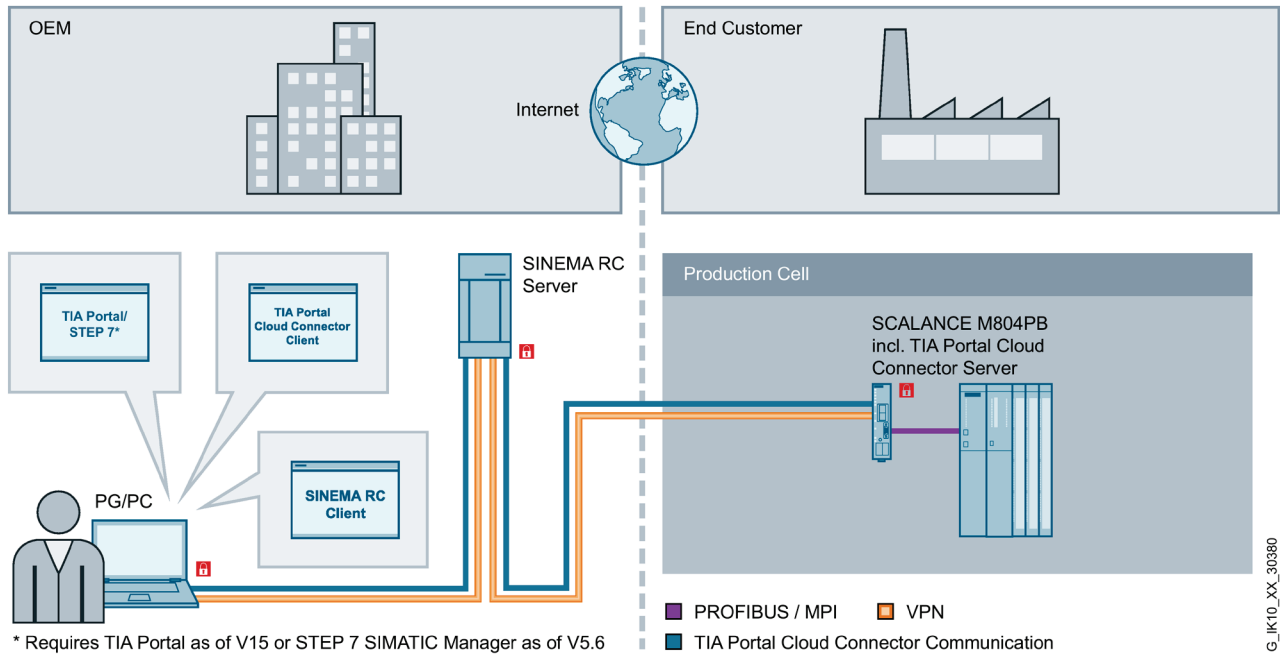


Figure 4-47 Example of a topology for the remote maintenance of PROFIBUS systems via the SCALANCE M804PB

4.7.4.2 Features and functions

Features

The device has the characteristics shown in the following table:

	M804PB
Diagnostics LED	•
Power supply	24 VDC
Redundant power supply	•
On site display (Set button)	•
C-PLUG slot	•

- Suitable / available or according to the specified standard

Functions

- Configuration with STEP 7
- Configuration using the WBM, CLI or SNMP
- MIB support
- TRAPs via e-mail
- HTTP, HTTPS, Telnet
- 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 inspection)
- VPN with up to 20 connections
- IPsec
- OpenVPN client to SINEMA Remote Connect

4.7.4.3 Interfaces

	M804PB
Ethernet interface	2x RJ45 10/100 Mbps
MPI/DP interface	1x RS485 (up to max. 12 Mbps)
Digital input and output (DI/DO)	2x 2-pin screw terminal

4.7.4.4 Article numbers

Device	Description	Article number
SCALANCE M804PB	IE router, 2x RJ45 ports, 1x PROFIBUS / MPI	6GK5804-0AP00-2AA2

4.7.5 TeleService Adapter IE

4.7.5.1 Description



Figure 4-48 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 IP20 degree of protection 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.

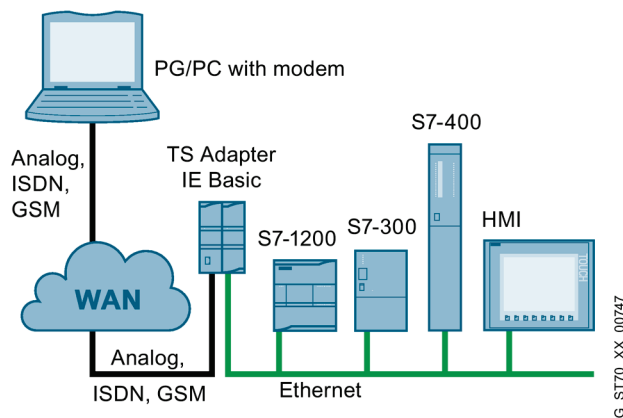


Figure 4-49 Example of the configuration of a TeleService Adapter IE Basic with TS module

4.7.5.2 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	1x RJ45 port	2x RJ45 port (switched)
Number and type of the LAN interfaces	-	1x RJ45 port
Power supply	24 VDC(19.2 to 28.8 VDC)	

The modules have the characteristics shown in the following table:

	Modem	ISDN	RS-232	GSM
Number and type of the LAN interfaces	1x RJ11 socket	1x RJ11 socket	1x D-sub male connector, 9-pin	1x 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 SP2 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.

4.7.5.3 Article numbers

Device	Description	Article number
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 RS232	Module for connection of an external modem	6ES7972-0MS00-0XA0
TS module GSM	Wireless modem for the GSM/GPRS network	6ES7972-0MG00-0XA0

4.7.6 Modem MD720

4.7.6.1 Description



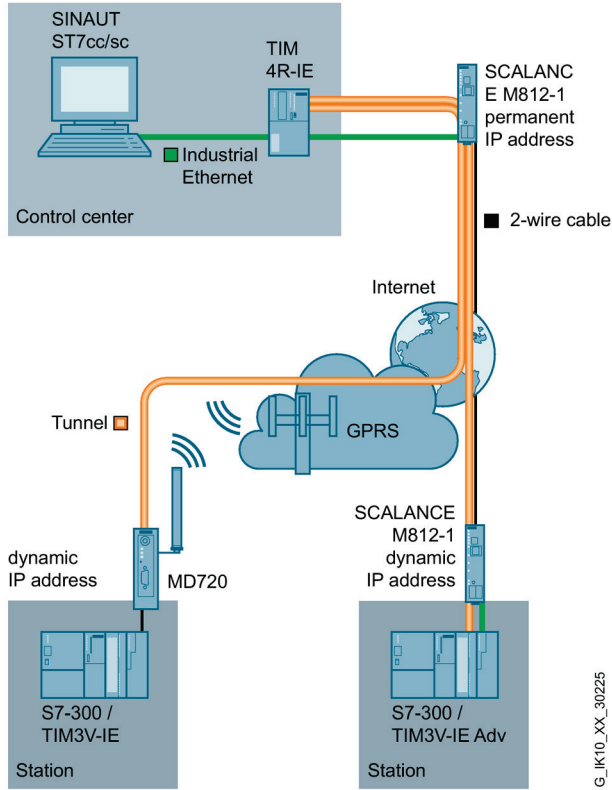
Figure 4-50 Modem MD720

The GSM/GPRS modem MD720 is used for the remote control system SINAUT ST7 for data transmission via a dial-up connection (CSD service) and for a remote control 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



4.7.6.2 Features and functions

Features

	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

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 MD720 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
- Username 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

Device	Description	Article number
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

4.7.7 Antennas for mobile wireless





4.7.7.1 Product overview

Table 4-9 Antennas for mounting directly on the device

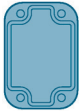
Antenna	GSM (2G)	GPRS	UMTS	LTE Europe	LTE North America	GPS	WLAN
 ANT896-4MA	•	•	•	•	•	-	-

- Suitable / available or according to the specified standard.

Table 4- 10 Antennas for detached mounting

Antenna	GSM (2G)	GPRS	UMTS	LTE Europe	LTE North America	GPS	WLAN
 ANT896-4ME	•	•	•	•	•	-	-
 ANT794-4MR	•	•	•	•	-	-	-
 ANT794-3M	•	•	-	-	-	-	-
 ANT895-6ML	-	-	-	-	-	•	-

• Suitable / available or according to the specified standard.

Antenna	GSM (2G)	GPRS	UMTS	LTE Europe	LTE North America	GPS	WLAN
 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
ANT896-6MH	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

Device	Description	Article number
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
ANT896-6MH	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.

Link: (<https://support.industry.siemens.com/cs/us/en/view/109480868>)

4.8 SCALANCE S Industrial Security Appliance

4.8.1 Overview

Areas of application for SCALANCE S

The SCALANCE S Industrial Security Appliance devices 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. For secure remote access via Internet, suitable devices of the SCALANCE M-800 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
- Problem-free integration into existing networks without reconfiguration of end nodes or setup of new IP subnetworks

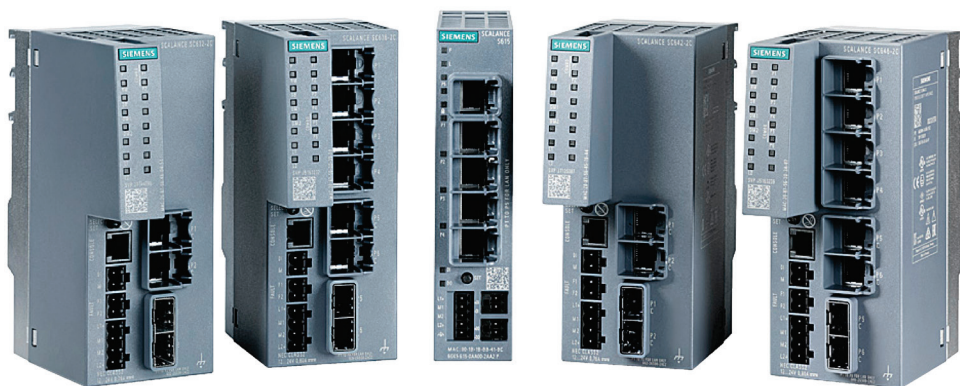


Figure 4-51 SCALANCE S product family

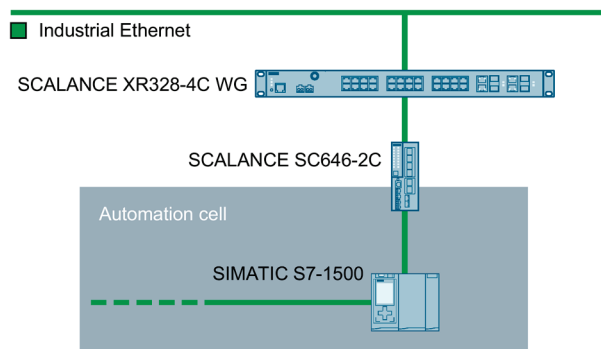


Figure 4-52 Example of a topology: Protection of an automation cell with a SCALANCE SC646-2C

4.8.2 Technical basics

Internal and external network nodes

The SCALANCE S Industrial Security Appliances 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 with external network segments only via a SCALANCE S Industrial Security Appliance. Further connection paths between the internal and external networks may not exist.

Configuration and administration

With the TIA Portal, all SIMATIC NET security products can be configured and diagnosed from a central location. The configuration of individual devices is possible in Web Based Management (WBM), Command Line Interface (CLI) or by using SNMP.

The configuration of a SCALANCE S device encompasses the IP parameters and the configuration of the firewall rules. With the SCALANCE SC642-2C and SCALANCE SC646-2C devices, it is also possible to configure IPsec tunnels, if necessary.

The SINEMA Remote Connect management platform is used for secure remote maintenance that enables the setup and management of the tunnel connections (VPN). A direct access to the company network is not required. The SINEMA Remote Connect server takes on the function of an agent between the communication nodes.

Firewall

The firewall functionality of SCALANCE S Industrial Security Appliances 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 the network nodes from the external networks are allowed. All network nodes that are located in the internal network segment of a SCALANCE S Industrial Security Application are protected by its firewall. Furthermore, up to four internal networks as well as the communication relationships permissible between these networks can be configured.

The SCALANCE S Industrial Security Appliances thus offer the realization of a flexible cell protection concept via firewall:

- Protection of random Ethernet-based automation devices and systems that have no own security functions
- Protection of several devices at the same time
- Reduction of potential network malfunctions and unauthorized network accesses by forming secure communication islands (network segmentation)
- Securing the communication from and to the automation cells

The firewall functionality can be configured for the following protocol levels:

- IP firewall including 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 (only with SCALANCE S615, SCALANCE SC642-2C and SCALANCE SC646-2C)
- As well as within a network segment for internal to internal communication

For all devices, user-specific firewall rules can also be specified. They are assigned during login, user-dependently, for a limited time.

SCALANCE S in routing mode

If SCALANCE S Industrial Security Appliances are operated in routing mode, they separate the internal network from the external network based on the evaluation of the IP addresses. The frames intended for an existing IP address in the subnetwork (internal or external) are forwarded. The firewall rules for the direction of transmission also apply. The configuration specifies which ports are assigned to the internal network and to 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 Appliances 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 test and monitoring purposes, the Industrial Security Appliances dispose of 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 Industrial Security Appliance (local logging) or of a server (network Syslog). You select the events to be logged in the log settings for the relevant Industrial Security Appliance.

IPsec tunnel (only for SCALANCE S615, SC642-2C, SC646-2C)

The Internet Protocol Security (IPsec) is a Layer 3 tunneling protocol. The IPsec tunnel provides the nodes with a secure data connection through the non-secure external network to other devices that are protected by the SCALANCE S devices.

The encryption of the data transmission with VPN (IPsec) provides the following:

- **Protection against espionage:** The data exchanged are safe from eavesdropping (ensuring confidentiality).
- **Protection against manipulation:** The data exchanged are safe from corruption/counterfeiting (ensuring integrity).
- **Authenticity:** Only authorized nodes can establish a tunnel (ensuring the legitimacy of the communication)

For the configuration of Virtual Private Networks (VPN), SCALANCE S devices as well as the SOFTNET Security Client modules, which are integrated in an internal network, are combined into groups in the configuration. IPsec tunnels are established automatically between the SCALANCE S devices and SOFTNET Security Client modules that belong to the same group.

4.8.3 Description

SCALANCE S615



Figure 4-53 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 the connection to SINEMA RC that is enabled with the KEY-PLUG SINEMA RC. SINEMA RC then allows fast and efficient connection configuration.

SCALANCE SC-600



Figure 4-54 SCALANCE SC632-2C and SCALANCE SC636-2C



Figure 4-55 SCALANCE SC642-2C and SCALANCE SC646-2C

The devices of the SCALANCE SC-600 product line are Industrial Security Appliances for protection against unauthorized accesses.

The rear of the robust enclosure in the SIMATIC S7-1500 format consists of die-cast aluminum and offers all options for the installation that are required in the industrial environment (SIMATIC S7-1500 and S7-300 standard rail standard DIN rail, wall mounting). The enclosures in IP20 degree of protection are designed for installation in a control cabinet. The RJ45 sockets with securing collar provide additional strain and bend relief for the use of FastConnect connectors. The redundant power distribution, a signaling contact, a console port for the direct device access as well as the optionally available exchangeable storage medium C-PLUG enable efficient operation of the devices.

The combo ports available with some devices provide for special flexibility. A combo port is a switch port with two optionally usable hardware interfaces, a combination of an RJ45 socket with a pluggable transceiver slot. If a pluggable transceiver is used, the RJ45 connector switches off and the pluggable transceiver is used for the data transfer. The pluggable transceivers can be used or replaced during operation.

4.8.4 Features and functions

Features

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

	S615	SC632-2C	SC636-2C	SC642-2C	SC646-2C
Gigabit Ethernet	-	•	•	•	•
Combo ports	-	•	•	•	•
Diagnostics LED	•	•	•	•	•
Signaling contact	-	•	•	•	•
Power supply	24 V DC	24 V DC	24 V DC	24 V DC	24 V DC
Redundant power supply	•	•	•	•	•

	S615	SC632-2C	SC636-2C	SC642-2C	SC646-2C
On site display (Set button)	•	•	•	•	•
C-PLUG slot	•	•	•	•	•

- Suitable / available or according to the specified standard.

Functions

The following table indicates the functions provided by the individual devices:

	S615	SC632-2C	SC636-2C	SC642-2C	SC646-2C
Configuration with WBM, CLI or SNMP	•	•	•	•	•
MIB support	•	•	•	•	•
HTTP	•	•	•	•	•
SNMPv1, SNMPv2 and SNMPv3	•	•	•	•	•
SysLog	•	•	•	•	•
DHCP client	•	•	•	•	•
DHCP server (internal network)	•	•	•	•	•
Static IP routing	•	•	•	•	•
NAT/NAPT	•	•	•	•	•
Firewall (Stateful Packet Inspection)	•	•	•	•	•
Max. firewall data throughput	100 Mbps	600 Mbps	600 Mbps	600 Mbps	600 Mbps
IPsec support	•	-	-	•	•
Max. number of VPN connections	20	-	-	200	200
Max VPN data throughput	35 Mbps	-	-	120 Mbps	120 Mbps
Softnet security client	•	•	•	•	•
Connection to SINEMA Remote Connect via VPN	•	•	•	•	•

- Suitable / available or according to the specified standard.

4.8.5 Interfaces

The SCALANCE S modules have the following connectors or interfaces:

Device	Total number of available ports	Twisted pair		Fiber-optic cables	Combo ports 100/1000 Mbps
		10/100 Mbps	10/100/1000 Mbps	1000 Mbps	
S615	5	5x RJ45	-	-	-
SC632-2C	2 ¹⁾	-	Max. 2x RJ45	-	2x SFP
SC636-2C	6 ¹⁾	-	Max. 6x RJ45	-	2x SFP
SC642-2C	2 ¹⁾	-	Max. 2x RJ45	-	2x SFP
SC646-2C	6 ¹⁾	-	Max. 6x RJ45	-	2x SFP

¹⁾ Of which 2 are combo ports

4.8.6 Article numbers

Device	Description	Article number
SCALANCE S615	5x 10/100 Mbps RJ45 ports; 1x digital input 1x digital output	6GK5615-0AA00-2AA2
SCALANCE SC632-2C	2x 100/1000 Mbps combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); 1x digital input	6GK5632-2GS00-2AC2
SCALANCE SC636-2C	4x 10/100/1000 Mbps RJ45 ports 2x 100/1000 Mbps combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); 1x digital input	6GK5636-2GS00-2AC2
SCALANCE SC642-2C	2x 100/1000 Mbps combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); 1x digital input	6GK5642-2GS00-2AC2
SCALANCE SC646-2C	4x 10/100/1000 Mbps RJ45 ports 2x 100/1000 Mbps combo ports (usable either for plug-in transceiver SFP 100/1000 Mbps or as 10/100/1000 Mbps RJ45 ports); 1x digital input	6GK5646-2GS00-2AC2

4.8.7 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 devices 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 enables secure IP-based access from the PC / programming device to programmable controllers that are protected by SCALANCE SC63x-2C or SCALANCE SC64x-2C.

