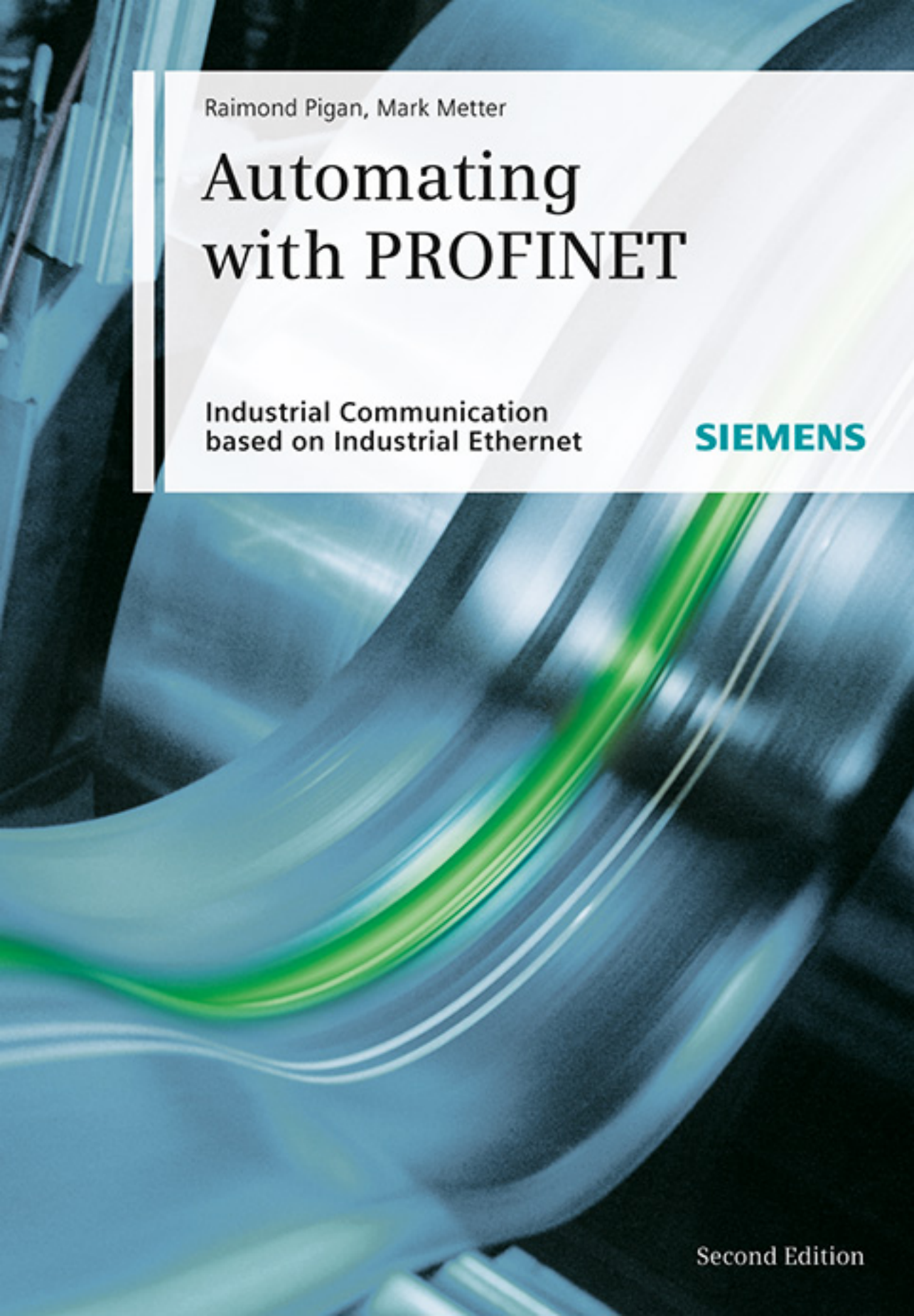
Raimond Pigan, Mark Metter

Automating with PROFINET

Industrial Communication based on Industrial Ethernet

SIEMENS



Second Edition

Automating with PROFINET

Industrial Communication
based on Industrial Ethernet

by Raimond Pigan
and Mark Metter

2nd revised and extended edition, 2008

Publicis Publishing

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

www.publicis.de/books

Print ISBN 978-3-89578-294-7
ePDF ISBN 978-3-89578-950-2

2nd edition, 2008

Editor: Siemens Aktiengesellschaft, Berlin and Munich
Translation: Siemens A&D Translation Services, Erlangen
Publisher: Publicis Publishing, Erlangen

Printed in Germany

Foreword

The success story of Industrial Ethernet began in 1985 when Siemens presented the SINEC H1 based on IEEE 802.3. Especially because of its ability to exchange large quantities of data, Industrial Ethernet was predestined for use in production control systems. Three years later, special fieldbus systems such as Profibus started to establish themselves for communication at the field level. These permitted fast and reliable exchange of data between controllers and distributed I/O devices.

However, the increase in the volume of data to be transmitted resulting from increasingly intelligent field devices means that current fieldbus systems have reached their performance limits. With the first presentation of Profinet by PROFIBUS International in August 2000, Industrial Ethernet started to overcome this limitation. Profinet is making the way free for continuous communication from the field level up to the corporate management level.

Profinet as an open Industrial Ethernet standard now satisfies all requirements for industrial applications. It is a standard which combines industrial performance and the strict real-time communication requirements necessary for motion control applications with the advantages of modern office communication.

Profinet IO permits automation solutions to be implemented which were previously exclusively reserved for fieldbus applications. Profinet CBA divides complex automation applications into autonomous technological modules of manageable size. In both cases, existing fieldbuses can be integrated into future structures using proxies.

Profinet is the first communications standard which permits both standard and safety-related communication over Industrial Ethernet. With the PROFIsafe profile certified in accordance with IEC 61508, Profinet satisfies the highest safety requirements for the process and manufacturing industries in accordance with SILþ3 and ENþ954-1 Category 4.

Profinet offers a complete solution ranging from industry-compatible cables and connectors up to switches with real-time capability. A security concept specially tailored to automation engineering covers access control, data encryption, authentication and logging, and takes into account the high network security requirements.

By means of Profinet, Industrial Ethernet has been “reinvented”, and its success story extended by a further chapter.

It is also our hope with the second edition of this book that readers will become rapidly and practically acquainted with the topic of Profinet. In addition to correc-

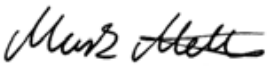
tions, the previous focal points “Distributed I/O” and “Distributed automation” have been updated, and the new topic “Safety” included.

This new edition would not have been possible without our readers and their interest in this exciting topic, without Siemens and its friendly support in all technical matters. Thanks also to everyone who proof-read it in their free time and contributed to continuous improvement of the book with a wide range of constructive suggestions, and last but not least to our families for their understanding and patience during many late nights.

Sincere thanks to all!

Erlangen, August 2008

Raimond Pigan



Mark Metter

Contents

1 From Contactor to Open Standard

The predecessors of current programmable logic controllers (PLC) were connection-oriented controls with the bis dato customary contactor controls. Up to that point in time, controls were characterized by circuit technology. Control tasks were solved by hardware connections between simple logic circuits. The hardware had high space requirements, but the flexibility was greatly limited: every modification usually required arduous conversion work.

In 1968, a group of engineers at General Motors designed the first PLC, and the first functional programmable controllers appeared at the beginning of the seventies. The first devices were designed similar to power equipment, and could be connected using the same cables and tools as for contactor controls. The most significant benefit was that modifications could be carried out independent of the hardware. Microprogrammed PLCs with multiprogram capability came on the market at the beginning of the 1980s, and permitted control tasks to be implemented in the form of software routines.

1.1 The Simatic Success Story

In 1958, Siemens AG introduced the Simatic G, a first modular but not yet programmable concept based on germanium semiconductors with resistor-transistor logic (RTL) (see Fig. 1.1). The Simatic N and H systems with silicone semiconductors and diode-transistor logic (DTL) initially followed in 1964. In the next step, the Simatic C1 and C2 with integrated circuits with high-noise-immunity and surge-proof logic (HLL) were launched on the market starting in 1971, as well as the Simatic C3 with transistor-transistor logic (TTL). One feature was common to these continuously improved systems: none of them was freely-programmable.

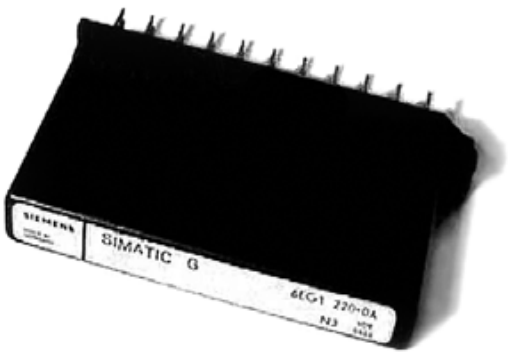


Fig. 1.1
Simatic G module

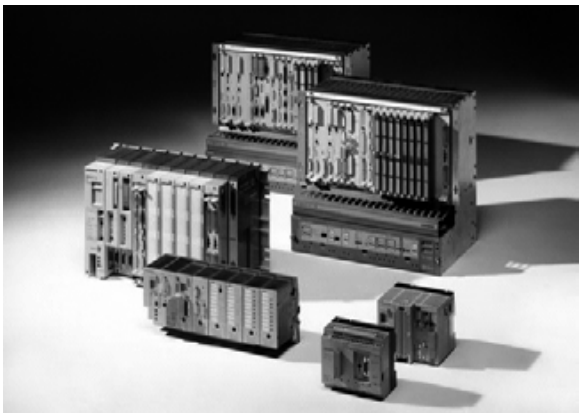


Fig. 1.2 Simatic S5

The freely-programmable Simatic S3 controller was developed in 1973. This PLC is the great-grandfather of modern PLCs. With the Simatic S5 system in 1979, Siemens achieved the complete breakthrough in the mass market to become the global leader (Fig. 1.2).

The Simatic S5 could be programmed using various special languages. Those initially used were the statement list (STL), function block diagram (FBD) and ladder diagram (LAD) in the Step5 software package.

The Simatic S7 range was introduced in 1995. Simatic S7 is the basis for Totally Integrated Automation (TIA). TIA is a uniform solution platform from Siemens for all industrial sectors, and consists of a complete range of matched products and solutions for solving automation tasks.

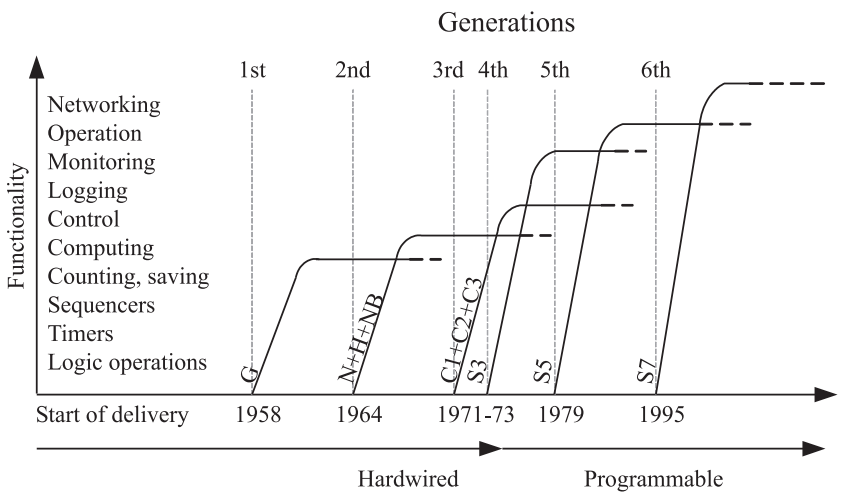


Fig. 1.3 Summary of dates and functions of the Simatic generations

In the course of further development of the Simatic S7, the range was extended by a series of controllers with graded performances and configurations with the associated signal converters for various input and output voltages as well as output currents. In the meantime, the range extends from small PLCs for simple binary operations up to large devices for complex tasks which previously could only be handled by process computers (see Fig. 1.3).

One of the most important factors in the development was the simple handling of the system. A rugged design without fans has been made possible which permits direct connection of external cables using screw or plug systems.

Not only the controllers developed further, the programming environment did as well. In addition to the generation of programs, the programming devices allowed their correction and documentation, plant commissioning and troubleshooting. To permit the supervision and documentation of functional sequences it soon became possible to connect standard I/O devices such as printers and display terminals to the PLCs. The first Windows-based graphical user interfaces for programming became available from 1985. Programming with comment lines and the structured design of PLC programs then became possible.