Details

- Easy handling due to minimum configuration
- No specialist knowledge of IT security is required
- 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 Industrial Security Appliances 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 devices.

The 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. Subsequently security settings are made based on the data from the configuration so that applications can access IP addresses downstream from the SCALANCE S Industrial Security Appliances.

If the learning mode for the internal nodes or programmable controllers is activated, the configuration module first sets a security policy for the secure access to the SCALANCE S devices. The SOFTNET Security Client then addresses the SCALANCE S devices 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

Product	Description	Article number
SOFTNET Security Client Edition 2008	For Microsoft Windows XP Professional, 32-bit incl. SP1, SP2 and SP3	6GK1704-1VW02-0AA0
SOFTNET Security Client V3	For Microsoft Windows 7 Professional, Ultimate and XP Professional 32-bit, incl. SP3	6GK1704-1VW03-0AA0
SOFTNET Security Client V4	For Microsoft Windows 7 Professional, Ultimate, 32/64-bit	6GK1704-1VW04-0AA0
SOFTNET SECURITY CLIENT V5	For Microsoft Windows 7 Ultimate and Professional (32+64-bit), Windows Server 2012 R2	6GK1704-1VW05-0AA0

4.8.8 SINEMA RC

Description

The management platform SINEMA Remote Connect (SINEMA RC) provides end-to-end connection management via the Internet. The service technician and the machine to be maintained each establish an IPsec or OpenVPN connection to the SINEMA RC Server, which can be reached via a static IP address. The SINEMA RC Client software is available to the service technician for establishing the VPN connection. The SINEMA RC Server checks the identity of the nodes via an exchange of certificates. In case of a successful logon, the VPN tunnel is established between the SINEMA RC Server, the service technician and the machine; and the service technician is authorized for pre-defined remote accesses to the machine. The SINEMA RC Server manages the individual VPN tunnels in accordance with the configured communication relations and the security settings. Direct access to the company network in which the machine is integrated is therefore not necessary.

The connection to SINEMA RC can be affected via mobile wireless, DSL or existing private network infrastructures. These can be easily parameterized for the connection to SINEMA Remote Connect via auto configuration.

The SINEMA RC Server is configured via the Web Based Management (WBM). The connection to the WBM via the Internet/WAN takes place over the HTTPS protocol. The access to the SINEMA RC Server is protected against unauthorized accesses via authentication mechanisms as well as through specified task-specific access rights.

Note

You will find more information on SINEMA RC in SINEMA RC (<https://siemens.com/sinema-remote-connect>).

Features and functions

SINEMA RC has the following characteristics and functions:

- Protocol-independent, IP-based communication
- Central management of all VPN connections
- Connection management
 - Establishment of encrypted connections with OpenVPN and IPsec
 - Establishment of permanent or event-based connections, for example via wake-up message or through a signal at the digital input
- Multi-factor authentication with username/password and PKI smartcard
- Support of the current encryption process, TLS 1.2
- Easy management of different users
 - Device and user management with group management
 - User management with the configuration of rights
- Connection of subnetworks behind SCALANCE M or Industrial Security Appliances SCALANCE S industrial routers
 - Support of routing
 - Support of NAT for mapping local identical subnetworks
 - Support of NAT for mapping dedicated local IP addresses
 - Support of multiple subnetworks behind SCALANCE M industrial routers or Industrial Security Appliances SCALANCE S
 - User-specific access rights to unique IP addresses in the subnetwork
- Address book function in the SINEMA RC client
 - List display of all devices assigned to a user
- SIMATIC TeleService
 - Selection of a device for execution of TeleService in the SIMATIC environment
- Proxy server
 - For communication with networks behind a proxy server infrastructure
- Support of HTTPS and SOCKS Proxy servers

- Auto configuration interface
 - For simple configuration to a connection of the SINEMA Remote Connect.
- Easy integration of the Siemens industrial routers, Industrial Security Appliances and selected SIMATIC CP units by means of auto-configuration
- Optimal connection and easy selection of identical machines with identical local subnetworks in series machine construction and at OEM (original equipment manufacturer)
- Tunnel encryption
 - OpenVPN
- Offline licensing for activating user and device licenses on the server, including without an internet connection
- Operation also in a virtualized environment

Supported products

The following products are suitable for connecting to the SINEMA RC Server:

- SCALANCE M874, SCALANCE M876, SCALANCE M816, SCALANCE M826, SCALANCE M804PB
- SCALANCE S615
- SINEMA RC Client
- SCALANCE SC632-2C, SCALANCE SC636-2C, SCALANCE SC642-2C, SCALANCE SC646-2C
- CP 1200
- CP 1543-1, CP 1543SP-1
- RM 1224
- RTU3010C, RTU3030C, RTU3031C

Hardware requirements for the installation of SINEMA RC Server

The installation of the SINEMA RC Server includes its own operating system. For the installation of SINEMA RC Server you require a PC without an operating system and a disk capacity of at least 60 GB. If you have already installed another operating system on the PC, all previously saved data is lost through the installation of SINEMA RC Server.

Software requirements for the installation of SINEMA RC client

SINEMA RC client is released for the following operating systems:

- Microsoft Windows 7 Professional 32/64-bit + Service Pack 1
- Microsoft Windows 7 Enterprise 32/64-bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64-bit + Service Pack 1
- Microsoft Windows 8.1 Professional 64-bit

4.9 Network management software

- Microsoft Windows Server 2008 R2 64-bit + Service Pack 1 (requirement: NET 3.5 or higher is installed)
- Microsoft Windows Server 2016 Standard (Desktop representation)
- Microsoft Windows 10 Professional 64-bit
- Microsoft Windows Server 2012 R2 64-bit

Licenses

Without a license extension, you can configure four nodes with the SINEMA RC Server. In addition, a license for SINEMA Remote Connect is included. You can increase the number of nodes with the following licenses:

- SINEMA Remote Connect 64: This license supports up to +64 nodes.
- SINEMA Remote Connect 256: This license supports up to +256 nodes.
- SINEMA Remote Connect 1024: This license supports up to +1024 nodes.

4.9 Network management software

4.9.1 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:
 - Searching a network 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 Industrial 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 online in the network.
- PROFIBUS interfaces can also be configured using PST only for modules that also have an accessible 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 SP 1
 - Windows 8.1 Professional
- 64-bit operating systems
 - Windows 7 Professional / Ultimate SP1
 - Windows Server 2008 Standard Server R2
 - Windows 8.1 Professional
 - Windows Server 2012 Standard R2
 - Windows 10 Pro
 - Windows 10 Pro Version 1607

It is possible to set addresses for the following SIMATIC NET network components using PST:

- SCALANCE W-700
- SCALANCE X-200
- SCALANCE X-300
- SCALANCE X-400
- SCALANCE X-500

It is possible to set addresses for the following Ethernet CPs using PST:

- CP 343-1
- CP 443-1

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 (**D**iscovery and basic **C**onfiguration **P**rotocol) and DLC (**D**ata **L**ink **C**ontrol) 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 PST (<https://support.industry.siemens.com/cs/ww/en/view/19440762>).

4.9.2 SINEC NMS

Description

The network management system SINEC NMS is a software for central monitoring and management of industrial networks with up to 12500 nodes. The distributed approach of SINEC NMS allows a subsequent expansion of the network infrastructures. The network management system SINEC NMS is subdivided into two levels:

- **Control**
Monitoring and administering the entire network
- **Operation**
Monitoring and administering a subnetwork

You configure the monitoring settings to be used by the Operations centrally at the Control and then load them onto the Operations. The Operations read the monitoring data from the devices and supply selected data and summarized status information to the Control.

Note

You will find more information on SINEC NMS in SINEC NMS (<https://siemens.com/sinec-nms>).

Features and functions

Cross-industry:

- Structured display of the network for quick determination of the overall status
- Monitoring and management of different device categories
 - Monitoring for Control
Provides an overview of the monitoring data determined by the devices of all Operations.
 - Monitoring for Operations
Detailed information from each Operation via the devices monitored
Device representation in network topologies, in as far as the devices provide the neighborhood information.
- Manufacturer-independent visualization of all network nodes and comprehensive support of Siemens devices
- Rule-based network configuration for industrial communication (Policy Based Network Management)
 - Device-independent configuration function and firmware update function for individual or multiple network components
 - Regular backups of the device configurations to allow tracking of the configuration changes
 - Comparison of the device configurations with colored marking of the differences
 - Policy-based bulk configuration
- Firmware management based on topology dependencies
 - Central management of the firmware files on the Control
 - Automatic synchronization of the firmware for update/upgrade at the affected Operations
- Hierarchical user/role concept for local and functional access control (role-based access control)
 - Assigning authorizations to users for access to devices and functions
 - Central storage of user data on the Control or, alternatively, via Univenton Management Console UMC per Single-Sign-On
- Northbound interface for direct access to pre-processed network information for further processing in other systems or applications.

- Distributed approach
 - Complete view of the network, irrespective of size and complexity
 - Scalability of the network for expanding systems
- Manufacturer-independent diagnostics of NAT routers and their lower-level networks
- Reporting function
 - Exportable evaluations of the network monitoring for diagnostics, validation or statistics over any period in both text and graphic form

Industry-specific:

- Manufacturer-independent PROFINET diagnostics
- SIMATIC Diagnostics (S7-300 and S7-400)
- Diagnostics of PROFINET-based PCS 7 applications
- Automatic detection and monitoring of changing PROFINET topologies (for example tool changers)

Hardware requirements for the installation of SINEC NMS

SINEC NMS must be installed on each computer that is to be used as a Controll or Operation.

The required hardware depends on the following factors:

- Installation types (single or multiple node)
- Number of Operations
- Number of supported devices

You will find further information in the operating instructions for the device.

Software requirements for the installation of SINEC NMS

SINEC NMS is released for the following operating systems:

- Microsoft Windows 10 (Pro / Enterprise) as of Version 1709
- Microsoft Windows Server 2016

Licenses

Each Operation is licensed by the license of a specific type. In the license type, the number of devices is specified on an Operation (50/100/250/500) and the management status ("Managed" or "Monitored"). Devices with the "Monitored" status are only monitored by SINEC NMS. Devices with the "Managed" status can be monitored and configured by SINEC NMS. Licenses for 50, 100, 250 or 500 nodes can be combined.

Basic steps for network monitoring

Network monitoring is performed with the following steps:

- **Network scan**
Before it is possible to monitor devices in the network, the devices must be recognized by a network scan. The detected devices that correspond to the detection settings are displayed.
- **Device profiles and discovery rules**
Based on the discovery rules and the device profiles, SINEC NMS assigns the discovered devices to a suitable, previously configured device profile. Devices that do not match any device profile have default profiles assigned to them, provided these default profiles are activated.
- **Supported device functions**
Through the network scan, SINEC NMS also determines the functions supported by the devices and shows the result. This detection of the device functions is crucial for their configuration via policies. Only devices that meet this requirement can assume the management status "Managed".
- **Management status of a device**
The management status of a device indicates how the device can be handled by SINEC NMS. The number of devices with "Monitored" and "Managed" management status is limited by the existing SINEC NMS license.

4.9.3 SOFTNET TSN

Description

The SOFTNET TSN software of the SIMATIC NET product family enables the connection of a PC station to a TSN network (Time Sensitive Networking) in accordance with the standard IEEE 802.1.

SOFTNET TSN uses a defined interface of the switch for connection of the end devices to a TSN network; the application or end device logs on to this interface and sends its data via the network. The focus with SOFTNET TSN is in the area of the data exchange on the controller level (M2M) with OPC UA PubSub. If an existing application is to be connected to an existing TSN network, the SOFTNET TSN establishes a connection layer for connecting to the corresponding interface of the TSN network. SOFTNET TSN provides the logon at the TSN network and sends its data without connection into the network (Publishing), where they can be received by machines.

SOFTNET TSN can only operate in connection with a corresponding OPC UA PubSub application and cannot be operated independently.

Features and functions

SOFTNET TSN has the following characteristics and functions:

- **Support of OPC UA (Open Platform Communications Unified Architecture)**
Open platform- and manufacturer-independent Ethernet-based communication standard with integrated security mechanisms.
- **Network convergence**
Multiple real-time protocols can be operated in a single network parallel to each other.
- **Enhanced Quality of Service" (QoS)**
Bandwidth reservation, synchronization, low latencies and bumpless redundancy
- **Powerful machine communication**
High-speed communication on the control and operator level via OPC UA on the basis of the Publish/Subscribe principle.
- Dynamic ad-hoc communication relationships are possible.
- Transmission of large amounts of data through scalable transmission speeds of 100/1000/10000 Mbps

Supported operating systems

There are two operating-system-specific variants:

- SOFTNET TSN for operating under Windows
- SOFTNET TSN for operating under Linux

TSN-compatible devices

The following SIMATIC NET network components are suitable for connection to a TSN network:

SIMATIC CP 1545-1TSN

SCALANCE XC208G TSN

SCALANCE XC206-2SFP G TSN

License key

The authorization of SOFTNET TSN is effected via a license key with the Automation License Manager.

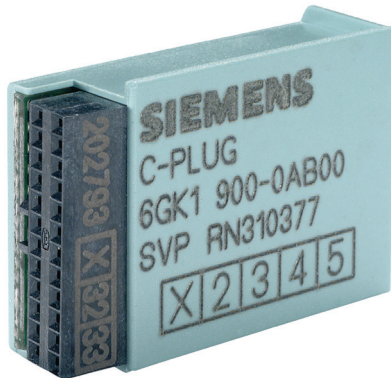
Requirements for the installation

Before you install SOFTNET TSN, you have to download the software package C++ based OPC UA Client/Server SDK Bundle as of V1.7. To do this, you need a login to Unified Automation.

4.10 Accessories

4.10.1 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 when 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. As a result, downtimes of network segments and connected Industrial Ethernet nodes can be minimized if a fault occurs.

The C-Plug can be used in all SIMATIC NET products with a C-PLUG slot.

Structure

The C-PLUG has IP20 degree of protection. With IP65 components the protection is ensured 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 diagnostic mechanisms of the end device (LEDs, PROFINET, SNMP, Web Based Management, etc.).

Article numbers

Component	Description	Article number
C-PLUG	Exchangeable storage medium for saving the configuration data, usable in SIMATIC NET products with C-PLUG slot	
	Memory capacity 32 MB	6GK1900-0AB00
	Memory capacity 256 MB	6GK1900-0AB10

4.10.2 KEY-PLUG

Description



Figure 4-56 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 of the function and the 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.

The KEY-PLUG can be used in all SIMATIC NET products with a C-PLUG slot.

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 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

Component	Description	Article number
KEY-PLUG W700 SECURITY	Activates the 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
KEY-PLUG SINEMA RC	Switches the connection to SINEMA Remote Connect for S615 and SCALANCE M816 / M826 / M874 / M876	6GK5908-0PB00

4.10.3 Configuration License PLUG (CLP)

Description

The SCALANCE CLP is an exchangeable storage medium for the storage and securing of configuration data that can be used in all SCALANCE devices with CLP slot (for example, with SCALANCE W1700). The SCALANCE CLP is used to transfer the configuration of the old device to the new device when a device is replaced. The CLP is also referred to as PLUG in the description.

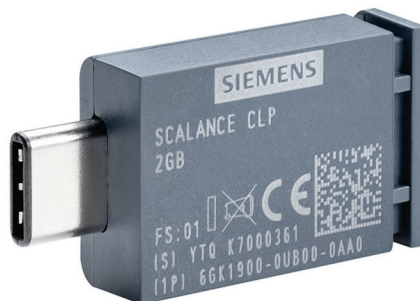


Figure 4-57 SCALANCE CLP

The PLUG is available in the following variants:

- **PLUG Configuration:** The exchangeable storage medium only saves the configuration data of the device.

How it works

NOTICE

Do not remove or insert the PLUG during operation.

A PLUG may only be removed or inserted when the device is turned off.

The device checks whether a PLUG is inserted at one second intervals. If it is detected that the PLUG has been removed, the device restarts.

If a valid PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.

If the device was configured at one time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

Devices with CLP slot support the following operating modes:

- **Without PLUG**

The device saves the configuration data in the internal memory. This mode is active when no PLUG is inserted.

- **With PLUG**

If an empty PLUG (as supplied) is inserted in the device, the device automatically backs up the configuration data on the PLUG during startup. If the PLUG contains a license, additional functions are also enabled. Changes to the configuration are stored directly on the PLUG and in the internal memory.

The configuration stored on the PLUG is displayed over the user interfaces.

When an unconfigured device starts up, it automatically adopts the configuration data of the inserted, written C-PLUG. The prerequisite for this is that the configuration data was written by a compatible device type.

One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.

Article numbers

Component	Description	Article number
SCALANCE CLP 2GB	Exchangeable storage medium for saving configuration data, can be used in SIMATIC NET products with CLP slot	6GK1900-0UB00-0AA0
SCALANCE CLP EEC 2GB	Exchangeable storage medium with coated PCBs for saving configuration data, usable in SIMATIC NET products with CLP slot	6GK1900-0UQ00-0AA0
SCALANCE CLP 2GB W1780 iFeatures	Exchangeable storage medium for saving configuration data and enabling iFeatures, can be used in SIMATIC NET products with CLP slot	6GK5907-8UA00-0AA0
SCALANCE CLP 2GB W1740 iFeatures	Exchangeable storage medium for saving configuration data and enabling iFeatures, can be used in SIMATIC NET products with CLP slot	6GK5907-4UA00-0AA0

Cloud Gateway

5.1 Description



Figure 5-1 CloudConnect 7 SIMATIC CC712 and SIMATIC CC716

The Cloud Gateway is used for the connection and data transmission of a SIMATIC S7 or Modbus process station to a cloud system or of a SIMATIC S7 process station to an OPC UA client.

There are two options for the transmission of process data:

- **Connection of a S7 or a Modbus process station to a cloud broker:**

The gateway is the publisher. It reads the data from the process station, establishes the communication with a cloud broker via the MQTT protocol and transfer the data. The gateway supports the connection to cloud systems that have a broker functionality, for example, MindSphere, Microsoft Azure, IBM Cloud or Amazon AWS.