1.1.1 Change in Structure Through Decentralization

The next innovation jump in the PLC's history was triggered by a change in structure toward the decentralization of inputs and outputs. Decisive for this was the desire to reduce cabling costs. The I/Os moved closer to the place of action, and were connected to the central controller by means of thin two-wire or four-wire cables (fieldbuses). Mini programmable controllers now handled simple tasks directly on site, the central PLCs were offloaded. Control commands were passed on from the central controllers to the distributed switching devices over fieldbus networks. The first I/O devices in IP 65/67 degree of protection meant that additional terminal boxes could also be omitted.

It became quickly evident that further field devices such as drives or valves are required for a distributed automation solution in addition to the distributed input and output devices. At the beginning of the 1990s, a start was made toward standardization of many fieldbuses with the target of defining a future-oriented standard open to all manufacturers. Nowadays, all important bus systems can be connected over different communication interfaces, where Industrial Ethernet, Profibus and AS-Interface are the most important representatives in Europe.

1.2 The Road to Industrial Ethernet

Robert Metcalf presented his idea of the "Ethernet" (Fig. 1.4) at the National Computer Conference in 1976. The term "Ethernet" should be a reminder of the old idea of the "light ether" which surrounds the earth and which, according to ancient tradition, was the propagation medium for electromagnetic energy. Similar to the "light ether", the coaxial cable should be the passive medium for passing on the message from a transmitter to all connected participants.

In 1980, a group of companies with DEC, Intel and Xerox published the so-called DIX standard. This replaced the bis dato experimental state of the Ethernet by an open, fully-specified 10-Mb/s system. Standardization was carried out in 1985 by the Institute of Electrical and Electronics Engineers (IEEE) under the number 802.3 as a networking standard for local area networks (LANs). The way was then opened up for establishment as an industrial standard.

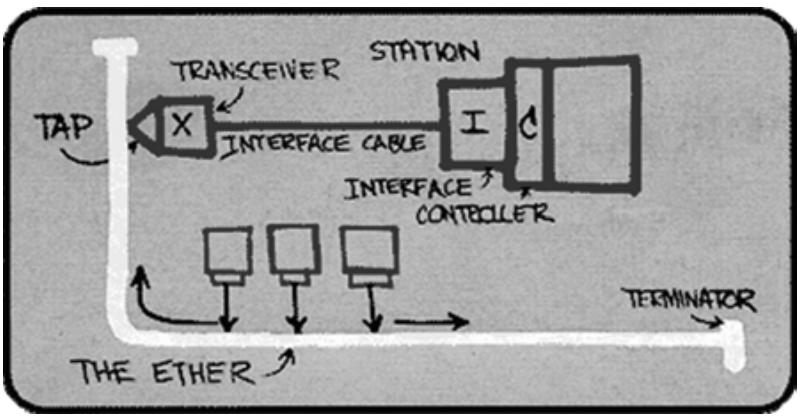


Fig. 1.4 Presentation of the Ethernet at the National Computer Conference

The so-called “Ethernet” is basically a data network technology based on data frames. Ethernet allows all participants present in a LAN to exchange data with every other device connected in the same network in the form of so-called frames or packets. Nowadays, Ethernet technology links devices over long distances all over the globe. The Internet is based completely on this technology. Ethernet describes the type of signaling, and defines the packet formats and protocols. Various components of it also specify standards for media such as cables and connectors. From the viewpoint of the OSI model, Ethernet specifies both the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2). Ethernet is standardized to the greatest possible extent in the IEEE standard 802.3. In the nineties, it advanced to the most widely used LAN technology, and has now displaced all other LAN standards such as Token Ring, FDDI and ARCNET. Ethernet can provide the basis for network protocols such as TCP/IP, AppleTalk or DECnet.

A number of extensions to the Ethernet standard were introduced in the course of time, especially with respect to cabling and speed. The original Ethernet 10BASE5, also known in the meantime as “Thicknet” is of no significance any more. The Thicknet was followed by 10BASE2 “Thinnet”, also named Thinwire or Cheapernet. 10BASE2 used significantly thinner and therefore cheaper coaxial cables, and became extremely popular. It can still be encountered in home or older office networks. The triumph of the twisted-pair standard started in 1990. With 10BASE-T and the associated data transmission rate of 10 Mb/s, Ethernet achieved the final industrial breakthrough.

The Fast Ethernet story started in June 1993. More than 50 vendors combined in the Fast Ethernet Alliance with the common goal of specifying a 100-Mb/s Ethernet. This goal was achieved in June 1995 with adoption of the Fast Ethernet standard IEEE 802.3u (100Base-T) for data transmission at 100 Mb/s on twisted pairs of cables. In 1999, a further step was completed with standardization of the Gigabit Ethernet, followed by the standard IEEE 802.3ae for 10-Gigabit Ethernet in 2001. In the meantime, Ethernet is the number one in the LAN landscape with a continuously increasing share of currently more than 80% worldwide.

1.2.1 Industrial Ethernet

In 1985, the year in which the IEEE 802.3 was adopted as the standard, Siemens AG introduced Ethernet for industrial applications under the name “SINEC H1”. This was the birth of Industrial Ethernet, which was necessary because the application conditions for Ethernet in an industrial environment differ fundamentally from those in an office environment:

- Plant-specific cable routing with an individual degree of networking for each machine/plant, with linear or redundant network structures
- Rugged and industry-compatible components with signaling contacts, cables and plug connectors, with special demands on EMC (electromagnetic compatibility)
- Ambient conditions such as temperature, vibration, moisture and contamination (oil, lubricants, coolants, cleaning agents).

In contrast to the conventional Ethernet, SINEC H1 had a significantly higher noise immunity, fixed screw connections, and a plant-wide earthing concept. It is the first example exhibiting the basic idea of Industrial Ethernet: existing standards are used to supplement necessary and beneficial details for industrial communication. A deviation from the standard is only present where the standard definitions do not consider the requirements of the production and process environment. In this manner, problem-free interaction between Industrial Ethernet and conventional Ethernet components is always guaranteed.

Milestones in the Industrial Ethernet history:

- 1985 SINEC H1 bus cable: standard yellow cable equipped with additional solid aluminium shield; plant-wide earthing concept.
- 1989 Redundant bus structure: increased network availability through dual bus structure; access control using special software in the automation systems.
- 1992 Fiber-optic networks: modular star hubs and rugged fiber-optic cables for industry.
- 1994 Redundant optical rings: high availability through optical rings with star hubs; ring structure reduces costs for media redundancy in the network.
- 1995 Industrial twisted pair: twisted two-wire cables with extra-thick shield; connections with Sub-D technology.