The SIMATIC CC712 device enables the communication of a SIMATIC S7-300 / S7-400 / S7-1200 or S7-1500 controller via Industrial Ethernet with the S7 protocol. The SIMATIC CC716 device is intended for the connection of up to seven SIMATIC S7 controllers via Industrial Ethernet or a PROFIBUS/MPI interface.

- **Connection of a S7 process station to OPC UA clients:**

The gateway takes on the function of an OPC UA Server. It reads process data from the S7 CPU and, as an OPC UA Server, makes it available to one or more OPC UA Clients.

In this case, the gateway supports the following server functions:

- Reading and writing variables
- Monitoring variables using subscriptions
- Hierarchical address browsing

The device has an industry-suitable housing in the SIMATIC S7-1500 format in the degree of protection IP20 and is suitable for operating temperatures of -20 °C to +60 °C. It offers the following installation options: SIMATIC S7-1500 and S7-300 standard rail, standard DIN rail, on a base or wall mounting. The device is designed for usage in the control cabinet. The RJ45 sockets with securing collar provide additional strain and bend relief for the use of FastConnect connectors. The configuration data can be saved on the optionally available exchangeable storage medium Configuration License PLUG (CLP), which makes a device exchange easier.

Example of a topology

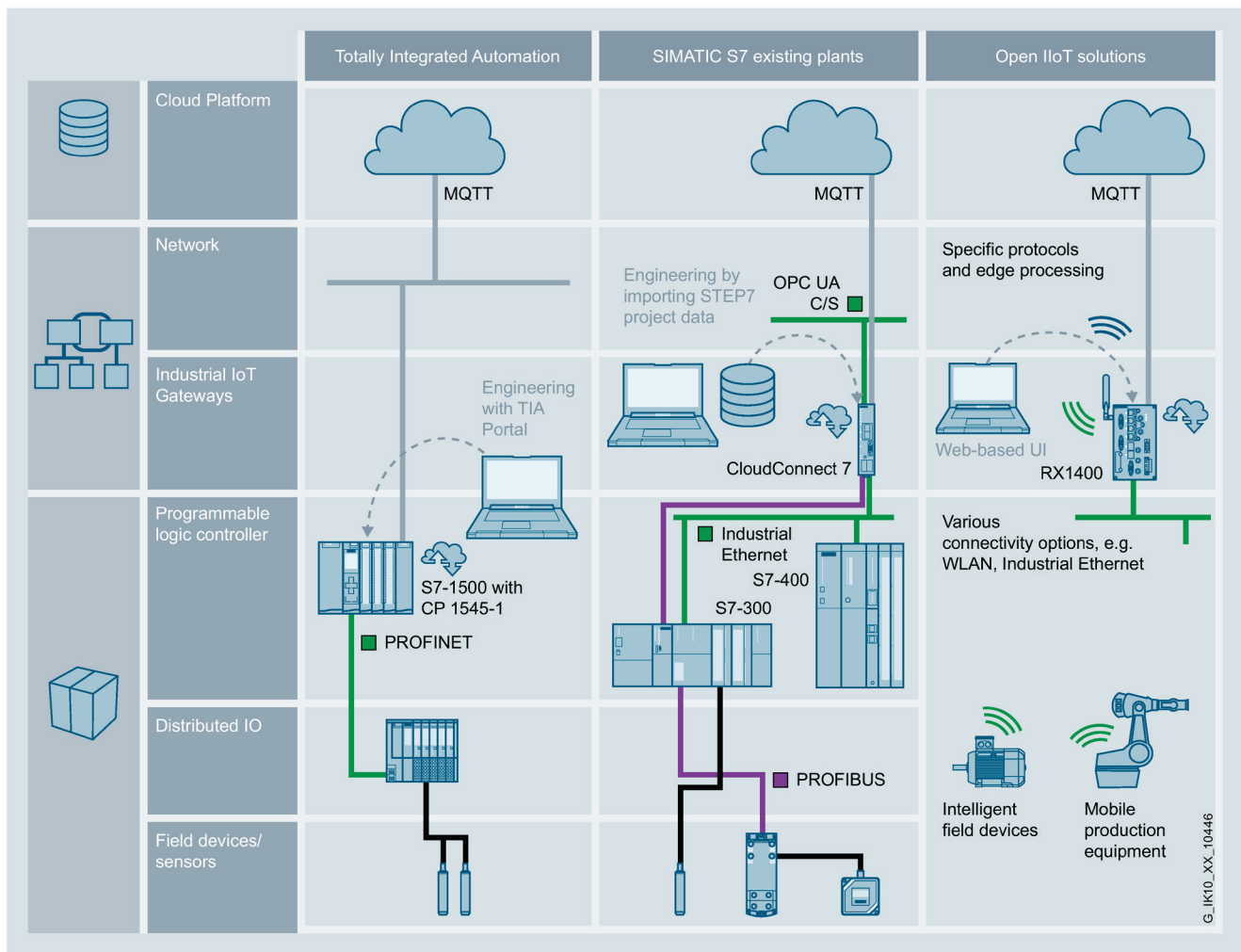


Figure 5-2 Connection options for CloudConnect 7

See also

Configuration License PLUG (CLP) (Page 285)

5.2 Features and functions

Features

The device has the characteristics shown in the following table:

	SIMATIC CC712	SIMATIC CC716
Diagnostics LED	•	•
On site display (Set button)	•	•
Power supply 24 V DC	•	•
Redundant power supply	•	•
CLP slot	•	•
Cloud interface	1x RJ45 (1000 Mbps)	1x RJ45 (1000 Mbps)
Interface for lower-level devices:		
Industrial Ethernet interface	1x RJ45 (1000 Mbps)	1x RJ45 (1000 Mbps)
PROFIBUS/MPI	-	1x RS485
Protocols:		
• S7	•	•
• Modbus TCP	•	•
• MPI	-	•
Number of automation devices	1	7
Total number of data points	500	3500

- Suitable / available or according to the specified standard

Functions

- Standard 1000BASE-T, IEEE 802.3ab with transmission rates 10/100/1000 Mbps
- Half duplex/full duplex, autocrossover, autonegotiation, Quality of Service
- Configuration using the WBM
- Web diagnostics via HTTPS
- Only HTTPS connections possible
- Configuration of the IP address with DHCP
- IP addresses according to IPv4 and IPv6
- Cloud interface
- OPC UA server function
- MQTT
- S7/ ModbusTCP
- MPI (only SIMATIC CC716)
- DNS server

- NTP/NTP (secure)
- Trigger Management: Event-driven/threshold/cyclic

5.3 Article numbers

Device	Description	Article number
SIMATIC CC712	Gateway for connection of a SIMATIC S7 or Modbus station to a cloud system or an OPC UA server for transmission of SIMATIC S7 data	6GK1411-0AC00
SIMATIC CC716	Gateway for connection of seven SIMATIC S7 controllers via Industrial Ethernet or PROFIBUS/MPI interface to a cloud system or an OPC UA server for transmission of SIMATIC S7 data	6GK1411-5AC00

TeleControl

6.1 SIMATIC RTU3000C

Overview

TeleControl means the monitoring and control of widely distributed process stations (RTUs / Remote Terminal Units) through one or more central control systems. The communication takes place via public networks, for example mobile wireless / Internet, or private networks with special transmission protocols. Both standard protocols (DNP3, IEC 60870) as well as Siemens protocols (SINAUT ST7, TeleControl Basic) are supported.

A distinction is made between compact and modular RTUs. This section describes the compact RTU series SIMATIC RTU3000C. You can find the the modular RTUs on the basis of SIMATIC S7-1200, ET 200SP, S7-1500 and S7-300/400 in section "Communications processors for SIMATIC S7 (Page 309)".

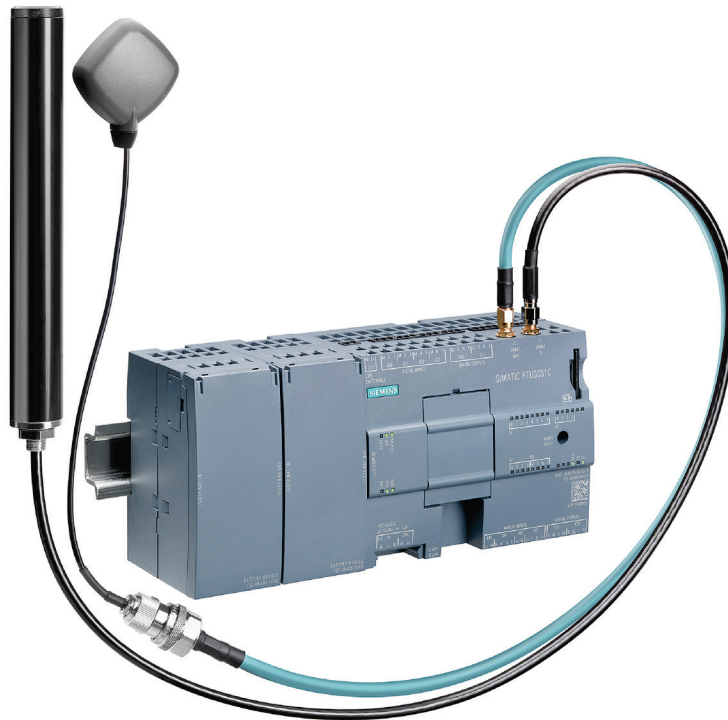


Figure 6-1 RTU3031C with two battery modules and antennas

The compact remote control units RTU (Remote Terminal Unit) offer secure monitoring and controlling of outlying stations that are located far from each other and from the control center and are not connected to a power supply network. The self-sufficient Low-Power RTUs are suitable in particular for usage in rugged environments of -40 to +70 °C, also without local power supply or communication infrastructure. An RTU can be supplied with the

12 - 24 V DC via the power supply unit. Optional modules are available for energy self-sufficient use cases: An accumulator with a solar panel or up to six redundant connectable battery modules. All options can be combined with each other.

The RTUs can be used for monitoring the following systems:

- Pumping stations and water storage for the detection of leaks
- Irrigation systems for gauge monitoring of standing and flowing waters
- Flood protection
- Remote inventory monitoring of levels in tanks and silos
- Wind measurements for design of wind turbines
- Positioning, for example, monitoring of floating buoys

You can find further telecontrol modules such as TIM 3V-IE, CP 1243-8 or TIM 1531 in section "Communications processors for SIMATIC S7 (Page 309)".

Example of a topology

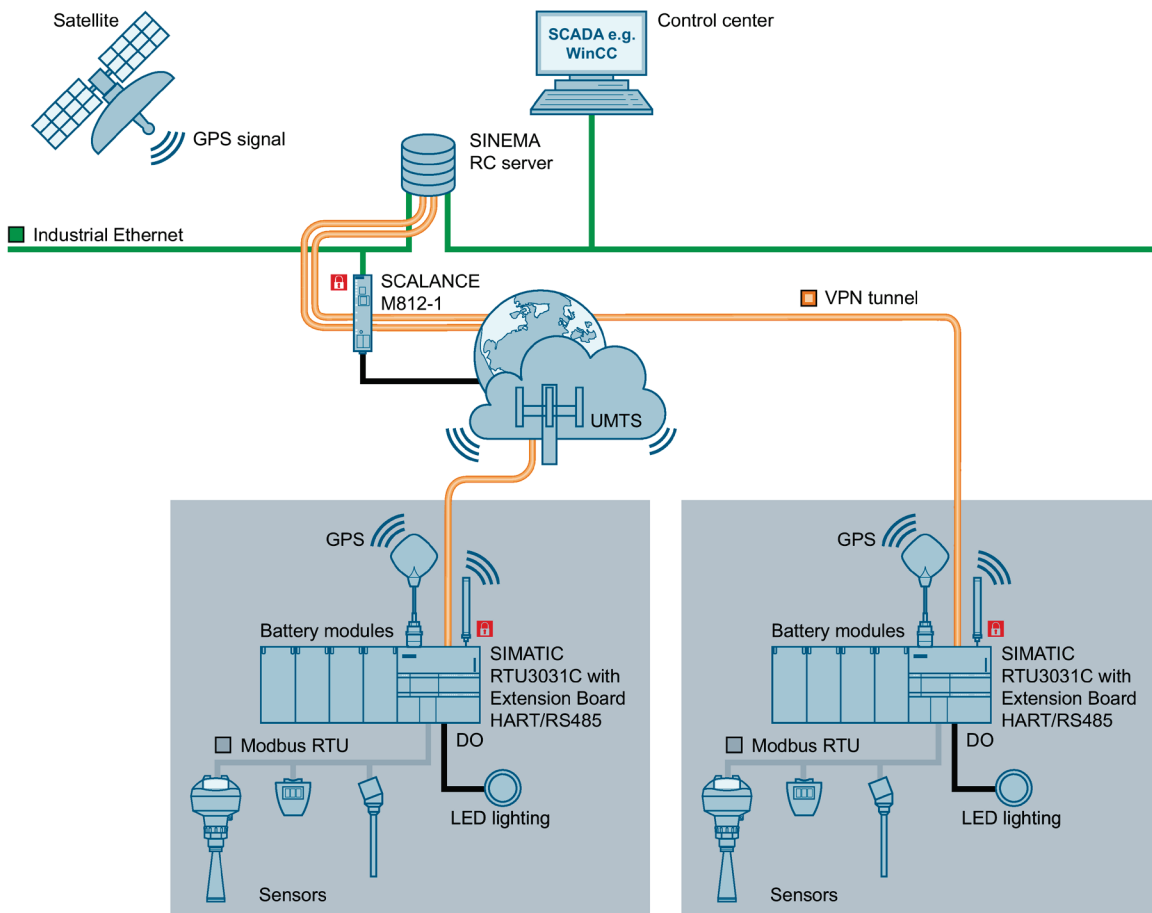


Figure 6-2 Example of a topology for the TeleControl network: SIMATIC RTU3031C connection incl. GPS positioning at a control center

6.2 Description

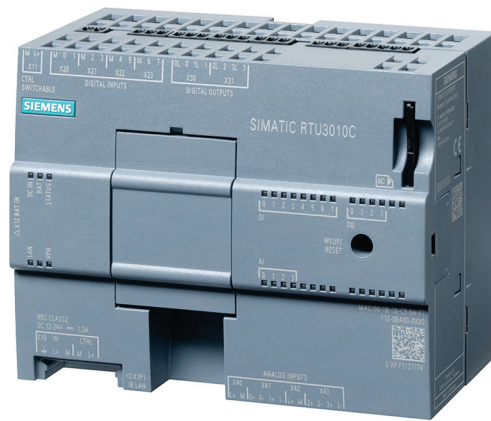


Figure 6-3 SIMATIC RTU3010C

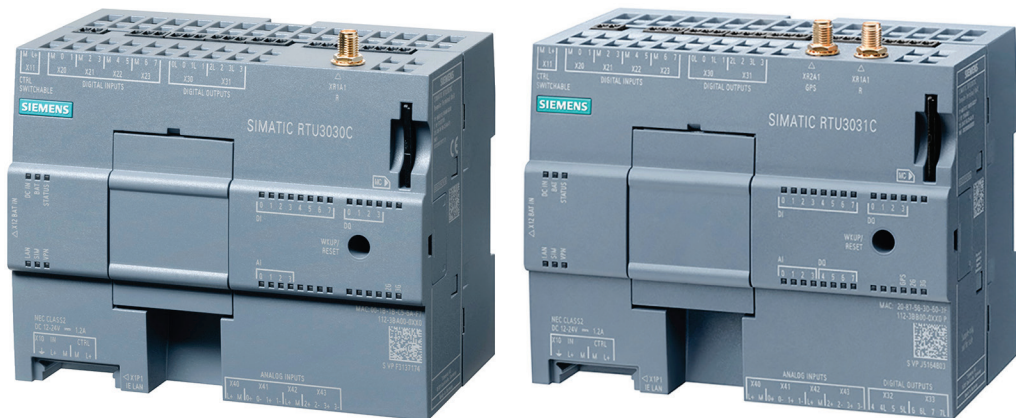


Figure 6-4 SIMATIC RTU3030C and RTU3031C

The remote control stations of the SIMATIC RTU3000C product line are used at remote measuring stations. An RTU is connected to the sensors of the measuring station and transfers recorded process values via the LAN interface and an external router to the central control center. When configurable limit values are exceeded, the RTU sends an alarm message to the central unit. This way an error state can be quickly detected and the error can be resolved. The RTU3031C and the RTU3041C can furthermore be located via GPS.

For connection to the sensors, the RTUs have up to 8 digital inputs and outputs as well as 4 analog inputs. With the optional extension board, eight additional sensors can be connected via Modbus RTU or HART Multidrop.

The RTUs are intended for the installation on a standard DIN rail. An optional protective housing in IP68 degree of protection enables the usage of a RTU in the flooding areas.

6.3 Features and functions

To ensure the self-sufficient operation and save energy, RTUs can switch between four different operating modes:

- **Sleep mode**
All inputs and communication functions are switched off so that energy consumption is minimal. Outputs can keep their last value.
- **Update mode**
The mode is used for querying the inputs and outputs. The query cycle can be configured individually.
- **Communication mode**
Cellular connection or connection via LAN interface and external router and communication to master station are active.
- **Service mode**
The maintenance work can be performed without the loss of data.

6.3 Features and functions

Features

The devices have the characteristics shown in the following table:

	RTU3010C	RTU3030C	RTU3031C	RTU3041C
Diagnostics LED	•	•	•	•
Redundant power supply	- 1)	- 1)	- 1)	- 1)
On site display (Set button)	•	•	•	•
Signaling contact	-	-	-	-
Communication	Any IP-based networks via external routers, for example SCALANCE M	2G, 3G via integrated modem or via external router	2G, 3G via integrated modem or via external router; GPS reception	2G, 3G via integrated modem or via external router; GPS reception
Automatic alerting via e-mail	•	•	•	•
Automatic alerting via SMS	-	•	•	•
Pre-processing of the recorded signals	•	•	•	•
Integrated UMTS modem	-	•	•	•
Antenna connection for GPS	-	-	•	•
SMA connector for GSM/GPRS/UMTS antenna	-	•	•	•
LTE-M/NB	-	-	-	•
Temperature sensor for monitoring the housing temperature	•	•	•	•
Slot for memory card (SD 1.0, SD 1.1, SDHC, Siemens SMC)	•	•	•	•

	RTU3010C	RTU3030C	RTU3031C	RTU3041C
Slot for SIM card	-	•	•	•
C-PLUG slot	-	-	-	-

- Suitable / available or according to the specified standard

1) A redundant power supply is possible through parallel connection to multiple energy suppliers: Combination of external power supply/battery modules/battery

Functions

All devices have the following functions:

- Web Based Management
- Configuration of the IP address with DHCP
- Communication with the master station with TeleControl Basic, SINAUT ST7, DNP3, IEC 60870-5-104
- NTP
- SNTP
- DHCP client
- OpenVPN

6.4 Interfaces

Device	RTU3010C	RTU3030C	RTU3031C	RTU3041C
Voltage supply via 5-pin plug-in terminal strip	1	1	1	1
Digital inputs (DI) / of which counter inputs	8 / 2	8 / 2	8 / 2	8 / 2
Digital outputs (DO)	4	4	8	8
Digital outputs (AI)	4	4	4	4
Analog inputs	-	-	2	2
Ethernet interface 10/100 Mbps for connection to external router	1x RJ45 ¹⁾	1x RJ45 ¹⁾	1x RJ45 ¹⁾	1x RJ45 ¹⁾
Antenna connection mobile wireless	-	1x SMA socket	1x SMA socket	1x SMA socket
Antenna connector GPS	-	-	1x SMA socket	1x SMA socket
Connection for battery modules	Max. 2x 3	Max. 2x 3	Max. 2x 3	Max. 2x 3

¹⁾ The LAN connector is not suitable for direct connection of the RTU to the Internet. To do this, an external router with suitable security mechanisms must be connected.

6.5 Article numbers

Device	Description	Article number
SIMATIC RTU3010C	Compact low power RTU	6NH3112-0BA00-0XX0
SIMATIC RTU3030C	Compact low power RTU, integrated UMTS modem	6NH3112-3BA00-0XX0
SIMATIC RTU3031C	Compact low power RTU, integrated UMTS modem, GPS	6NH3112-3BB00-0XX0
SIMATIC RTU3041C	Compact low power RTU, integrated LTE-M/NB modem, GPS	6NH3112-4BB00-0XX0

Accessories

The following products are currently released for usage with SIMATIC RTU3000C:

Component	Description	Article number
Extension Board HART/RS485	Extension Board HART/RS485 for Low Power RTU3000C family; connection of 8 Modbus RTU slaves or 8 HART devices in multi-drop mode	6NH3112-3BA00-6XX1
Battery module	Battery housing for storing of two D cells	6NH3112-3BA00-1XX2
Battery module	Battery extension housing for storing of two D cells	6NH3112-3BA00-1XX6
IP68 housing	Stainless steel housing in IP68 degree of protection, suitable for SIMATIC RTU3030C, temperature range -60 to +135 °C	6NH3112-3BA00-1XX1
IP68 housing	Aluminum housing in IP68 degree of protection, suitable for SIMATIC RTU3030C, temperature range -40 to +80 °C	6NH3112-3BA00-1XX3

Note

For devices with SMA socket, the antennas listed in the section "SCALANCE W components for the Industrial Wireless LAN" can be used. For further information, refer to the section "Product overview (Page 236)".

Communications processors for PCs

Overview

Communication 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 communication processors for PCs/PGs:

- Communication 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).
- Communication processors without their own microprocessor.
These communication processors are less expensive than the communication processors that have their own microprocessor. If there is, however, a 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 communication processors with their own microprocessor are used this does not occur.

Device versions

Functionality	CP 1604 EEC	CP 1616	CP 1623	CP 1626	CP 1628
PCI interface	-	•	-	-	-
PCI Express interface	-	-	•	•	•
PCI-104 interface	•	-	-	-	-
RJ45 connections	4	4	2	4	2
Configurable connections	128	128	120	256	512
Gigabit Ethernet	-	-	•	-	•
Integrated switch	•	•	•	•	•
PN IO	•	•	-	•	-

- Suitable / available or according to the specified standard

Example of a topology

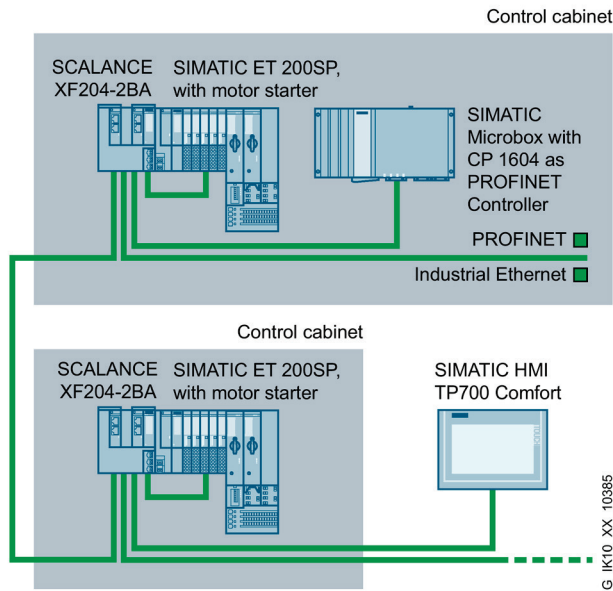


Figure 7-1 Connection of PROFINET nodes via CP1604 to Industrial Ethernet

7.1 CP 1604

Description

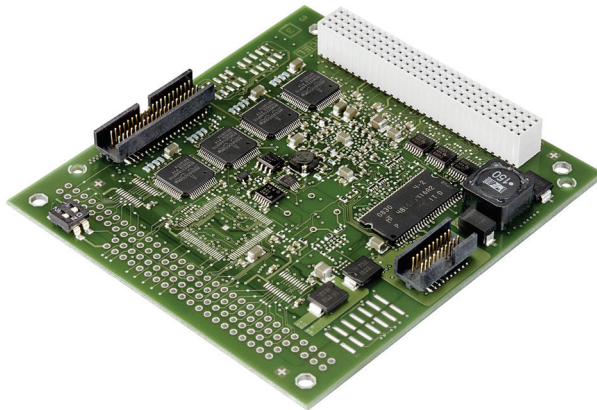


Figure 7-2 CP 1604 EEC

The CP 1604 is a PCI-104 card with its own microprocessor Ethernet real-time ASIC ERTEC 400 which supports PN IO communication. This module has an integrated 4-port real-time switch for 10/100 Mbps.

Features

	CP 1604 CP 1604 EEC
Required slot on the PC	PCI-104 (32-bit)
Number and type of the interfaces for Industrial Ethernet	4x RJ45
Gigabit Ethernet	-
Own microprocessor	•
Optional external power supply 12 ... 24 VDC	•

Functions

- Up to 128 connections can be configured at one time
- Transmission rates 10/100 Mbps (half/full duplex)
- Autocrossover and autonegotiation
- Ring redundancy with redundancy manager
- 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

Component	Description	Article number
CP 1604	Communication processor PC/104 plus card (32-bit; 33/66 MHz; 3.3/5 V) with ASIC ERTEC 400 for connection to PROFINET IO with 4-port real-time switch	6GK1160-4AA01
CP 1604 EEC	Communication processor PC/104 plus card (32-bit; 33/66 MHz; 3.3/5 V) with ASIC ERTEC 400 for connection to PROFINET IO with 4-port real-time switch, version suitable for railways	6GK1160-4AT01

7.2 CP 1616

Description

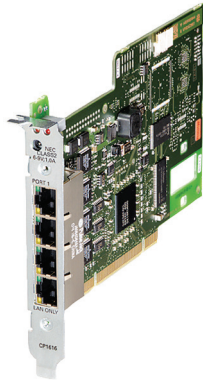


Figure 7-3 CP 1616

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; 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	4x RJ45
Gigabit Ethernet	-
Own microprocessor	•
Optional external power supply 6 ... 9 VDC	•

Functions

- Up to 128 connections can be configured at one time
- Transmission rates 10/100 Mbps (half/full duplex)
- 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

Component	Description	Article number
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 (RJ45); including IO-Base software for PROFINET IO controller and NCM PC	6GK1161-6AA02

7.3 CP 1623

Description



Figure 7-4 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 x1
Number and type of the interfaces for Industrial Ethernet	2x RJ45
Gigabit Ethernet	•
Own microprocessor	•
Optional external power supply 12 ... 24 VDC	•

Functions

- Up to 120 connections can be configured at one time
- Transmission rates 10/100/1000 Mbit/s (half/full duplex)

- Autosensing, 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

Component	Description	Article number
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

7.4 CP 1626

Description



Figure 7-5 CP 1626

The CP 1626 is a PCI Express card with its own microprocessor and two integrated 2-port real-time switches for connecting PCs and SIMATIC PG/PC to PROFINET IO.

The module is designed for the operating voltage 3.3 V / 12 V via PCI. External 12 - 24 V DC power supply to allow operation of switches when the PC/PG is turned off.

Features

	CP 1626
Required slot on the PC	PCI Express x1
Number and type of the interfaces for Industrial Ethernet	4x RJ45
Gigabit Ethernet	-
Own microprocessor	•
Optional external power supply 12 to 24 V DC	•

Functions

- In PROFINET IO controller mode, up to 256 PN IO RT devices or 64 PN IO IRT devices can be operated.
In PROFINET IO devices mode, up to 512 submodules can be operated.
- Transmission rate 100 Mbps
- Autosensing, autocrossover and autonegotiation
- IRT (Isochronous Real Time)
- LLDP
- DCP
- 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

Component	Description	Article number
CP 1626	Communication processor for connecting to PROFINET IO as a controller and device with main supply disconnection and series machines support, with Ethernet real-time ASICs	6GK1162-6AA01

7.5 CP 1628

Description

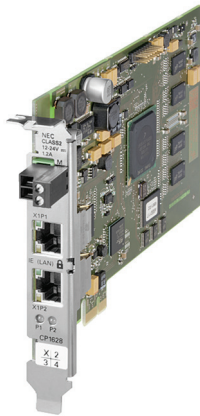


Figure 7-6 CP 1628

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 x1
Number and type of the interfaces for Industrial Ethernet	2x RJ45
Gigabit Ethernet	•
Own microprocessor	•
Optional external power supply 12 ... 24 VDC	•

Functions

- Up to 512 connections can be configured at one time
- Transmission rates 10/100/1000 Mbit/s (half/full duplex)
- Autosensing, autocrossover and autonegotiation
- Time-of-day synchronization
- DCP
- Network management and diagnostics using SNMP

- 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

Component	Description	Article number
CP 1628	PCI Express x1 card for connection to Industrial Ethernet (10/100/1000 Mbps), with 2-port switch (RJ45) and integrated security (firewall, VPN) via HARDNET-IE S7 and S7 REDCONNECT; Support of operating systems according to the SIMATIC NET software	6GK1162-8AA00

Communications processors for SIMATIC S7

Overview

For each SIMATIC S7 system there are communications processors that provide a connection of a station (the so called system connection) to a communication network. This means that S7 controllers can exchange data with other network nodes via Industrial Ethernet or PROFIBUS. These network nodes can be other S7-CPs/CPUs or PCs with an Ethernet card. This makes remote programming and diagnostics via the PG/PC possible. With the communications processors that support PROFINET, PROFINET IO-compliant field devices can be addressed directly.

Device versions

The following figure shows the various device types and the corresponding categories of the SIMATIC S7 product line.

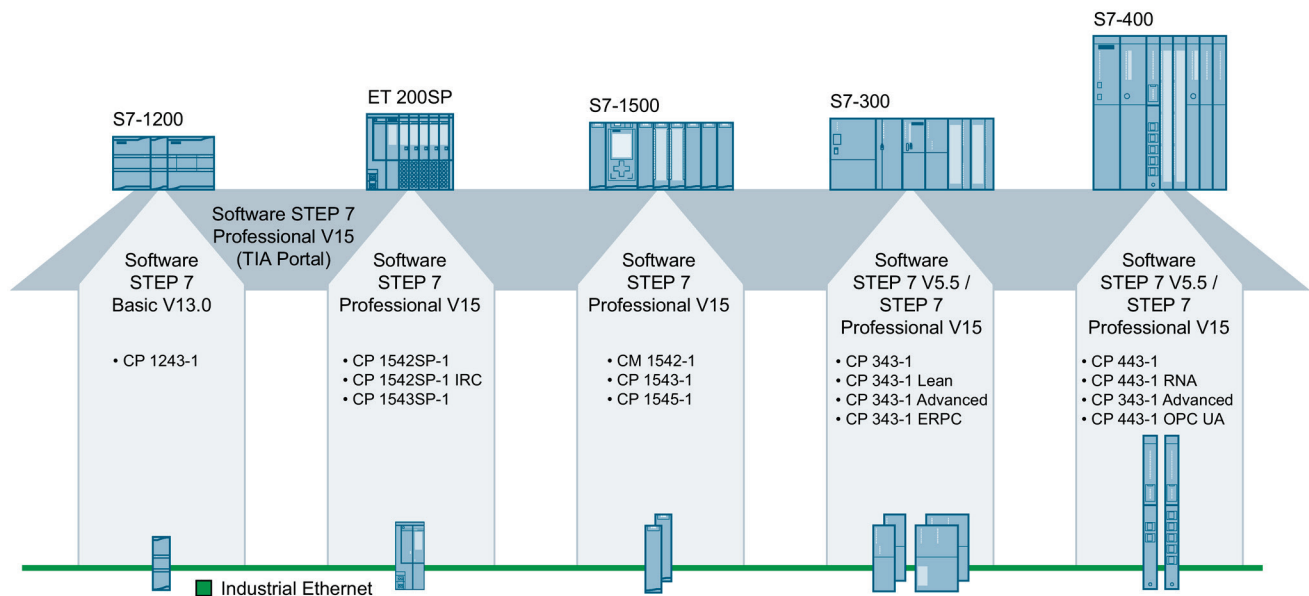


Figure 8-1 SIMATIC S7: CP communication processors for Industrial Ethernet

Example of a topology

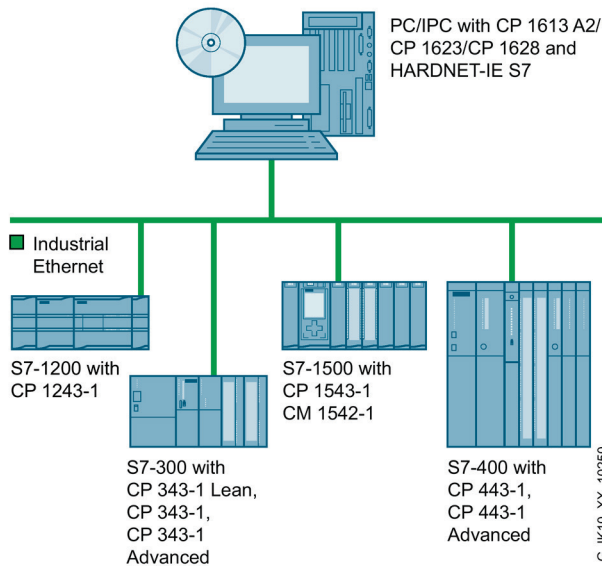


Figure 8-2 Connecting S7 systems to Industrial Ethernet based on the example of a linear bus topology

8.1 SIPLUS version

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, two upgraded SIPLUS versions are available.

- For an expanded temperature range of -25 °C to +60 °C, some devices up to +70 °C.
- With conformal coating for extreme ambient conditions and for use on rolling stock according to EN 50155.

Note
SIPLUS

Detailed information and the technical documentation on SIPLUS is available under: SIPLUS (<https://w3.siemens.com/mcms/siplus/en/siplus-extreme/Pages/Default.aspx>)

8.2 Communications processors for SIMATIC S7-300

Description



Figure 8-3 SIMATIC S7-300: CP 343-1 ERPC

The communication processors of the category SIMATIC S7-300 have a rugged plastic housing for installation on an S7-300 standard rail. The connection to S7-300 components is made via a backplane bus.

Features

	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 V DC	•	•	•	•
Connectors Industrial Ethernet / PROFINET	1x RJ45	2x RJ45	2x RJ45	2x RJ45
Integrated 2-port switch	-	•	•	•

	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
Gigabit interface	-	-	•	•
30 MB flash memory / 28 MB RAM	-	-	•	-
C-PLUG supplied	-	-	•	•

• Suitable / available or according to the specified standard.

Functions

The communications processors of this category support the following protocols and technologies:

Protocol / function	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):
 - In an Ethernet network with ring topology, the communication 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 programming device by storing the configuration data on the CPU
- Connection for connecting SIMATIC S7-300 systems to Industrial Ethernet, except for SINUMERIK
 - Two RJ45 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 the 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 as well as via 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 RJ45 connectors
- 10/100 Mbps, full / half duplex with the functionality for autosensing as well as 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 to be carried out
- 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):
 - In an Ethernet network with ring topology, the CP 343-1 supports the media redundancy protocol MRP
- Diagnostics and network management:
 - Extensive diagnostic functions of all modules within the racks
 - 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 programming device by storing the configuration data on the CPU
- SIPLUS CP 343-1

The SIPLUS CP 343-1 module is designed 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 secure Web browser.
- An integrated ESMTP 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 device 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 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

Device	Description	Article number
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	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, MRP, integrated 2-port switch ERTEC	
	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	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	
	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 connection to SIMATIC S7-300 in Industrial Ethernet; 1x 10/100/1000 Mbps; 2 x 10/100 Mbps (IE SWITCH); RJ45 ports; TCP; UDP; ISO; PROFINET IO controller and IO device, S7 communication (Client and Server); Open communication (SEND/ RECEIVE)	
	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 connection to SIMATIC S7-300 in Industrial Ethernet; 1x 10/100/1000 Mbps; 2 x 10/100 Mbps (IE SWITCH); RJ45 ports; TCP; UDP; ISO; PROFINET IO controller and IO device, S7 communication (Client and Server); Open communication (SEND/ RECEIVE) 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	6GK7343-1FX00-0XE0

8.3 Communications processors SINAUT ST7 for SIMATIC S7-300

Description



Figure 8-4 SINAUT TIM 3V-IE

The SINAUT ST7 TIM communication 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

	TIM 3V-IE	TIM 3V-IE Ad- vanced	TIM 3V-IE DNP3	TIM 4R-IE	TIM 4R-IE DNP3
RS 232 connections for external data transfer	1x D-sub 9-pin	1x D-sub 9-pin	1x D-sub 9-pin	2x D-sub 9-pin	2x D-sub 9-pin
Connections for Industrial Ethernet	1x RJ45	1x RJ45	1x RJ45	2x RJ45	2x RJ45
External power supply 24 V DC	2-pin plug-in terminal strip	2-pin plug-in terminal strip	2-pin plug-in terminal strip	2-pin plug-in terminal strip	2-pin plug-in terminal strip
Number of active connections multiprotocol mode	12	24	-	128	-
No. of TIMs per S7-300	1	Multiple ¹⁾	1	Multiple ¹⁾	1
C-PLUG	-	-	-	Optional	Optional

• Suitable / available or according to the specified standard.