- 1996 Optimized optical components and uniform signaling concept: optical link module (OLM) and DIN rail star hub provide cost benefits with comparable redundancy functionality. Digital signaling contacts are available for OLM and star hub through which the network statuses can be incorporated into an existing HMI system (e.g. WIN CC), expensive network management is omitted.
- 1998 Switching and 100 Mb/s: proven Industrial Ethernet concepts are now also available for Fast Ethernet. Information technology is introduced to industrial communication (Simatic Net-CP 443-1 IT for Simatic S7-400).
- 1999 Simatic S7 goes IT – CP 443-1 IT links Simatic to the Internet.
- 2001 Mobile communication starts in industry: mobile applications are implemented using wireless LAN by means of the MOBIC Internet pad.
- 2003 Profinet: the two bus systems grow together by means of link modules for Profibus and Ethernet. Component-based automation becomes possible.
- 2004 Profinet: Industrial Ethernet receives real-time capability.
- 2005 Profinet starts in the field – many automotive companies are applying Profinet as the standard for future applications.

1.3 Profinet

Four years after being initially announced by Profibus International at a press conference in August 2000, the basis for Profinet (PROcess FIeld NET) is now available. This includes installation technology, real-time communication, network management and functions for Web integration (Fig. 1.5).

To provide optimum support for different types of application, Profinet offers two possibilities: Profinet IO for the integration of distributed I/O, and Profinet CBA for

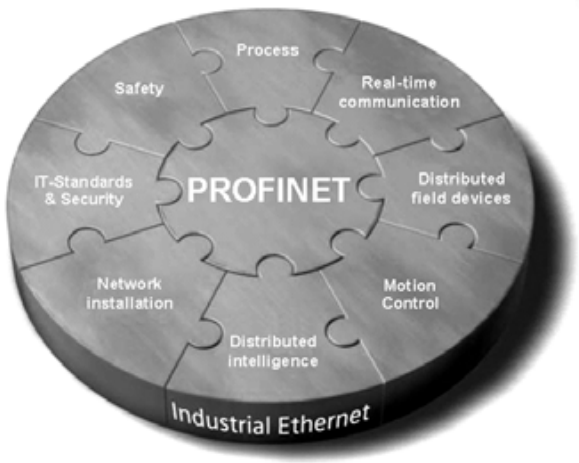


Fig. 1.5
Profinet as modular concept

Layer	Task	ISO/OSI reference model	
7b	Processing	Profinet IO services (IEC 61784) Profinet IO protocol (IEC 61158)	Profinet CBA (IEC 61158 Type 10)
7a		Connectionless RPC	DCOM Connection-oriented RPC
6	Display	Empty	Empty
5	Communication	Empty	Empty
4	Transport	UDP (RFC 768)	TCP (RFC 793)
3	Switching	IP (RFC 791)	
2	Security	Full duplex (IEEE 802.3), priority tagging (IEEE 802.1Q) real-time expansion (IEC 61784-2 available soon)	
1	Bit transmission	100Base-TX, 100Base-FX (IEEE 802.a3)	

Fig. 1.6 Profinet in the ISO/OSI 7-layer model

the creation of modular plants in distributed automation. Through its proxy concept, Profinet allows seamless integration of fieldbus systems. This is an important function to permit simple plant expansions.

However, Profinet is much more than just an optimum communication system for automation engineering based on Industrial Ethernet (Fig. 1.6). Profinet is a comprehensive standard which fulfills all demands for use of Ethernet in industrial automation, covering communication at the controller level, standard automation with I/O systems, up to powerful motion control applications. Profinet is therefore suitable for all automation applications.

The development of Profinet is still continuing. Work is in progress on definitions for the topics of security and safety, as well as conversion of the Profidrive profile to Profinet to permit motion control applications. The topic of maintenance operations has also been started as an initial step toward an interface to the MES level.

With respect to process automation, demands for the use of Profinet are currently being defined. With the establishment of the Working Group (WG) “Train Applications”, work has been started on the first “thoroughbred” Profinet profile.

Early introduction of product certification was additionally very important for Profinet. This is a measure accompanying the technological development through which a high quality standard for Profinet products is guaranteed right from the beginning.

1.3.1 Profinet IO

Profinet IO permits direct interfacing of distributed field devices on the Ethernet. All devices used are connected in a uniform network structure, and therefore offer uniform communication throughout the complete production plant. The user view of Profibus DP has been largely applied to configuring, programming and diagnostics.

Profinet IO specifies the complete data exchange between IO controllers and the IO devices, as well as their parameterization and diagnostics. It is designed for fast data exchange with bus cycle times of a few milliseconds, and is based on a provider/consumer model. Field devices in a subordinate Profibus segment can be integrated into the Profinet IO System using a proxy.

1.3.2 Profinet CBA

Profinet CBA (CBA: Component Based Automation) defines a further view of an automation plant. The basic consideration of CBA is that an automation plant can be divided in many cases into autonomous units, the so-called technological modules. The design and functionality may also be found in several units in identical or slightly modified form.

Such technological modules are usually controlled by a manageable number of input signals. They possess a functionality defined by a control program written by the user, and output the signals generated in this manner to another controller.

Profinet components are the representatives of such a module with its inputs and outputs in the engineering system. They are produced independent of the vendor, and the communication of a component-based system is programmed. Profinet CBA supports exception-based and deterministic communication, and with its transmission cycles of up to 10 ms is highly suitable for communication between controllers.

1.3.3 Real-Time Communication

Profinet communication can be scaled in three steps. Profinet CBA uses both TCP/IP (Transmission Control Protocol/Internet Protocol) and real-time communication (RT), and permits cycle times with an order of magnitude of 100 ms (TCP/IP) down to 10 ms (RT). It is preferably used for communication between PLCs.

Profinet IO exclusively uses real-time communication for exchanging process data. With the cycle times which can be achieved with an order of magnitude of 10 ms, Profinet IO is highly suitable for use in the distributed I/O sector (factory automation).

Isochronous real-time communication (IRT) enables cycle times with an order of magnitude of 1 ms, and is therefore highly suitable for use in the motion control sector.

Profinet CBA basically comprises the component-based communication using TCP/IP and the RT communication with components. Profinet IO uses the RT and IRT communication with the distributed I/O.

1.3.4 Fieldbus Integration

Profibus can already look back to an installed basis of more than ten million nodes. This world leadership is also associated with the obligation to offer a simple and seamless transition strategy for interfacing existing Profibus systems to

Profinet. For this purpose, Profinet supports a proxy concept which makes it possible to integrate any installed field devices into Profinet without modifications.