¹⁾ Depending on the connection resources of the CPU

Functions

The communications processors of this category support the following protocols:

Protocol / function	TIM 3V-IE	TIM 3V-IE Advanced	TIM 3V-IE DNP3	TIM 4R-IE	TIM 4R-IE DNP3
TCP/IP	•	•	•	•	•
DNP3	-	-	•	-	•
SINAUT ST1	•	•	-	•	-
SINAUT ST7	•	•	-	•	-
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

Device	Description	Article number
TIM 3V-IE	Communication module for SIMATIC S7-300; 1x RS 232 interface for SINAUT communication via WAN and 1x RJ45 interface for SINAUT communication via an IP-based network	6NH7800-3BA00
TIM 3V-IE Advanced	Communication module for SIMATIC S7-300; 1x RS 232 interface for SINAUT communication via WAN and 1x RJ45 interface for SINAUT communication via an IP-based network	6NH7800-3CA00
TIM 3V-IE DNP3	Communications module for SIMATIC S7-300; 1x RS 232 interface for DNP3 communication via a WAN and 1x RJ45 interface for DNP3 communication via an IP-based network	6NH7803-3BA00-0AA0
TIM 4R-IE	Communication module for SIMATIC S7-300; 2x RS 232 interface for SINAUT communication via WAN and 2x RJ45 interfaces for SINAUT communication via an IP-based network	6NH7800-4BA00
TIM 4R-IE DNP3	Communication module for SIMATIC S7-300; 2x RS 232 interface for DNP3 communication via WAN and 2x RJ45 interfaces for DNP3 communication via an IP-based network	6NH7803-4BA00-0AA0

8.4 Communications processors for SIMATIC S7-400

Description



Figure 8-5 CP 443-1, CP 443-1 Advanced, CP 443-1 RNA and CP 443-1 OPC UA

The communication processors of the category SIMATIC S7-400 have a rugged plastic housing for installation on an S7-400 rack. The connection to S7-400 components is made via a backplane bus.

Features

	CP 443-1 SIPLUS CP 443-1	CP 443-1 Advanced SIPLUS CP 443-1 Advanced	CP 443-1 RNA	CP 443-1 OPC UA
Connectors Industrial Ethernet / PROFINET	2x RJ45	5x RJ45	3x RJ45	1x RJ45
Integrated switch	●	●	-	-
Gigabit interface	-	●	-	●
30 MB flash memory / 28 MB RAM	-	●	-	-
C-PLUG supplied	-	●	-	-

- Suitable / available or according to the specified standard.

Functions

The communications processors of this category support the following protocols and technologies:

Protocol / function	CP 443-1 SIPLUS CP 443-1	CP 443-1 Advanced SIPLUS CP 443-1 Ad- vanced	CP443-1 RNA		CP 443-1 OPC UA
			Ethernet interface	RNA inter- face	
PROFINET					
→ IO controller	•	•	-	-	-
→ IO device	-	-	-	-	-
→ CBA	-	•	-	-	-
IT ¹⁾	• (only Web serv- er)	•	-	-	-
IP-R ²⁾	-	•	-	-	-
MRP	•	•	-	-	-
PRP	-	-	-	•	-
FTP	-	•	-	-	-
S7 communication					
→ Programming device function, operator con- trol and monitoring	•	•	• (only ISO)	•	-
→ Data exchange	•	•	• (only ISO)	•	-
SEND/ RECEIVE					
→ ISO transport con- nection	•	•	•	•	-
→ TCP, ISO-on-TCP, UDP	•	•	-	•	-
→ Multicast through UDP	•	•	-	•	-
→ FETCH/WRITE	•	•	• (only ISO)	•	-
Open TCP/IP communi- cation	•	•	-	•	•
PG/OP communication	•	•	•	•	•
Communication via OPC UA					
→ As an OPC UA server	-	-	-	-	•
→ As an OPC UA client	-	-	-	-	•
Firewall and VPN (IP- sec)	-	•	-	-	-

• 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

*) Only web server

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.
- 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 communication services operate via the following interfaces:
 - Open communication (TCP/IP and UDP), multicast for the 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, such as for HMI
- Media redundancy (MRP):
 - In an Ethernet network with ring topology, the communication 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 RJ45 connection for 10/100/1000 Mbps full / half duplex with the autosensing functionality.
 - PROFINET interface with four RJ45 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 device 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 modes:
 - 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 factory-set 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 time-consuming 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)

CP 443-1 OPC UA

The CP 443-1 OPC UA is designed to connect a SIMATIC S7-400 system to Industrial Ethernet networks via OPC UA mechanisms.

The communication processors support:

- PG/OP communication
- Communication via OPC UA as OPC UA server and/or OPC UA client for exchanging process data (data access)

With this CP, the SIMATIC S7-400 control unit exchanges data via a standardized OPC UA interface with other nodes. The CP can be used as OPC UA Server and/or OPC UA Client. The communication as OPC UA Client takes place via the application blocks standardized by the PLCOpen organization.

The device has the following additional characteristics and functions:

- 1x RJ45 socket for the connection to Industrial Ethernet with 10/100/1000 Mbps (full/half duplex)
Connection is possible via an IE FC RJ45 Plug 180 with 180° cable outlet or via a standard patch cable.
- Automatic data rate detection with autonegotiation and autocrossover function.
- Diagnostic LEDs for displaying the operational and communication status.
- Fanless operation of the communication processor
- The communication services operate via the following interfaces:
 - As an OPC UA server: Read/write access for data exchange (DA), access via subscriptions
 - As an OPC UA client: Read/write access for data exchange (DA). Communication via standardized function blocks according to PLCOpen
 - Programming device communication via configuration of the CP, internetworking with S7 routing
 - Forwarding the time to the CPU as NTP time client (optional secure NTP) module replacement without programming device: All configuration information is stored on the CPU
 - The CP can operate simultaneously as an OPC UA Server and OPC UA Client. Corresponding restrictions of the configuration limit can be found in the manual
- Diagnostics and network management:
 - With HTTPS via a Web browser
 - Standard diagnostics and extended diagnostics in STEP 7
 - Integration in network management systems by supporting SNMP V1/ V3
- Security mechanisms:
 - Access protection through authentication via certificate, encryption and signing of data
 - HTTPS communication with the webserver
- A wide range of diagnostic options with LEDs, in STEP 7 and Web-based diagnostic units with monitoring by IT network management tools (SNMP V1 MIB II)
- Configuration of all functions with STEP 7 as of V5.5
- Configuration with STEP 7 Professional V14 or higher
- Module replacement without programming device by storing all data on the CPU

Article numbers

Device	Description	Article number
CP 443-1	Communication processor for connection of SIMATIC S7-400 to Industrial Ethernet 2x 10/100 Mbps RJ45; TCP/IP, ISO and UDP; PROFINET IO controller, MRP, integrated real-time switch ERTEC with two ports	6GK7443-1EX30-0XE0
SIPLUS CP 443-1	Communication processor for connection of SIMATIC S7-400 to Industrial Ethernet 2x 10/100 Mbps RJ45; TCP/IP, ISO and UDP; PROFINET IO controller, MRP, integrated real-time switch ERTEC with two ports Ambient temperature from 0 °C to +60 °C, for harsh environmental loads	6AG1443-1EX30-4XE0
CP 443-1 Advanced	Communication processor for connection of the SIMATIC S7-400 CPU to Industrial Ethernet 1x 10/100/1000 Mbps and 4x 10/ 100 Mbps RJ45 ports; ISO, TCP, UDP, PROFINET IO controller, S7 communication; S7 routing, IP configuration via DHCP/ block; access protection with IP ACL, with security function: Firewall and VPN	6GK7443-1GX30-0XE0
SIPLUS CP 443-1 Advanced	Communication processor for connection of SIMATIC S7-400 CPU to Industrial Ethernet 1x 10/100/1000 Mbps and 4x 10/100 Mbps RJ45 ports; ISO, TCP, UDP, PROFINET IO controller, S7 communication; S7 routing, IP configuration via DHCP/ block; access protection with IP ACL, with security function: Firewall and VPN Ambient temperature from 0 °C to +60 °C, for harsh environmental load	6AG1443-1GX30-4XE0
CP 443-1 RNA	Communication processor for connection of SIMATIC S7-400 to Industrial Ethernet 1x 10/100 Mbps RJ45 port; TCP/ IP, ISO and UDP, S7 communication, 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	6GK7443-1RX00-0XE0
CP 443-1 OPC UA	Communication processor for connecting a SIMATIC S7-400 to Industrial Ethernet networks via OPC UA mechanisms (Data Access), 1x 10/100/1000 Mbps RJ45 port	6GK7443-1UX00-0XE0

8.5 Communications processors for SIMATIC S7-1200

Description

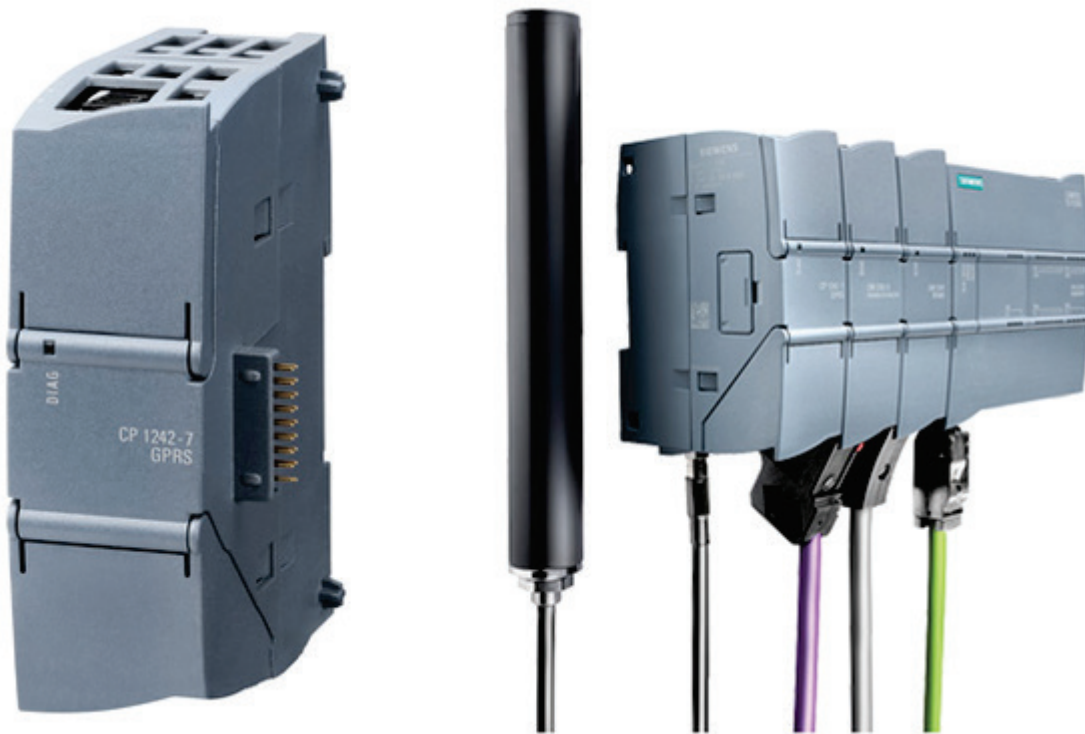


Figure 8-6 SIMATIC S7-1200: CP 1242-7 (GPRS) and communication with S7-1200

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 a second interface can be configured via an optional TS module. The Ethernet interface is intended for connection to router. This allows to implement remote terminal units that transmit 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.

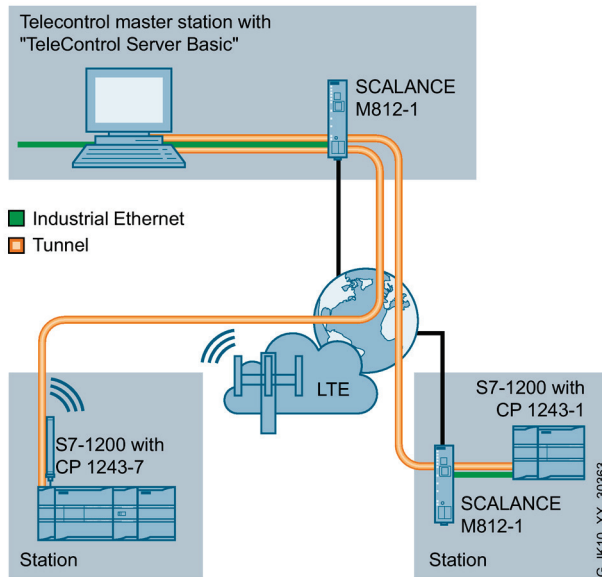


Figure 8-7 Example of the configuration for connecting two stations with a CP 1243-7 and a CP 1243-1

The following product variants exist:

Modules with Ethernet interface

- **CP 1243-1**
for connecting SIMATIC S7-1200 to TeleControl Server Basic
- **CP 1243-8 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 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.
- **CP 1243-7 LTE US**
for connecting SIMATIC S7-1200 to TeleControl Server Basic via an LTE network with the frequencies used in the US.

Features

The devices have the features listed in the table:

	CP 1243-1	CP 1243-8 IRC	CP 1242-7 V2 CP 1243-7 LTE
RJ45 interface Industrial Ethernet	•	•	-
Interface / TS module	-	•	-
SMA socket for external antenna	-	-	•
External power supply via 3-pin terminal strip	-	•	•

- Suitable / available or according to the specified standard.

Functions

The communication processors of this category support the following protocols:

Protocol / function	CP 1243-1	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 conforming to DNP3	•	•	-	-
→ Control room conforming to IEC 60870-5	•	•	-	-
→ Control room conforming to ST7	-	•	-	-
Firewall	•	•	-	•
VPN with IPsec	•	•	-	•
SNMPv1	-	-	-	-
SNMPv3	-	•	-	-
DCP	-	•	-	-
NTP	•	•	•	•

Article numbers

Device	Description	Article number
CP 1243-1	For connecting SIMATIC S7-1200 to TeleControl Server Basic	6GK7243-1BX30-0XE0
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⁾
CP 1243-7 LTE US	For connecting SIMATIC S7-1200 to TeleControl Server Basic via an LTE network with the frequencies used in the U.S.	6GK7243-7SX30-0XE0 ¹⁾

¹⁾ Note the national approvals in: Approvals (<https://www.siemens.com/mobilenetwork-approvals>)

8.6 Communications processors for SIMATIC S7-1500

Description



Figure 8-8 Communication processors CP 1543-1 and CP 1545-1

The communications modules for the SIMATIC S7-1500 connect the S7-1500 controllers to Industrial Ethernet or PROFINET.

CM 1542-1

The communication module CM 1542-1 expands an S7-1500 control system by a PROFINET connection which is 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 figure shows an application example of the network separation with an CM1542-1:

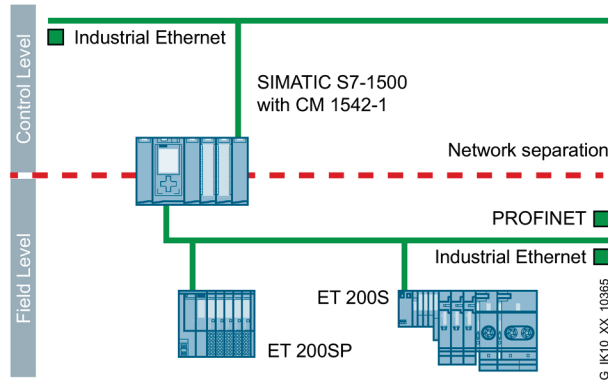


Figure 8-9 PROFINET segment with a CM1542-1

CP 1543-1

This communication processor CP 1543-1 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 rates 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 SIPLUS product variant comes with coated PCBs (conformal coating) and is designed for usage in extended temperature ranges $-40\text{ }^{\circ}\text{C}$ to $+60\text{ }^{\circ}\text{C}$.

The figure shows an application example:

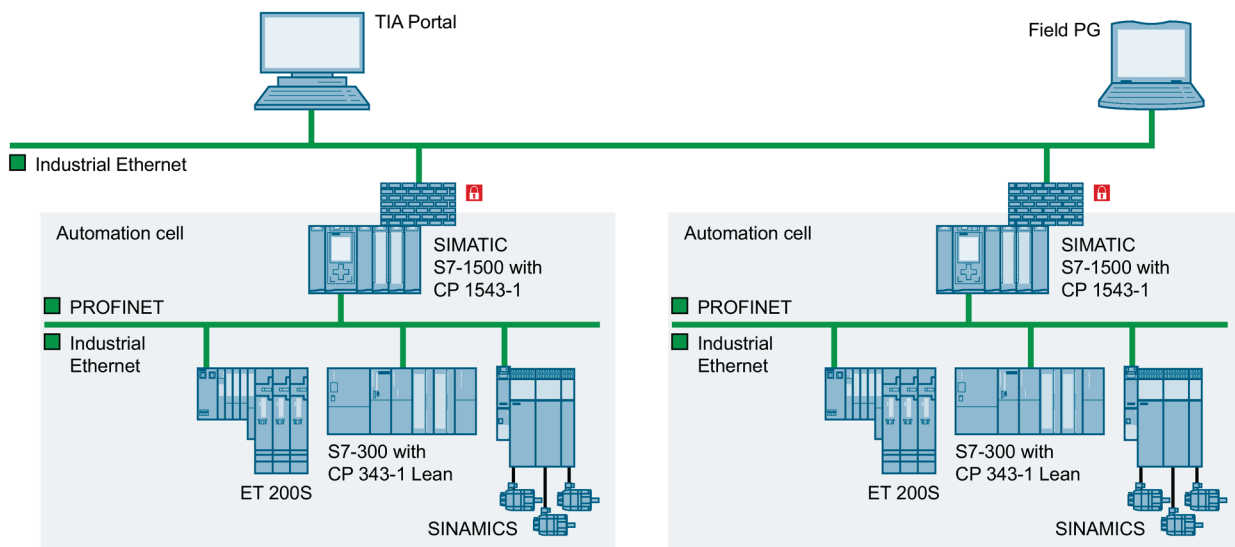


Figure 8-10 Protection and segmentation by firewalls with the CP 1543-1

CP 1545-1

The communication processor CP 1545-1 with CloudConnect functionality transfers data recorded by SIMATIC S7-1500 to MindSphere or a cloud solution that supports the standardized MQTT protocol, for example, Microsoft Azure or IMB Cloud. Through the integrated firewall with Stateful Packet Inspection, the CP protects the SIMATIC S7-1500 station against unauthorized access.

Die CloudConnect function can be configured in TIA Portal in just a few steps.

The CP 1545-1 enables the integration in an IPv6 infrastructure: Parallel to the connection to cloud applications, it supports the connection to other automation devices, such as HMI, via Industrial Ethernet using the SIMATIC S7 protocol.

The figure shows an application example:

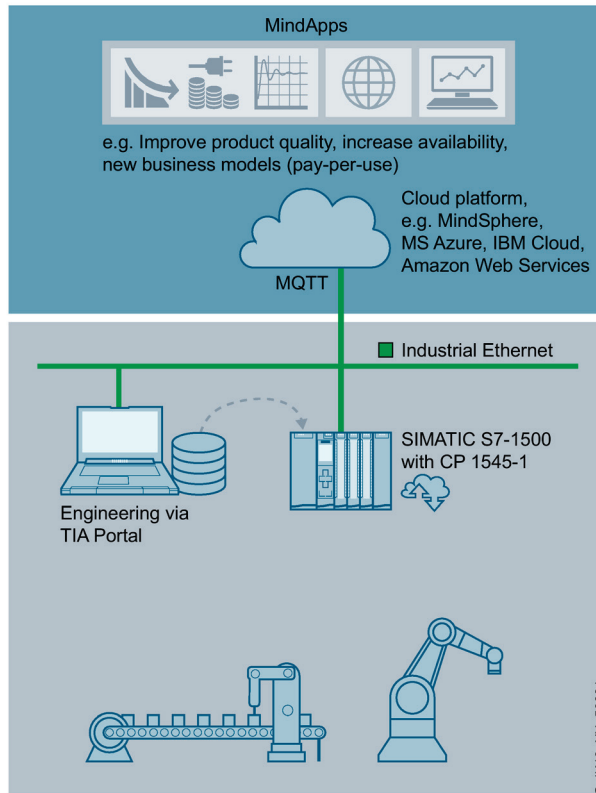


Figure 8-11 Cloud connection with SIMATIC CP 1545-1 as part of modern TIA systems

Features

The devices have the features listed in the table:

	CM 1542-1	CP 1543-1 SIPLUS CP 1543-1	CP 1545-1
Power supply	15 VDC via backplane bus	15 V DC via backplane bus	15 V DC via backplane bus
Connection Industrial Ethernet	2x RJ45 (switched)	1x RJ45	1x RJ45
Transmission rate	10/100 Mbps	10 / 100 / 1000 Mbps	10/100/1000 Mbps
Number of active connections for multiprotocol mode	64	118	118

- Suitable / available or according to the specified standard.

Functions

The communication processors of this category support the following protocols and technologies:

Protocol / function	CM 1542-1	CP 1543-1 SIPLUS CP 1543-1	CP 1545-1
IPv6	-	•	•
TCP/IP	•	•	•
UDP	•	•	•
PROFINET IO controller/device	•	-	-
ISO	-	•	•
Redundancy manager	•	-	-
Firewall	-	•	•
VPN with IPsec	-	•	
SNMPv1	•	•	•
SNMPv3	-	•	•
DCP	•	•	•
LLDP	•	-	•
NTP	•	•	•
MQTT	-	-	•

- Suitable / available or according to the specified standard.

Article numbers

Device	Description	Article number
CM 1542-1	Communication module for connection of S7-1500 to PROFINET as an IO controller with 2x RJ45 ports to the Ethernet interface	6GK7542-1AX00-0XE0
CP 1543-1	Communication processor for connecting an S7-1500 to Industrial Ethernet with 1x RJ45 port on the Ethernet interface. IT functions (FTP, HTTP, e-mail) and security functions (firewall, VPN with IPsec)	6GK7543-1AX00-0XE0
SIPLUS CP 1543-1	Communication processor for connecting SIMATIC S7-1500 to Industrial Ethernet: 1x RJ45 (10/100/1000 Mbps); based on 6GK7543-1AX00-0XE0 with coated PCBs (conformal coating) for extended temperature ranges -40 °C to +60 °C, start up -25 °C	6AG1543-1AX00-2XE0
CP 1545-1	Communication processor for connecting SIMATIC S7-1500 to Industrial Ethernet; TCP/IP, UDP, S7 communication, security (firewall), SNMPv1/v3, DHCP, FTP client/server, e-mail, IPv4/IPv6, time synchronization via NTP, connection to cloud systems via MQTT, 1x RJ45 (10/100/1000 Mbps)	6GK7545-1GX00-0XE0

8.7 Communication module TIM 1531 IRC

Description



Figure 8-12 TIM 1531 IRC for SIMATIC S7-1500

The TIM 1531 IRC is a communication module for TeleControl applications for the SIMATIC automation systems S7-300, S7-400 and S7-1500. The TIM is designed as an independent device and can be used as a substation, node station or central station. It is equipped with three Ethernet interfaces for TeleControl communication via IP-based WAN/LAN networks and with a serial interface for communication via classic WAN networks.

By means of the TIM, SIMATIC stations can be connected via public or private infrastructures to a TeleControl master station. In this case, one local CPU is assigned to the TIM. As a standalone device, the TIM is not dependent on the S7 device family or rack type of the assigned CPU.

The following protocols can be selected for TeleControl communication:

- SINAUT ST7
- IEC 60870-5-101/104
- DNP3

The TIM has its own processors and a RAM memory for buffering data frames and events. This way data losses during a connection failure or the failure of a communication partner are avoided. In addition, the TIM 1531 IRC provides the option of using media redundancy over physically separate connection paths without data loss at the changeover.

Examples of a topology

Use as node station

In a node/master station with a SIMATIC S7-1500, the TIM 1531 IRC is connected to the S7-1500 and the control center via one of its three Ethernet interfaces and can exchange data with the lower-level stations, for example, via other Ethernet interfaces with path redundancy.

The figure shows an application example:

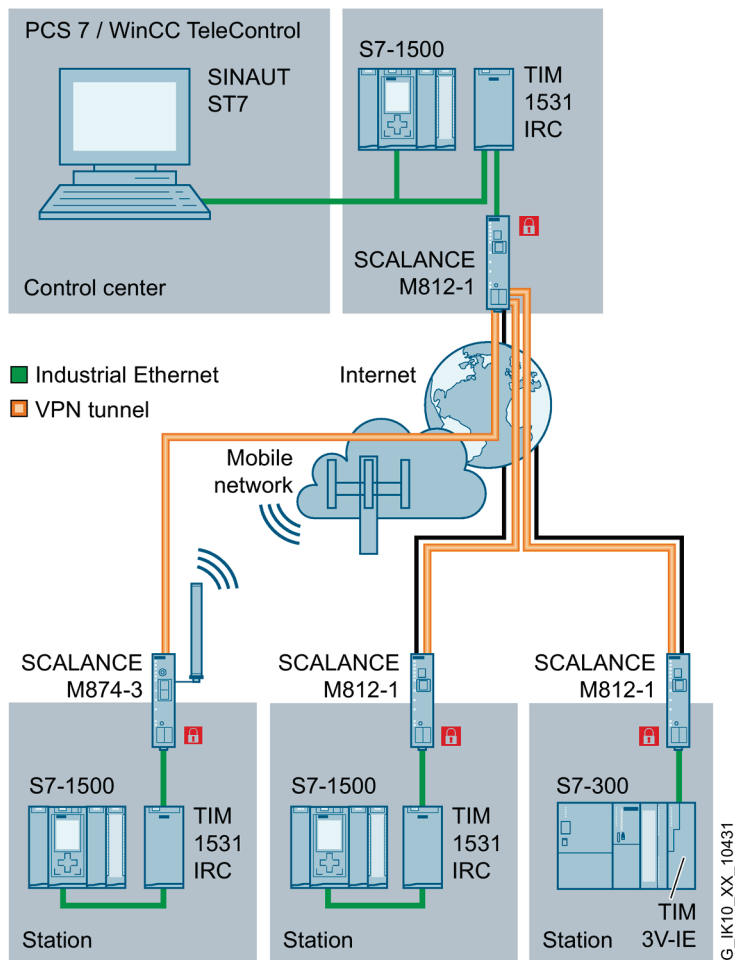
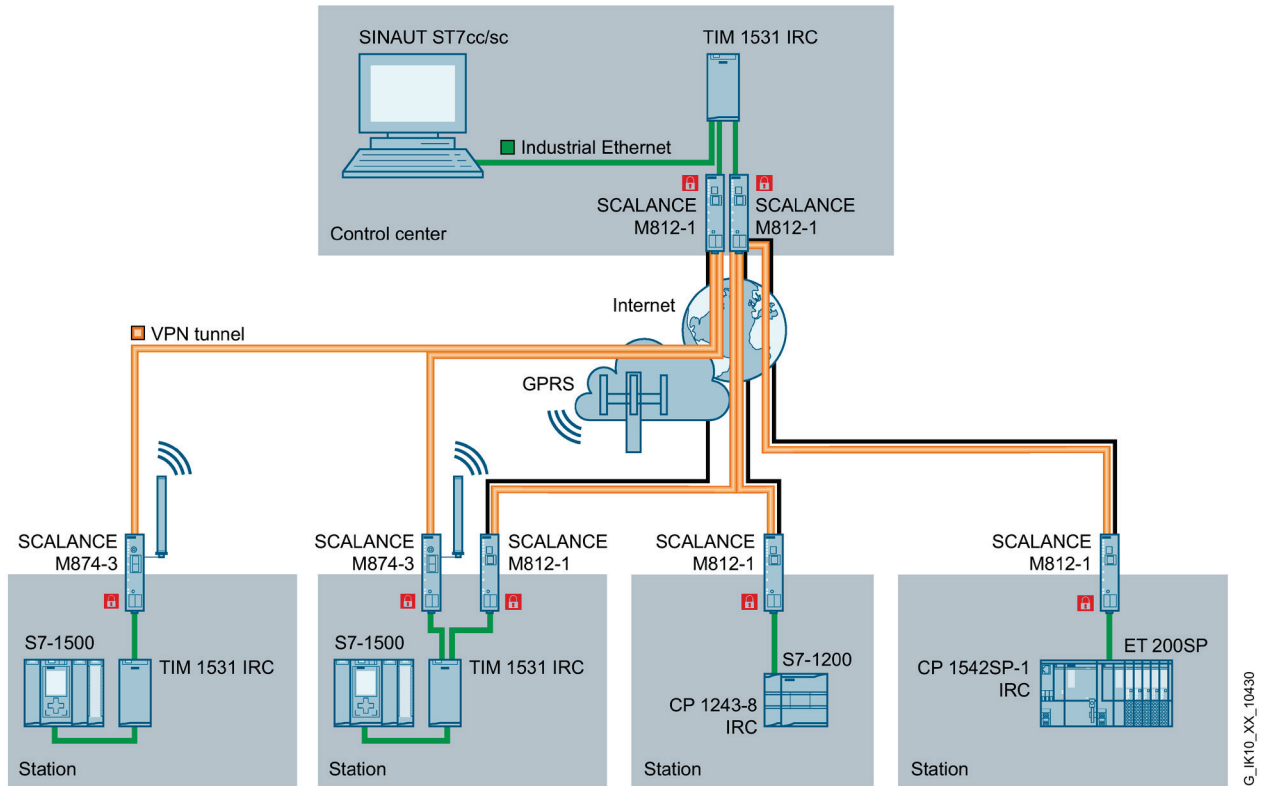


Figure 8-13 Example of a topology: TIM 1531 IRC stand-alone use with master or node functionality

Redundant transmission paths

With the TIM 1531 IRC a station can be connected to a control center through redundant paths. To this purpose, the TIM 1531 IRC is used both in the station and in the master station. The example shows a combination of DSL network and radio as redundant paths. The data transfer takes place as normal via the main path and in case of a failure via the substitute path. When the main path returns, the system automatically switches back to this path.



G_IK10_XX_10430

Figure 8-14 Example of a topology: Connection of telecontrol stations on the basis of S7-1500 with TIM 1531 IRC to a TeleControl control center

Features

The TIM 1531 IRC offer the features listed in the table:

	TIM 1531 IRC
RS 232 connections for external data transfer	1x D-sub 9-pin
Connections for Industrial Ethernet	3x RJ45 (switched)
Transmission rate	1x 1000 Mbps 2x 10/100 Mbps
External power supply	24 V DC via 2-pin plug-in terminal strip
Number of TIMs per S7-1500	1
Number of TeleControl connections	128
C-PLUG	-
SIMATIC Memory Card (SMC)	Optional

- Suitable / available or according to the specified standard

Functions

The communication module TIM 1531 IRC supports the following protocols and technologies:

Protocol / function	TIM 1531 IRC
TCP/IP	•
DNP3	•
IEC 60870-5-101/104	•
SINAUT ST1	-
SINAUT ST7	•
Modbus RTU	-
IPv6	•
Redundancy manager	-
Firewall	-
VPN with IPsec	-
SNMPv1	•
SNMPv3	•
DCP	•
LLDP	•
NTP	•

- Suitable / available or according to the specified standard.

Article numbers

Device	Description	Article number
TIM 1531 IRC	Communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with 1x 100/1000 Mbps and 2x 10/100 Mbps RJ45 ports and 1x RS 232/ RS 485 port	6GK7543-1MX00-0XE0

8.8 Communication processors for SIMATIC ET 200SP

Description



Figure 8-15 CP 1542SP-1 with plugged in BusAdapter

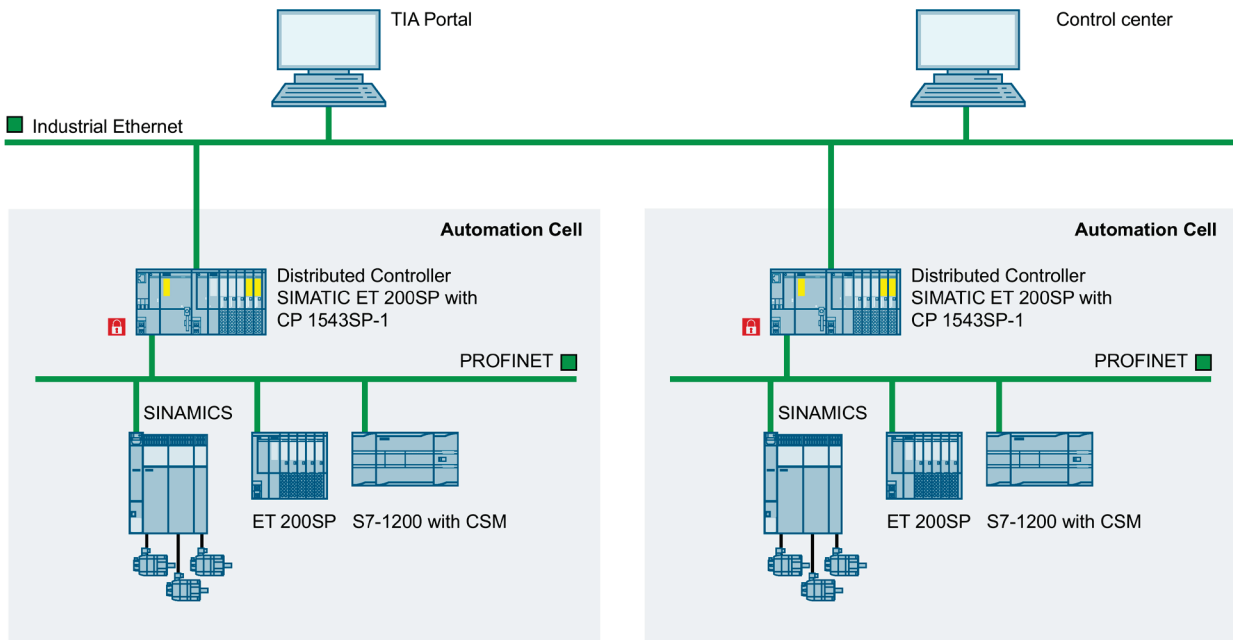
The communication modules for the SIMATIC ET 200SP connect the SIMATIC ET 200SP Distributed Controller with Industrial Ethernet networks. The module can also be used for the integration of the ET 200SP Distributed Controller into an IPv6-based network. The CP 1543SP-1 communication processor also offers the integrated security functions firewall (Stateful Packet Inspection), VPN (IPsec) and protocols for data encryption (for example, SNMPv3) and this way protects individual ET 200SP Distributed Controllers and complete automation cells against unauthorized access.

The CP 1542SP-1 IRC supports the TeleControl communication. By using the CP 1542SP-1 IRC, the ET 200SP Distributed Controller can be used as a remote terminal unit (substation) in TeleControl systems. The Ethernet-based connection to the control center takes place via the protocols SINAUT ST7, TeleControl Server Basic, IEC 60870-5-104 or DNP3. The CP 1542SP-1 IRC has the function of a data buffering. This allows up to 100000 events to be buffered in case of a connection termination.

All functions can be configured with STEP 7 Professional as of V14 (TIA Portal).

Examples of a topology

The figure shows an application example for connection to a higher-level network and the network separation of automation cells:



G_1K10_XX_50716

Figure 8-16 Example of a topology: Network separation and access protection with CP 1543SP-1

The figure shows an application example for the connection of TeleControl stations on the basis of S7-1500 to a TeleControl control center.

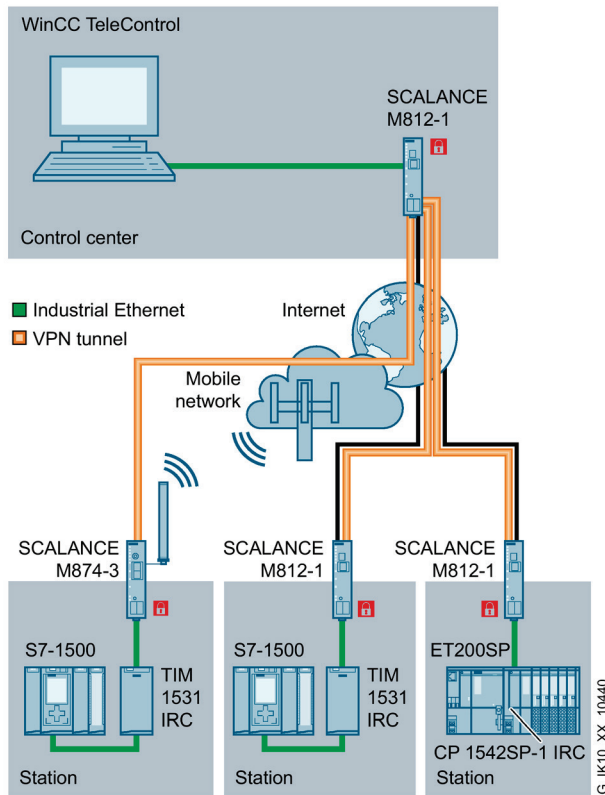


Figure 8-17 Example of a topology: Using the CP 1543SP-1IRC in TeleControl applications

Features

	CP 1542SP-1	CP 1542SP-1 IRC	CP 1543SP-1
External power supply 24 V DC	•	•	•
Connections Industrial Ethernet	1x RJ45	1x RJ45	1x RJ45
Integrated switch	•	•	•
Gigabit interface	-	-	-
Number of active connections for multiprotocol mode	32	32	32

- Suitable / available or according to the specified standard.