A proxy largely consists of two main components, an Ethernet-based unit and a fieldbus unit, for example a Profibus DP master. This guarantees that all I/O and diagnostics data can be exchanged with the configured slaves. The result is then placed by the DP master in a common memory. With Profinet CBA, for example, the Profinet unit of the proxy accesses this memory and transmits the data present there to the respective consumers by means of the configured links. If the consumer is present in the Profibus unit, the Profibus DP master transmits the arriving link data to the respective DP slave in the next Profibus cycle.

1.3.5 Security

The following trend has been recognized for some time in the automation sector: comparatively isolated cell or island solutions are being replaced by networked and increasingly homogeneous automation structures. It is basically already possible today to communicate with any PLC from any location.

This is associated with increased possibilities for errors both during operation and also in the device addressing. In addition, the number of possibilities for espionage and sabotage is increased. The increasing use of Ethernet in the automation sector, the possibilities for remote maintenance over the Internet, and interconnection of the plant network with office networks or a company's own intranet are not exceptions.

Since the security concepts from the office sector are hardly suitable for the special requirements in the automation sector, the development of new security concepts is necessary for the automation technology. These concepts must be simple to use and tailored to the special requirements, protocols and network topologies of the automation technology, since even short-term network breakdowns can result in production outages or enormous damage to mankind and machines.

The Profinet security concept takes account of the higher network security requirements in Ethernet-based automation systems. This concept covers access control, data encryption, authentication and logging of safety-relevant events.

The core of the security concept is the security-oriented segmenting of the automation network. Protected automation cells are then generated. The network nodes within a cell are protected by special security network components such as switches or security appliances. These network components control the data transfer to and from such a cell, and only permit it if it has been previously authorized by access privileges.

Special security client software can be used for access to protected PLCs by client PCs. The data terminals do not require their own security functionality. Data transfer between the protected cells or between the client and the cell nodes can additionally be encrypted, and thus reliably protected against data espionage or manipulation. This is particularly interesting for communication over non-secure networks, as is the case e.g. with remote access over Internet for servicing purposes.

1.3.6 Motion Control with Profinet

Profinet's performance allows motion control applications with a higher number of axes, larger data quantities and shorter cycle times. Corresponding activities for implementation in Profinet were commenced by the Profidrive Working Group of Profibus International in summer 2004. The objective of the activities is to map the Profidrive profile established for Profibus in Profinet such that simple conversion is possible.

The functionality and interface modeling remain consistent. Profidrive@Profinet applies the known application scenarios and an unchanged user view, meaning that it is not necessary to modify the user program when converting the devices. Profidrive@Profinet applies RT and IRT for communication.

1.3.7 Safety on Profinet

Safety engineering is a central component of many automation systems. Whereas this was solved in the past using classical relay technology, the trend is now toward integration in open, standardized communication systems. Special buses are being accepted less and less. For example, the automotive industry demands rapid implementation of the more secure Profinet communication.

As a result, activities for achieving user-friendly and secure data transmission for Profinet IO was initiated by Profibus International in the middle of 2004. The draft specification was completed for the Hanover trade fair 2005 for review by the members. The necessary coordination with the TÜV and the Bundesgenossenschaftliche Institut für Arbeitsschutz (Federal Cooperative Institute for Occupational Safety, BIA) has already been commenced.

Based on Profinet IO, the protocol of the proven PROFIsafe will be applied, thus making use of the "black channel" principle. It will be possible to use the safety solution for safety applications up to Category 4 and SIL3 (Safety Integrity Level 3).

2 Ethernet – Fundamentals and Protocols

Profinet is based on Ethernet technology and uses standards such as TCP/IP. To be able to understand Profinet better, it is important to know and apply these fundamentals. It would be beyond the scope of this book to treat the physical Ethernet with all its required protocols completely and in detail. However, we wish to present the most important information on Ethernet and the basic protocols here so that you can understand and apply the necessary background knowledge.

2.1 Fundamental Structure of Ethernet

In the "classical" Ethernet, all stations have equal privileges, so that each station can exchange any quantity of data with any other station at any time. Since the classical Ethernet is basically designed as a logical bus system, a sending station is listened to by all other stations. Each Ethernet station filters out the data packets meant for it, and ignores all others. All stations therefore share the transmission medium, and are combined in the so-called collision domain. Network access is controlled by the CSMA/CD procedure (Carrier Sense Multiple Access with Collision Detection). If a station wishes to send data, it first checks whether the network is free (carrier sense). Data transmission can commence if this is the case. A check is carried out at the same time as to whether other stations have also commenced sending (collision detection). A data collision occurs if this is the case. All involved stations then stop transmitting data, and wait for a period of time generated according to a random principle. A new attempt to send is carried out after this time has expired. As a result of the CSMA/CD procedure, the transmission time for data packets largely depends on the network loading, and cannot be determined in advance. The complete network becomes "slower" as the number of collisions increases. Shared Ethernet with collisions is therefore only conditionally suitable for industrial automation.

In industrial applications, use is therefore made of segmenting (division of collision domains), higher bandwidths such as Fast Ethernet and Gigabit Ethernet, and switching technology. All these technologies are used for Profinet, and Ethernet therefore becomes interesting and useful for industrial automation.

Profinet Ethernet is basically a network of stations which are connected together through network components by means of cables with point-to-point connections. The stations with their NIC (Network Interface Card) – CPs (communications processors) in the case of automation systems – are the end points of the network. Network components such as hubs, switches and routers are required in order to switch the data between the end points. Twisted copper conductors with a maximum transmission rate of 100 Mb/s (Fast Ethernet) are mostly used for the wiring

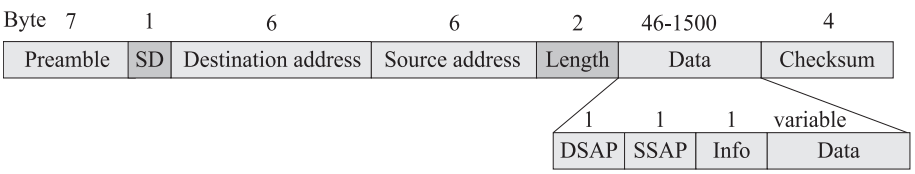
between network components and stations. Through the use of separate send and receive lines (one-way streets), the stations are able to send and receive data simultaneously without collision. This type of communication is referred to as full duplex (FDX, simultaneous sending and receiving of data). Full duplex is always based on a star topology where two components are always linked to each other by a point-to-point connection. The network then consists of many point-to-point connections. The actual access control is thus reduced to the connection of the two stations of the point-to-point link.