Functions

The communication processors of this category support the following protocols and technologies:

Protocol / function	CP 1542SP-1	CP 1542SP-1 IRC	CP 1543SP-1
TCP/UDP	•	•	•
IT	•	•	•
FTP	-	-	•
PG/OP	•	•	•
S7	•	•	•
DNP3	-	•	-
IEC 60870-5-104	-	•	-
SINAUT ST7	-	•	-
TeleControl Server Basic (TCSB)	-	•	-
IPv6	•	•	•
Firewall	-	-	•
VPN with IPsec	-	-	•
SNMPv1	•	•	•
SNMPv3	-	-	•
DCP	•	•	•
LLDP	•	•	•
NTP	•	•	•

- Suitable / available or according to the specified standard.

Article numbers

Device	Description	Article number
CP 1542SP-1	Communication processor for connecting a SIMATIC S7-ET 200SP to Industrial Ethernet 1x 10/100 Mbps RJ45 ports; TCP/IP, ISO-on-TCP, UDP, bus adapter required (does not ship with the product)	6GK7542-6UX00-0XE0
CP 1542SP-1 IRC	Communication processor for connecting a SIMATIC S7-ET 200SP to Industrial Ethernet, SINAUT ST7, TeleControl Server Basic, IEC-60870-5-104 or DNP3 protocol to a control center; TCP/IP, ISO-on-TCP, bus adapter required (does not ship with the product)	6GK7542-6VX00-0XE0
CP 1543SP-1	Communication processor for connecting a SIMATIC S7-ET 200SP to Industrial Ethernet, security function firewall and VPN; TCP/IP, ISO-on-TCP, UDP, bus adapter required (does not ship with the product)	6GK7543-6WX00-0XE0

Compact switch module

Overview

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.

Device versions

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 corresponds to the industrial, technical requirements of the new SIMATIC generation S7-1200. It is intended for installation on a 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 is in conformity with the standards EN 60721-3-3 of the class 3B2, EN 60721-3-3 of the class 3C4 incl. salt spray as well as the ISA –S71.04, the immunity test levels G1, G2, G3 and GX.
- LOGO! CSM is designed with four RJ45 ports for external access or connection to Industrial Ethernet networks. With the LOGO! CMS an Ethernet interface of the SIMATIC LOGO! system modules 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 V and 24 V
- LOGO! CSM 230 for the operation with an AC voltage of 110 V and 230 V

Example of a topology

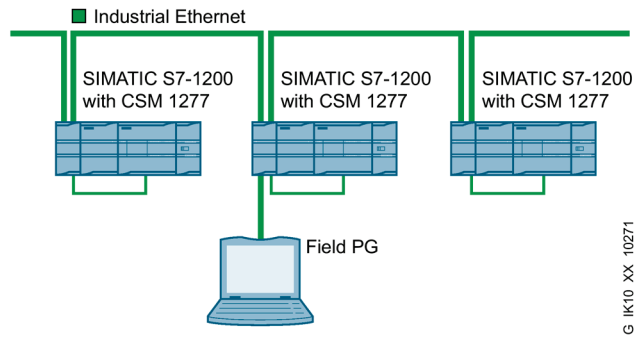


Figure 9-1 Linear bus structure with CSM 377

9.1 CSM 377

Description



Figure 9-2 CSM 377 unmanaged

The Compact Switch Module CSM 377 is an unmanaged switch for connecting a SIMATIC S7-300 module with an integrated PROFINET interface or with an Industrial Ethernet CP or ET 200M to an Industrial Ethernet network. The CSM 377 is suitable for the design of line, tree and star structures. The CSM 377 is intended for integration of small machines into existing automation networks or for standalone operation of the machines. It offers a cost-effective solution for the implementation of small, local Ethernet networks.

The module has a rugged plastic housing with IP20 degree of protection and is intended for installation on a SIMATIC S7-300 standard 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 takes place either via an Industrial Ethernet cable or an Industrial Ethernet twisted pair cord.

Features

	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 device has the following functions:

- Display LEDs for diagnostics and for the status of the respective Industrial Ethernet ports
- 10/100 BaseTX
- Autosensing and autocrossover functions for automatic data detection
- Three further Industrial Ethernet interfaces (TP ports) are available for connecting additional Ethernet nodes such as HMI panels or ET 200.
- The module can be exchanged without a programming device
- Fanless operation, a backup battery is unnecessary

Article numbers

Device	Description	Article number
CSM 377	Unmanaged switch for connecting a SIMATIC S7-300, ET 200M and up to three further nodes to Industrial Ethernet; 4x 10/100 Mbps RJ45 ports	6GK7377-1AA00-0AA0

9.2 CSM 1277

Description



Figure 9-3 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 in line, tree or star structure. Simple automation networks can be implemented at low cost with the CSM12 connection of the SIMATIC S7-1200 77 and control of SIMATIC S7-1200 systems. Through the use of CSM 1277, the Ethernet interfaces on a SIMATIC S7-1200 module are 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. The use of straight-through connecting cables is possible thanks to integrated autocrossover function.

The module has a rugged plastic housing with IP20 degree of protection and is intended for installation on a SIMATIC S7-1200 standard rail.

Features

	CSM 1277
External power supply 24 VDC	•
Connection for Industrial Ethernet/PROFINET	4x RJ45
Gigabit interface	-

- Suitable / available or according to the specified standard.

Functions

The individual devices have the following functions:

CSM 1277 unmanaged

- Display LEDs for diagnostics and for the status of the respective Industrial Ethernet ports
- Autosensing and autocrossover functions for automatic data detection
- Replication of the Ethernet interfaces of the SIMATIC S7-1200 systems
- The module can be exchanged without a programming device
- 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 RJ45 connection of the SIMATIC S7-1200 remains free, for example, for connecting a programming device.
- Connection of the SIMATIC S7-1200 to a higher-level network with a tree or star structure
At least two RJ45 connections of the SIMATIC S7-1200 remain free, for example, 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.

Detailed information and the technical documentation on SIPLUS is available in the portal of Siemens AG under SIPLUS (<https://w3.siemens.com/mcms/siplus/en/siplus-extreme/Pages/Default.aspx>).

Article numbers

Device	Description	Article number
CSM 1277	Unmanaged switch for connecting a SIMATIC S7-1200 and up to three further nodes to Industrial Ethernet, 4x 10/100 Mbps RJ45 ports	6GK7277-1AA10-0AA0
SIPLUS NET CSM 1277	Unmanaged switch for connecting a SIPLUS S7-1200 and up to three further nodes to Industrial Ethernet, 4x 10/100 Mbps RJ45 ports Ambient temperature from 0 °C to +55 °C (for exceptional environmental load)	6AG1277-1AA00-4AA0

9.3 LOGO! CSM

Description



Figure 9-4 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

	CSM 12/24	CSM 230
Power supply	12/24 VDC (10.2 ... 30.2 VDC)	230 VAC
Connector - Industrial Ethernet	4x RJ45	
Transmission rate	10/100 Mbps	
Design	LOGO! module	
Degree of protection	IP20	

- Suitable / available or according to the specified standard.

Functions

The individual devices have the following functions:

- Diagnostics LEDs
- 1x Ethernet port on the front of the module for direct diagnostic access in the cabinet
- 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 usage for networking different Ethernet devices

Article numbers

Device	Description	Article number
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

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.

Examples of a topology

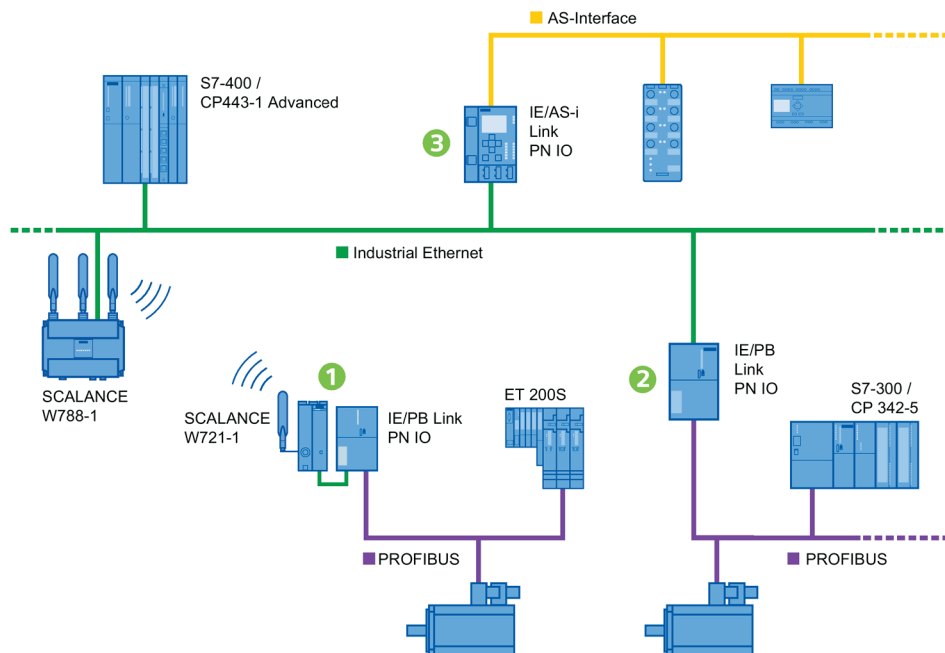


Figure 10-1 ① Connection between IWLAN and PROFIBUS via the IE/PB Link PN IO in connection with a SCALANCE W721-1
 ② Connection between Industrial Ethernet and PROFIBUS via the IE/PB Link PN IO
 ③ Connection between Industrial Ethernet and AS-interface via the IE/AS-i Link PN IO

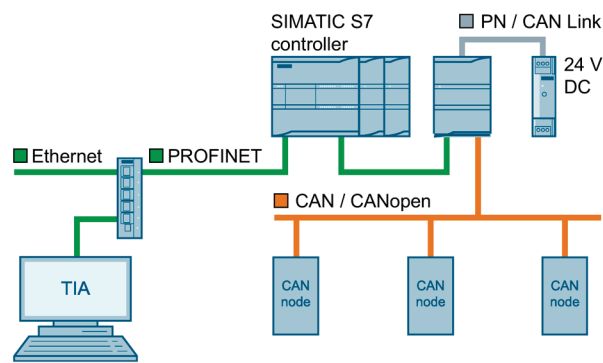


Figure 10-2 PN/CAN Link Gateway

Device versions

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. The device allows transparent data access to the AS interface of an Industrial Ethernet.

PN/BACnet link

The PN/BACnet Link is a gateway between a PROFINET network and a BACnet building automation bus. The device enables communication and data exchange with up to 1000 BACnet objects.

PN/CAN link

The PN/CAN Link is a gateway for PROFINET data exchange between PROFINET and the CAN 2.0A/B fieldbus or CANopen Manager or Slave (according to CiA 301 & 302). The device enables communication and data exchange with up to 126 CAN nodes.

10.1 IE/PB Link PN IO

Description



Figure 10-3 IE/PB LINK PN IO

- Rugged plastic housing in SIMATIC ET 200SP design, IP20 degree of protection
- Installation on the DIN rail
- Optional use of the C-PLUG memory medium (does not ship with the product) for storage of device parameters to allow quick device exchange
- SIMATIC ET200 SP modular design: Optional connection possibility for Industrial Ethernet via bus adapter (does not ship with the product) of the SIMATIC ET 200SP system for free selection of the connection physics and technology on the side of the PROFINET.

Features

	IE/PB Link PN IO SIPLUS NET IE/PB LINK PN IO
Connector - Industrial Ethernet	1x RJ45
Connector PROFIBUS	1x D-sub 9-pin, female (RS485)
Transmission rate - Industrial Ethernet	10/100 Mbps
Power supply	24 VDC
Integrated 2-port real-time switch	•
Diagnostic LEDs	•
C-PLUG slot	•

- Suitable / available or according to the specified standard.

Functions

- Ethernet transmission rate 10/100 Mbps full/half duplex with autosensing for the automatic switchover
- 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
- Support of the Media Redundancy Protocol (MRP)
- LLDP
- SNMP v1
- DCP
- NTP

Article numbers

Device	Description	Article number
IE/ PB Link PN IO	Gateway between Industrial Ethernet and PROFIBUS with PROFINET IO functionality, S7 routing and data record routing, 10/100 Mbps Fast Ethernet, MRP, 9.6 kbps to 12 Mbps PROFIBUS, NTP	6GK1411-5AB10
SIPLUS NET IE/PB LINK PN IO	Gateway between Industrial Ethernet and PROFIBUS with PROFINET IO functionality, with coated PCBs, S7 routing and data record routing, 10/100 Mbps Fast Ethernet, MRP, 9.6 kbps to 12 Mbps PROFIBUS, NTP -40 °C to +70 °C start up -25 °C with conformal coating	6AG1411-5AB10-2AA0

10.2 IE/AS-i Link PN IO

Description



Figure 10-4 IE/AS-i LINK PN IO

- Single or double AS-Interface master for connection of 62 or 124 AS-Interface slaves (for dual master)
- Compact plastic housing with IP20 degree of protection 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 to allow quick device exchange

Features

	IE/AS-i Link PN IO
Connector - Industrial Ethernet	2x RJ45 (switched)
Connector - AS-i	Screw connector
Transmission rate - Industrial Ethernet	10/100 Mbps
Power supply	24 VDC or via AS-i
Integrated 2-port real-time switch	•
Diagnostic LEDs	•
C-PLUG slot	•

- Suitable / available or according to the specified standard.

Functions

- AS-Interface bus cycle time 5 ms for 31 slaves, 10 ms for 62 slaves
- Use as single and double AS-interface master for the connection of 62 AS-interface slaves and integrated analog value monitoring
- Integrated Web server through 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

Device	Description	Article number
IE/ AS- i Link PN IO	Gateway between PROFINET/Industrial Ethernet and AS-Interface incl. plug-in screw connections COMBICON for connection of an AS-Interface cable, with a double master two AS-interface cables and an optional power supply of 24 V. According to the AS-interface specification 3.0.	
	Single master with display	6GK1411-2AB10
	Double master with display	6GK1411-2AB20

10.3 PN/BACnet Link Gateway

Description



Figure 10-5 SIMATIC PN/BACnet Link gateway

Gateway between PROFINET and BACnet/IP networks according to EN ISO16484-5 and addendum ANSI/ASHRAE Standard 135-2012

- Compact plastic housing in S7-1200 design, IP20 degree of protection
- Mounting on a DIN rail or a panel
- LEDs for visualization of operating states for BACnet, PROFINET and Ethernet ports
- Diagnostics alarms

- Configuration via STEP 7 TIA Portal as of V14 SP1 or higher
- Supported controllers: S7-1200, S7-1500, ET 200SP, OpenController

Features

	SIMATIC PN/BACnet link
Connection PROFINET/Industrial Ethernet	2x RJ45
Connection BACnet/IP	1x RJ45
Transmission rate - Industrial Ethernet	Max. 100 Mbps
Power supply	24 V DC
Integrated 2-port real-time switch	•
Diagnostic LEDs	•
C-PLUG slot	•

- Suitable / available or according to the specified standard.

Functions

- PROFINET IO
- Operation as "BACnet Client" or "BACnet Server"
The functionality is specified during configuration, mixed operation of client and server functionality possible.
- Data transmission:
 - Acyclic (programmed from the automation program); via the "Data record read/write" services
 - Cyclic (can be parameterized in HSP by the user); via updating of the IO image
 - At change of value via Change of Value (COV) mechanism
- Scan of the BACnet/IP network
- Supported BACnet object types:
 - Device
 - Binary input / binary output
 - Analog input / analog output
- Supported BACnet services:
 - DS-COV-A/B
 - DM-DDB-A/B
 - DM-DOB-B
 - DS-RP-A/BDS-WP-A/P
 - GW-EO-B

Article numbers

Device	Description	Article number
SIMATIC PN/BACnet link	SIMATIC PN/BACnet LINK gateway from PROFINET to BACnet/IP networks, device profile: B-GW, IP20	6BK1621-0AA00-0AA0

10.4 PN/CAN link

Description



Figure 10-6 PN/CAN link

Gateway between PROFINET and CANopen Manager or Slave (according to CiA 301 & 302)

- Compact plastic housing in S7-1200 design, IP20 degree of protection
- Mounting on a DIN rail or a panel
- LEDs for visualization of operating states for BACnet, PROFINET and Ethernet ports
- Diagnostics alarms
- Configuration via STEP 7 TIA Portal as of V14 SP1 or higher
- Maximum permissible cable length of the CAN network of up to 1000 m (depending on data transmission rate, cable cross-section, number of nodes)
- Supported controllers: S7-1200, S7-1500, ET 200SP, OpenController

Features

	SIMATIC PN/CAN Link
Connection PROFINET/Industrial Ethernet	2x RJ45
CAN bus connection	1x D-sub connector (9-pin, socket)
Transmission rate - Industrial Ethernet	100 Mbps
Power supply	24 V DC

	SIMATIC PN/CAN Link
Integrated 2-port real-time switch	•
Diagnostic LEDs	•
C-PLUG slot	•

- Suitable / available or according to the specified standard.

Functions

- PROFINET IO
- Per 512 receive /transmit PDOs
- Baud rates from 50 kBaud up to 1000 kBaud on the CAN side
- Operating modes:
 - CANtransparent
 - CANopen Manager
 - CANopen slave
- Data transmission:
 - For value change / acyclic
Acyclic communication via the "Data record read/write" services
 - Cyclic
Cyclic data exchange between the PN/CAN LINK and the connected SIMATIC S7 CPUs via updating of the IO image
 - On request from the application (RTR)
- Supported CAN services:
 - Nodeguarding/Lifeguarding
 - Heartbeat
 - SYNC (producer / consumer)

Article numbers

Device	Description	Article number
SIMATIC PN/CAN Link	SIMATIC PN/CAN LINK gateway from PROFINET to CAN or CANopen networks CAN 2.0A/B CANopen Manager to CiA301/302 CANopen slave to CiA301/302, IP20	6BK1620-0AA00-0AA0

Appendix

A.1 Overview of the standards relevant for network installation

Introduction

The section provides you with a general overview of the standards that you need to consider during the installation of networks in buildings in general and of Industrial Ethernet in particular.

Note

This section can only contain general information that is valid at the time of printing.

For detailed guidelines that are always up-to-date please refer to the PROFIBUS User Organization e.V.