In this network, the cables to the communication partners are switched in line with the requirements by special network components, simply referred to as switches. This principle is referred to as “Switched media”. Profinet always applies Ethernet with a 100 Mb/s Fast Ethernet connection in full duplex in a switched network.

2.2 Standard Ethernet Frame

Ethernet is a so-called packet switching network. This means that the data to be transmitted are divided into smaller units referred to as packets or frames (see Fig. 2.1). Each of these packets contains all required information, e.g. receiver and transmitter addresses, data and error checking information. The packet is sent as a unit, and can be between 64 and 1526 bytes long. Two frame formats exist in the original Ethernet definition:

- The original standard of the DIX group (also called Ethernet II, DIX or BlueBook)
- The standard according to IEEE 802.3



Preamble	7 bytes for synchronizing the stations (101010...101010)
SD (Start Delimiter)	1 byte for completion of transient reaction (10101011)
Destination address	6 bytes for identification of destination station (MAC address)
Source address	6 bytes for identification of data source of destination station (MAC address)
Length	2 bytes length block
Data block	46-1500 bytes user data. This block contains the data and header which have been transmitted by the higher layers. It contains: DSAP: Destination service access point (1 byte) SSAP: Source service access point (1 byte) Info: Control block (1 byte) Data: User data (variable)
Checksum	4-byte checksum. This is generated and applied to check the correct transmission of data.

Fig. 2.1 Ethernet data packet, IEEE 802.3

The difference between the two packet formats is in the use of the header blocks: DIX Ethernet has a type block, IEEE 802.3 has a length block at the same position. Because the IEEE 802.3 standard is used to a far greater extent, only this will be treated below.

2.3 Ethernet or MAC Address

The specific addressing in the network means that each station must have its own address at which it can be reached. Each Ethernet interface has therefore been assigned an address by the vendor which is fixed and unequivocal worldwide. This address is referred to as the hardware or MAC address (Media Access Control), but also as the Ethernet, station, physical or network card address. This is saved on the network card, and is used to identify it in the local network. Through cooperation between vendors, it is guaranteed that this address is unequivocal worldwide. The MAC address has a fixed length of 48 bits (6 bytes). The first three bytes are used to identify the device vendor, the others are freely-assigned by the vendor. In order to guarantee that identical addresses cannot occur in a network, the Ethernet addresses are usually coded in the hardware by the vendors and cannot be changed. The distribution is carried out in line with a fixed key.

2.3.1 How to Find Out the MAC Address of an Ethernet Device?

With Simatic Ethernet devices, the simplest way is to look at the stamp/label on the network card or on the housing of the communications processor. A red leaflet may also be enclosed with the device with a guaranteed unequivocal Ethernet address assigned by Siemens to this device. This address is then assigned to the Ethernet station in the HW-Config of Step 7.

Such a stamp/label is normally missing with PC network cards. Depending on the operating system used, there are various possibilities for determining and displaying the hardware address. With Windows systems, start the DOS prompt *Start > Run > cmd* and enter the command *ipconfig /all*.

2.4 Shared Ethernet

A so-called Shared Ethernet functions according to the non-deterministic principle: all stations have equal rights, and are arranged in a linear topology. Every station on the network receives the data sent by the other stations. Each station filters out the data packets intended for it from the data stream, and ignores the uninteresting packets. Reliable collision detection is necessary to prevent the data collisions which can result with this principle. The term Shared Ethernet indicates that the transmission medium available is divided.

The access procedure required was developed at the University of Hawaii, and therefore also has the byname “Aloah protocol”. The correct designation is

CSMA/CD (Carrier Sense Multiple Access with Collision Detect). The procedure controls access of the systems to the shared medium, and is shown in Fig. 2.2. Each station on the network can send at any time when the transmission medium is free, and can exchange data with any other station.

In the Ethernet, one can imagine the common medium as a cable in a type of bus topology. All stations have equal rights – there is no master. All Ethernet stations access the common transmission medium independent of one another. Before a station actually carries out a transmission, it first taps the cable (carrier sensing) to establish whether data exchange is already taking place between other stations. If the medium is free, the station immediately starts to transmit. If the line is occupied, the station waits until it becomes free, and then starts the transmission. Since the network is designed as a bus system, all data packets pass through all connected segments. Tapping is continued throughout the transmission in order to determine whether there is a collision with another station which by chance started a transmission at the same time (collisions detect). If there are no collisions, all stations in the network check the received data packets and accept those which are addressed to themselves. All other packets are ignored by the station.

If several stations are waiting to transmit messages over the LAN, it may be that a number of them recognize the medium as being free at the same time. If these stations then attempt to simultaneously transmit their data to the medium, the messages are superimposed. The result is that data are lost. This type of event is referred to as a collision. Since the station is still tapping the LAN when transmitting, it recognizes that a collision has occurred and immediately stops transmitting any further.

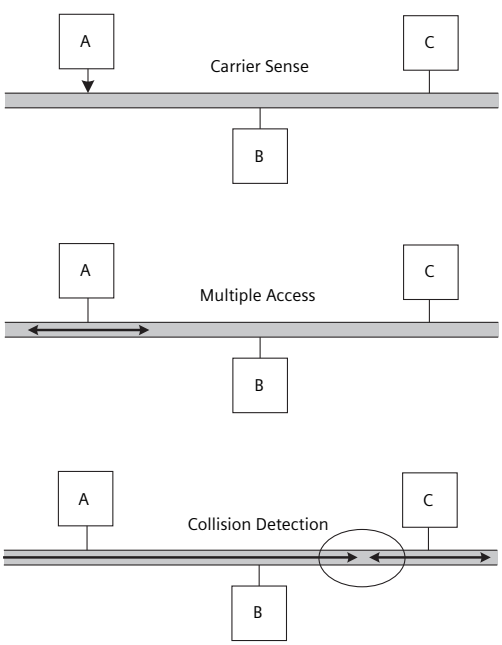


Fig. 2.2
The CSMA/CD principle

The station which detects the collision first then applies a jam signal (101010 ... = AAAAAAAA(hex.)) to the line which indicates to all connected stations that a collision has occurred, and requests the interruption of all transmissions.

Following the collision, each of the involved stations waits for a random time – which differs from station to station – before attempting to send its data packet again. This procedure is repeated until an abort occurs or until the complete data transmission has been successful. Since this transmission duration is unpredictable, it is not possible to determine in advance when exactly a data packet will reliably reach the receiver. Therefore, Shared Ethernet networks are inappropriate for real-time communication, since this requires an exact, deterministic message frame runtime.