The PROFIBUS Users Organization

PROFIBUS Users Organization e.V.

Haid-und-Neu-Str. 7

D-76131 Karlsruhe, Germany

Phone +49 (0) 7 21 / 96 58 590, Fax +49 (0) 7 21 / 96 58 589

germany@profibus.com, www.profibus.com

Standards for application-neutral communication cable networks in the office environment

Standard	Area of application
ISO/IEC 11801	International standards for network planning, in office buildings
EN 50173	European standard for network planning in office buildings; applied as a national standard

Through the use of Ethernet, also in the automation technology, the existing standards needed to be extended by the industrial area.

Standards for application-neutral communication cable networks in the industrial environment

Standard	Area of application
ISO/IEC 24702	International standards for the planning of application-neutral networks in industrial buildings
EN 50173-2 EN 50173-3	European standard for network planning in industrial buildings; applied as national standard

For the industry application itself further standards are required that describe the constraints for this application.

Cabling standards for industrial networks and their sphere

Standard	Area of application	Sphere
IEC 61918	International standards for communication networks in industrial automation systems; suitable for field buses, general aspects on planning, installation, operation ¹⁾	Describes network structure and general requirements in and between automation cells
IEC61784-5-x	International series of standards for special requirement of the industrial networks, such as PROFINET / PROFIBUS, in addition to IEC 61918.	Describes specific requirements of the communication profile

¹⁾ Fieldbus-specific aspects are described in separate, subordinate standards

The guideline "PROFINET Cabling and Interconnection Technology Guideline"

The PROFIBUS User Organization, among other things, has compiled the guideline "PROFINET Cabling and Interconnection Technology" that serves as input for the IEC 61918 and the IEC 61784, among other things, and also refers to it.

The technical benchmarks for cables and the connection technology (electrical and optical) for PROFINET networks are described. These are intended to help new manufacturers with making products that are PROFINET compliant.

The guideline can be downloaded in English under:

Link (<https://www.profibus.com/download/profinet-cabling-and-interconnection-technology/>)

A.2 Content of the standards

Content of the standards IEC 24702 and EN50173-3

The standards for the application-neutral building networking of industrially used buildings describe:

- Structure of the building network
- Performance requirements for cables (fiber-optic cable, electrical),
- Performance requirement for plug-in connector (fiber-optic cable, electrical),
- Limit values for permanent links.

The IEC 24702 references the IEC 11801.

Installation-specific aspects are described in the IEC 14763 (EN50174).

Content of the standards IEC 61918 and IEC61784

The standards for the automation networks contain a general part which describes the following points:

- Network design (network structure, grounding, bonding),
- Planning and installation,
- Component requirements (plug-in connectors, cables, grounding, etc.)
- Installation inspection,
- Maintenance and repair

The *IEC 61918* contains general requirements that are common for all fieldbuses (PROFINET, PB, Interbus, etc.).

Fieldbus-specific aspects/requirements that deviate from the general part are also described in the 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	
EN501714-1	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

Index

5

50174
Standard, 364

8

802.11
WLAN standards, 54

A

Access point, 60, 60, 128
Active network components
in PROFINET, 37
Ad hoc
Wireless network, 66
Ad hoc networks, 66
Address of the gateway, 29
Advanced Encryption Standard, 58
AES, 58
AMQP, 26
Antennas
Antenna gain, 234
Directional, 234
Dual antennas, 234
MIMO antennas, 234
Omnidirectional, 234
Product overview, 236
Radiation characteristics, 233
RCoax, 241
RCOAX cable, 234
Article number, 167, 188, 193
Autocrossover function, 129
Automated guided vehicle system, 65
Autonegotiation, 129

B

Backbone, 75
Bus adapter
SCALANCE XF-200 IRT, 171

C

Cable length, 130
Carousels, 53
Cell protection concept, 102
Client, 60, 128
Cloud Gateway, 287
CloudConnect 7
SIMATIC CC712/CC716, 287
CLP, 285
Collision detection, 59
Collision domain, 50
Communication processor
CP 1623, 303
CP 1628, 306
For SIMATIC ET 200SP, 339
For SIMATIC S7-1200, 327
For SIMATIC S7-1500, 330
For SIMATIC S7-1500 TIM 1531 IRC, 335
For SIMATIC S7-300, 311
For SIMATIC S7-300 SINAUT ST7, 317
For SIMATIC S7-400, 319
Communications processor
CP 1604, 300
CP 1616, 302
CP 1626, 304
Compact switch module
LOGO!CSM 12/24, 348
LOGO!CSM 230, 348
Compact Switch module
CSM 1277 unmanaged, 346
CSM 377 unmanaged, 344
Connection diagnostics, 324
CP 1604
Description, 300
Features, 301
Functions, 301
CP 1616
Description, 302
Features, 302
Functions, 302
CP 1623
Description, 303
Features, 303
Functions, 303
CP 1626
Description, 304

- Features, 305
- Functions, 305
- CP 1628
 - Description, 306
 - Features, 306
 - Functions, 306
- C-PLUG, 282
- Cranes, 53
- CSM 1277, 346
- CSM 377, 344
- CSMA/CA, 59
- CSMA/CD, 59
- Cut through, 45

D

- DCP protocol, 276
- Denial of Service, 101
- Diagnostics buffer extract, 324
- DLC protocol, 276
- DoS, 101
- DSSS, 54
- Dynamic routing, 46
 - VRRP, 46

E

- EAP, 58
- E-mail, 100
- EN 50173
 - Standard, 361, 364
- ERTEC-ASIC, 45
- EtherNet/IP, 49
- Extensible Authentication Protocol, 58

F

- Fast Ethernet, 17
- Fault mask, 129
- Fault-tolerant system, 324
- Firewall, 100
- Formation of loops, 130
- FTP, 100
- Functions
 - SCALANCE W1750D, 232
 - SCALANCE W1788/W1748, 229
 - SCALANCE X-200IRT/X-200IRT PRO, 153
 - SCALANCE X-200RNA, 155
 - SCALANCE X-300/XR-300, 180
 - SCALANCE XB-200, 159
 - SCALANCE XC-200, 162

- SCALANCE XF-200/XF-200IRT, 169
- SCALANCE XF-200BA, 174
- SCALANCE XM-400, 190
- SCALANCE XP-200, 176
- SCALANCE XR-300WG, 186
- SCALANCE XR-500, 198
- SIMATIC RTU3000C, 295

G

- Gateways
 - IE/ AS-i Link PN IO, 355
 - IE/PB Link PN IO, 353
 - PN/BACnet Link Gateway, 356
- Gigabit Ethernet, 17
- Glossary, 4
- GPRS router, 128
- GSM, 128
- GSM/GPRS modem
 - Modem MD720, 255

H

- H system, 324, 324
- High-Availability, 44
- High-bay storage rack, 53

I

- IE/ AS-i Link PN IO, 355
- IE/PB Link PN IO, 353
- IEC 61784
 - Standard, 364
- IEC 61918
 - Standard, 362
- IEC 62439-3, 89
- IEEE 1588, 25
- IEEE 802.11ac, 55, 208, 209
 - Frame aggregation, 57, 212
 - Guard interval, 56, 211
 - Maximum ratio combining, 57, 212
 - MIMO, 55, 210
 - Spatial multiplexing, 56, 211
- IEEE 802.11n, 55, 207, 209
 - Frame aggregation, 57, 212
 - Guard interval, 56, 211
 - Maximum ratio combining, 57, 212
 - MIMO, 55, 210
 - Spatial multiplexing, 56, 211
- IEEE 802.1Q, 26
- Industrial Ethernet, 15

Infrastructure mode, 61
 Wireless networks, 61
 IP access protection (IP-ACL), 324
 IP address, 28
 iPCF, 16
 iPCF-MC, 16
 IPv6
 Notation, 30
 IRT, 136
 ISO/IEC 11801
 Standard, 361
 ISO/IEC 24702
 Standard, 362
 Isochronous Real Time, 24, 136
 IWLAN, 52

K

KEY-PLUG, 283

L

Layer 3 function
 Dynamic routing, 46
 Static routing, 46
 Line
 Network topology, 75
 LOGO! CSM 12/24, 348
 LOGO! CSM 230, 348

M

MAC address, 323
 Main entry, 346
 Management functions, 135
 MDI/MDIX autocrossover function, 129
 Media modules
 SCALANCE X-300/XR-300, 183
 SCALANCE XR-500, 201
 MIMO, 54
 Mobile wireless, 128
 Modem MD720
 Description, 255
 Features, 256
 Functions, 257
 Module access protection, 323
 Monorail suspension track, 53
 MRP Interconnection
 Operating principle, 87
 Topology, 87

N

NAPT, 101
 NAT, 101
 Network Address Port Translation, 101
 Network Address Translation, 101
 Network management software
 Primary Setup Tool (PST), 274
 SINEC NMS, 277
 SINEMA RC, 271
 SOFTNET TSN, 280
 Network topology, 75
 Line, 75
 Star, 76
 NTP mode (NTP: Network Time Protocol),

O

OFDM, 54
 OPC UA (PubSub), 26

P

Packet filter, 100
 Parallel Redundancy Protocol, 89
 Passive network components
 in PROFINET, 37
 Personal firewall, 101
 PING function, 324
 Plug and play, 129
 Pluggable transceiver
 SFP, 157, 165, 167, 187, 192, 192
 SFP+, 202
 Pluggable transceiver SFP (100 Mbps)
 Interfaces, 157, 166, 193
 Pluggable transceiver SFP (1000 Mbps)
 Interfaces, 167, 188, 194
 Pluggable transceiver SFP (1000 Mbps) bidirectional
 Interfaces, 167, 188, 194
 Pluggable transceiver SFP+ (10 Gbps)
 Interfaces, 202
 PN/BACnet Link Gateway, 356
 Point-to-point, 92
 Port, 100
 Power over Ethernet
 IEEE 802.3af, 41
 IEEE 802.3at, 41
 Primary Setup Tool (PST), 274
 PROFIBUS International, 20
 PROFIBUS Users Organization, 361
 PROFINET, 15
 Cable installation, 39

- Fault-tolerant systems, 44
- Implementation, 19
- Isochronous Real Time, 24
- Redundancy, 44
- Switching mechanisms, 45
- PROFINET Cabling and Interconnection Technology
 - Guidelines, 362
- PROFINET IO, 19, 20
- PRP, 89
- Pseudo random numbers, 58
- PTP
 - TSN, 25

R

- RADIUS
 - Network authentication protocol, 58
- Range of values for IP address, 28
- RCoax cable, 60
- Redundancy manager, 51, 80
- Redundancy methods
 - HRP, 89
 - MRPD, 88
 - MSTP, 93
 - RSTP, 92
 - STP, 92
- Redundant Network Access, 91
- Redundant ring, 51
- Redundant systems, 44
- Remote maintenance, 110
- Repeater, 50
- Ring
 - Network topology, 79
- RNA, 91
- Roaming, 60
- RSTP+
 - Properties, 93
 - Topology, 94
- RTS/CTS, 59

S

- S5/S7 addressing mode, 324
- SCALANCE M, 241
 - M804PB, 250
 - M812-1/ M816-1/ M826-2, 244
 - M874/ M876, 247
- SCALANCE M804PB
 - Description, 250
 - Features, 251
 - Functions, 251
- SCALANCE M812-1
 - Description, 244
 - Features, 245
 - Functions, 246
- SCALANCE M816-1
 - Description, 244
 - Features, 245
 - Functions, 246
- SCALANCE M826-2
 - Description, 244
 - Features, 245
 - Functions, 246
- SCALANCE M874-x
 - Description, 247
 - Features, 249
 - Functions, 249
- SCALANCE M876-x
 - Description, 247
 - Features, 249
 - Functions, 249
- SCALANCE S, 261
 - Configuration and administration, 262
 - How it works, 262
- SCALANCE S15
 - Features, 266
 - Functions, 267
- SCALANCE S615
 - Description, 265
 - Interface, 267
- SCALANCE SC6-00
 - Interface, 267
- SCALANCE SC-600
 - Description, 265, 265
 - Features, 266
 - Functions, 267
- SCALANCE TAP
 - Characteristics, 140
 - Description, 139
 - Interfaces, 140
- SCALANCE W
 - Access points, 204
 - Antennas, 233, 236
 - Client modules, 204
 - Direct Access Point, 204
 - Performance classes, 205
 - W1750D, 231
 - W1788/W1748, 227
 - W786, 221
 - W788/W748, 224
- SCALANCE W1750D
 - Description, 231
 - Features, 231

- Functions, 232
- Interfaces, 233
- SCALANCE W1788/W1748
 - Description, 227
 - Features, 228
 - Functions, 229
 - Interfaces, 229
- SCALANCE W760/W720
 - Description, 212
 - Features, 213
 - Functions, 213
 - Interfaces, 214
- SCALANCE W774/W734
 - Description, 215
 - Features, 216
 - Functions, 216
 - Interfaces, 217
- SCALANCE W778/W738
 - Description, 218
 - Features, 219
 - Functions, 219
 - Interfaces, 220
- SCALANCE W786
 - Description, 221
 - Features, 221
 - Functions, 222
- SCALANCE W788/W748
 - Features, 225
 - Functions, 225
 - Interfaces, 226
- SCALANCE X
 - Performance classes, 133
 - Pluggable transceiver SFP (100 Mbps), 157, 166, 193
 - Pluggable transceiver SFP (1000 Mbps), 167, 188, 194
 - Pluggable transceiver SFP (1000 Mbps) bidirectional, 167, 188, 194
 - Pluggable transceiver SFP+ (10 Gbps), 202
 - TAP, 139
 - X-000, 140
 - X-100, 144
 - X-200IRT/X-200IRT PRO, 151
 - X-200RNA, 154
 - X-300/XR-300, 178
 - X500, 197
 - XB-000, 142
 - XB-100, 146
 - XB-200, 158
 - XC-100, 148
 - XC-200, 161
 - XF-200/XF-200IRT, 168
 - XF-200BA, 172
 - XM-400, 189
 - XP-200, 175
 - XR-100WG, 150
 - XR-300WG, 185
 - XR-500, 197
- SCALANCE X-000
 - Description, 140
 - Features, 141
 - Interfaces, 141
- SCALANCE X-100
 - Characteristics, 145
 - Description, 144
 - Interfaces, 145
- SCALANCE X-200IRT/X-200IRT PRO
 - Description, 151
 - Features, 152
 - Functions, 153
 - Interfaces, 153
- SCALANCE X-200RNA
 - Description, 154
 - Features, 155
 - Functions, 155
 - Interfaces, 156
- SCALANCE X-300
 - SFP transceiver, 184
- SCALANCE X-300/XR-300
 - Description, 178
 - Features, 180
 - Functions, 180
 - Interfaces, 181
 - Media modules, 183
- SCALANCE X500
 - Description, 197
 - External power supply unit, 202
- SCALANCE XB-000
 - Characteristics, 143
 - Description, 142
 - Interfaces, 143
- SCALANCE XB-100
 - Description, 146
 - Features, 147
 - Interfaces, 147
- SCALANCE XB-200
 - Description, 158
 - Features, 158
 - Functions, 159
 - Interfaces, 160
- SCALANCE XC-100
 - Description, 148
 - Features, 149
 - Interfaces, 149

- SCALANCE XC-200
 - Description, 161
 - Features, 162
 - Functions, 162
 - Interfaces, 163
- SCALANCE XF-200 IRT
 - Bus adapter, 171
- SCALANCE XF-200/XF-200IRT
 - Description, 168
 - Features, 169
 - Functions, 169
 - Interfaces, 170
- SCALANCE XF-200BA
 - Description, 172
 - Features, 173
 - Functions, 174
 - Interfaces, 174
- SCALANCE XM-400
 - Description, 189
 - Extender module interfaces, 195
 - Extender modules, 194
 - External power supply units PS-900 PoE, 195
 - Features, 189
 - Functions, 190
 - Interfaces, 191
- SCALANCE XP-200
 - Description, 175
 - Features, 176
 - Functions, 176
 - Interfaces, 177
- SCALANCE XR-100WG
 - Description, 150
 - Features, 150
 - Interfaces, 150
- SCALANCE XR-300WG
 - Description, 185
 - Features, 185
 - Functions, 186
 - Interfaces, 186
- SCALANCE XR-500
 - Description, 197
 - Features, 198
 - Functions, 198
 - Interfaces, 199
 - Media modules, 201
 - SFP transceiver, 201
- Security modules, 128
- SFP transceiver, 157, 165, 167, 187, 192, 192
 - SCALANCE X-300, 184
 - SCALANCE XR-500, 201
- Shared LAN, 50
- Shared medium, 60
- Signaling contact, 137
- Silent listener
 - Wireless network, 53
- SIMATIC CC712/CC716
 - Description, 287
 - Features, 289
 - Functions, 289
- SIMATIC ET 200SP
 - Communication processor CP 1500SP-1, 339
- SIMATIC mode, 323
- SIMATIC NET, 15
- SIMATIC NET glossary, 4
- SIMATIC RTU3000C, 291
 - Description, 293
 - Features, 294
 - Functions, 295
 - Interfaces, 295
- SIMATIC S7-1200
 - Communication processor CP 1200-1/ CP 1200-7, 327
- SIMATIC S7-1500
 - Communication processor 1500-1, 330
 - Communication processor TIM 1531 IRC, 335
- SIMATIC S7-300
 - Communication processor CP 300-1, 311
 - Communication processor SINAUT ST7, 317
- SIMATIC S7-400
 - Communication processor CP 400-1, 319
- SINEC NMS, 277
- SINEMA Remote Connect, 271
- Slip contacts, 53
- SNMP agent, 323
- SOFTNET TSN, 280
- Spanning Tree, 92
 - Multiple Spanning Tree, 93
 - Rapid Spanning Tree, 92
- SSH, 100
- Standalone network, 61
- Standards for application-neutral communication cable networks
 - Industrial environment, 362
 - Office environment, 361
- Standby redundancy, 81
- Star
 - Network topology, 76
- Star coupler, 50
- Stateful packet inspection, 101
- Static routing, 46
- Store and forward, 45
- Subnet mask, 28
- Switch, 50, 76, 128
- Switched LANs, 50

T

TeleService Adapter IE Basic, 252
TIA, 20
Time-of-day synchronization on the RNA interface, 323
Totally Integrated Automation, 20
Trailing cable, 53
TSN, 24
Tunneling, 102

U

UMTS, 128

V

Virtual Private Network, 102
VPN, 102

W

Web diagnostics, 324
WEP, 58
Wi-Fi Protected Access, 58
Wired Equivalent Privacy, 58
Wireless cell, 60, 60
Wireless networks
 Unstructured, 66
WLAN, 52
WPA, 58
WPA2, 58