2.5 Switched Ethernet – Fast Ethernet

The Fast Ethernet standard is basically oriented on the classic Ethernet standard with a transmission rate increased by a factor of 10 to 100 Mb/s as well as intelligent switching technology in full duplex mode. This collision-free procedure is also referred to as Switched Ethernet.

Shared Ethernet and Switched Ethernet have the following common features:

- Data format: packet lengths from 64 to 1518 bytes,
  address field length: 48 bytes
- Access procedure: CSMA/CD
- Same cables (except for the coaxial cables)

Addressing, frame format, access procedure, installation etc. are practically identical to the old Shared Ethernet standard. It is only necessary to observe the extensions which are specific to the Fast Ethernet and which basically refer to the specifications of cables, cable lengths and repeaters. The advantage for users is quite clear: existing technological know-how and old investments or plants can continue to be used without limitation.

In the Switched Ethernet, the linear topologies are canceled and replaced by star topologies with intelligent star distributors, the so-called switches. Point-to-point connections are made via the central nodes. This procedure is identified by the name Switched Ethernet. Nowadays, Fast Ethernets always operate as a collision-free Switched Ethernet.

2.5.1 Switches as Intelligent Star Distributors

A switch is an electronic device similar to a hub for connecting several computers or network segments in a local network (LAN). One also refers to a switch as an intelligent hub.

The task of the switches is to intelligently redefine the path of each data packet depending on the destination address. Communication is then possible in full du-

plex mode, i.e. data can be sent and received simultaneously. Division of the transmission medium as with the Shared Ethernet no longer takes place. At any one time, different data packets can be simultaneously present in the network on different transmission paths. The data packets only pass through segments which lead to the receiver. The collision domain is thus divided into several smaller collision domains, resulting in a reduction in the number of collisions or the complete elimination thereof. Individual LAN segments or even individual stations can then communicate with one another without loading the rest of the network. This freedom from collisions permits almost deterministic operation. The available bandwidth of a local network is therefore divided more effectively between a few users, resulting in a significant increase in data throughput.

A switch is hardware-based, and thus permits extremely short switching cycles. It processes and analyzes the MAC addresses of the received data packets, and generates a SAT (Source Address Table). This table lists which stations can be accessed via which port. For this purpose, the sender MAC addresses of the frames which have been passed through are saved during operation. Data is therefore only passed on to the port to which the receiver is actually connected. As a result of this filtering and specific forwarding, the local data traffic really remains local. Packets with an unknown destination MAC address are handled like broadcasts, and passed on to all ports except the source port. Switch intelligence also analyzes the data packages, and only valid message frames are passed on. Invalid or damaged frames are destroyed in the switch and not passed on to any stations, thus preventing undesirable spreading. The individual ports of a switch can receive and send data independently of each other. The ports are connected together over an internal high-speed bus (backplane). Data buffers ensure that no message frames are lost if at all possible. This means packets can be transferred at maximum speed between the individual ports.

2.5.2 Full Duplex and Half Duplex Modes in the Switched Ethernet

An optional transmission procedure for Switched Ethernet is full duplex (FDX). An adaptation of this is half duplex (HDX). Both procedures are basically nothing more than operating modes in the network. Whereas stations can alternately send and receive data with HDX, they are able in FDX mode to simultaneously send and receive data without collisions. Since collisions are no longer possible in this case, the transmission rate is increased even further. The more recent Ethernet standards such as Gigabit Ethernet will only be available with the full duplex procedure. A star topology is always used with FDX, where two components are always connected together by a point-to-point connection. The network therefore comprises many point-to-point connections. This means that the actual access control is reduced to connection of the two stations involved in the point-to-point connection.

Each station is always connected to a transmitter line and a receiver line. Simultaneous transmission and receiving is therefore possible at all times, since no collisions can occur in these “one-way streets”. The only potential problem is that a receiver cannot pass on the received data fast enough from its receive buffer, the re-

sult being an overflow with data loss. If this can be foreseen, the receiver sends a pause frame with a defined waiting time to the transmitter. When received, the transmitter immediately stops its transmission, and starts the defined waiting time of the pause frame. The transmitter recommences data transmission following expiry of this time. If the receiver memory has been emptied faster than expected, the receiver can send a pause frame with a waiting time of zero, and the transmitter then starts a further transmission immediately.

With half duplex mode, the transmitter and receiver use the same physical medium (line). Only one partner can transmit at any one time, the other partner can only receive data. The communication partners alternate in the use of the medium for transmitting data. The classic coaxial cable is a typical example of a half duplex medium. The majority of installed twisted-pair and fiber-optic cables also use half duplex mode. Whereas a number of proprietary full duplex solutions exist for the classic Ethernet, collision-free full duplex connections are specifically defined in the Fast Ethernet standard.

Full duplex mode has some important advantages:

- Very simple procedure, extremely stable and collision-free
- 100% network loading is possible
- Since no collisions occur, the data throughput is increased to twice the nominal data transfer rate of the network
- It is possible to expand the network size up to the performance limits of the transmitter and receiver components used since the maximum cable length is only limited by the signal attenuation.

As a result of the deterministic message frame runtime without collisions in full duplex mode as present in the Switched Ethernet, it is possible to use this type of connection for real-time communication with Profinet.

2.6 Functions for Ethernet

The following functions are implemented in every Profinet device. They will be briefly explained to enable better understanding.

2.6.1 Autonegotiation

This is understood to be automatic recognition of the interface functionality of the opposite end. Repeaters or data terminals can use the autonegotiation procedure to determine this functionality, permitting automatic configuration of different devices. The autonegotiation procedure enables two components connected in a link segment to exchange parameters and to apply these parameters to permit adjustment to the respectively supported fundamental communication data.

To guarantee explicit configuration, it is also possible to deactivate the autonegotiation. The great advantage of autonegotiation is the problem-free interoperability

of all Ethernet components. Classical Ethernet components which do not support autonegotiation can work together without problem with the new Fast Ethernet components which possess this function. Devices without autonegotiation must at least be set to fixed values of 100 Mb/half duplex or 10 Mb/half duplex.

2.6.2 Autosensing – Automatic Recognition of Data Rate

Autosensing describes the property of network nodes (data terminals and network components) to automatically determine the data rate of a signal (10 Mb/s or 100 Mb/s) and to set themselves to this if possible. Autonegotiation is usually supported at the same time. All new Simatic Net Profinet devices possess the autonegotiation/autosensing functionality.

2.6.3 MDI/MDI-X Autocrossover

This function offers the advantage of continuous cabling without the need for external, crossed Ethernet cables. This prevents malfunctions caused by incorrectly connected transmit and receive lines. Installation becomes far simpler for the user.

2.7 Gigabit Ethernet – an Introduction

The Gigabit Ethernet activities are handled in the working groups 802.3z and 802.3ab of the Institute of Electrical and Electronics Engineers (IEEE) which were established in November 1995. The Gigabit Ethernet activities result in a tenfold increase in data throughput compared with Fast Ethernet technology. Transmission rates of 1 Gb/s make this technology particularly interesting for use in LAN backbones. At the same time, downward compatibility is guaranteed with the existing 802.3 Ethernet format, along with partial retention of the CSMA/CD access procedure. The frame format of 802.3 is to be retained, as well as the minimum frame length limit of 64 bytes and the maximum frame length limit of 1,518 bytes. The collision domain is 200þm for all transmission media. Gigabit Ethernet offers full duplex mode for point-to-point connections as well as half duplex mode.

Gigabit Ethernet only supports star topologies with all transmission media recommended in cabling standard ISO/IEC 11801. Working group 802.3z develops the standards for monomode fibers, multimode fibers and STP cables, whereas working group 802.3ab concentrates on the standardization of Gigabit Ethernet on UTP cables (Unshielded Twisted Pair) in the cabling of workstations. In the latter, UTP cables of Category 5 can be used with the connection length of up to 100þm defined in the cabling standard.

The Gigabit Ethernet architecture standard draft not only defines modifications to the existing CSMA/CD procedure. The basic standard also comprises – in addition to the MAC layer which is unchanged apart from the higher transfer rate – four different physical technologies: 1000Base-CX, 1000Base-T, 1000Base-SX and 1000Base-LX.

2.8 10-Gigabit Ethernet

The IEEE working group 802.3ae has been occupied since 1999 with standardization of the 10-Gb/s Ethernet (10GbE), and has defined the basic elements for this technology. The 802.3 and Ethernet frame formats, the existing minimum and maximum frame lengths, as well as the coexistence with Power over Ethernet (PoE) in accordance with 802.3af have been retained. Also supported are star topologies with point-to-point connections (PP) and just one full duplex mode in accordance with IEEE 802.3x. The 10GbE layer model supports a data transfer rate of 10 Gb/s on the MAC interface. Furthermore, structured cabling in accordance with ISO/IEC 11801 has been integrated into the latest version.

2.9 Power over Ethernet (PoE)

Power over Ethernet (PoE) is a technology with which networkable devices can be supplied with power over the 8-core Ethernet cable. The term PoE is commonly used to refer to IEEE standard 802.3af (“DTE power over MDI”) whose final version was adopted in June 2003. A number of vendor-specific implementations were previously available which also used the name Power over Ethernet. With this technology, either the vacant cores of the cable are used, or a DC component is transmitted via the four used cores in addition to the data signal. Correspondingly designed devices are provided with 48þV and up to 15.4þwatts. A logic circuit prevents devices without PoE capability from being supplied with power. In the standard, various scenarios are considered for transmitting power over the Ethernet for existing Ethernet infrastructures.

With PoE, it is possible for IP telephones, cableless access points and other devices to transmit power and data via the existing LAN infrastructure. The advantage of this technology is that devices connected to the Ethernet can be directly supplied with power. This includes those situated in inaccessible locations, such as for IP cameras and WLAN access points, or devices for IP telephony which draw power from a telephone cable.

Table 2.1 Power classes for the supply of devices using Power over Ethernet (PoE)

Power class in accordance with 802.3af	Current range	Max. input power of the Power Sourcing Equipment (PSE)	Max. power drawn by Powered Device (PD)
0	0 ... 15 mA	15.4 W	0.44 ... 12.9 W
1	8 ... 13 mA	4.0 W	0.44 ... 3.84 W
2	16 ... 21 mA	7.0 W	3.84 ... 6.49 W
3	25 ... 31 mA	15.4 W	6.49 ... 12.9 W
4	35 ... 45 mA	15.4 W	Reserved

A data connection must already be available in order to provide devices with power. So-called Power Sourcing Equipment (PSE) determines via this connection which devices are PoE-compatible and require power. Such terminal equipment is referred to as a Powered Device (PD). The PoE architecture can be used in the Ethernet, Fast Ethernet and Gigabit Ethernet, and consists of the Power Sourcing Equipment and the terminal equipment to be powered. Depending on the pin assignments of the data connectors, the vacant pin pairs 4/5 can be used with the RJ-45 connector for the positive and pin pairs 7/8 for the negative supply voltage. The assigned pin pairs 1/2 and 3/6 can also be used.

The standard 802.3af covers different performance classes with drawn powers between 0.44þW and 12.9þW (see Table 2.1). The voltage is 48þV. In a more powerful version PoE+, the drawn power is to be increased to at least 30þW, or even better to 60þW.

The challenge for the early manufacturers of proprietary PoE solutions was to avoid damage as far as possible to terminal equipment without PoE capability. Although cores 4, 5, 7 and 8 are not used according to the Ethernet standard, this does not mean that no network cards or similar exist on which the corresponding pins are routed somewhere. If Power over Ethernet is then present by mistake, this may lead to irreparable damage on the device. 802.3af solves this problem using a procedure referred to as Resistive Power Discovery. In this case the power supply repeatedly applies only a minimum current to the cores. The magnitude is such that no device would normally be damaged. It can then be recognized whether the load has a 25-kW terminating resistor, and where, and therefore a PoE capability. The load is then provided with a low power and must now signal which of the four power classes defined in the standard it belongs to. The PD is only then provided with the full power and can commence operation.

2.10 Protocols Based on Ethernet for Profinet

With the Ethernet protocol and TCP/IP (Transmission Control Protocol/Internet Protocol), this established standard for networks has also gained acceptance in industrial applications. Each Profinet station must support various protocols. These are at least TCP/IP and UDP/IP (User Datagram Protocol/Internet Protocol). Reason enough to become acquainted with the basic principles of these protocols.

2.10.1 TCP/IP

The TCP/IP protocol family was developed by the DARPA (Defense Advanced Research Projects Agency) in the seventies. The objective was to allow computer systems of highly different design to communicate with each other freely, whatever the location. TCP/IP is currently the most significant protocol both in offices and industrial environments. Not least because almost all communication on the Internet is handled using TCP/IP.

TCP/IP is actually a collection of individual protocols, each of which makes its contribution to allowing computers to communicate using the same language. The

protocol specifications are defined and published in so-called RFC documents (Request for Comment). As a result of their general implementation, they can be regarded as semi-official standards.

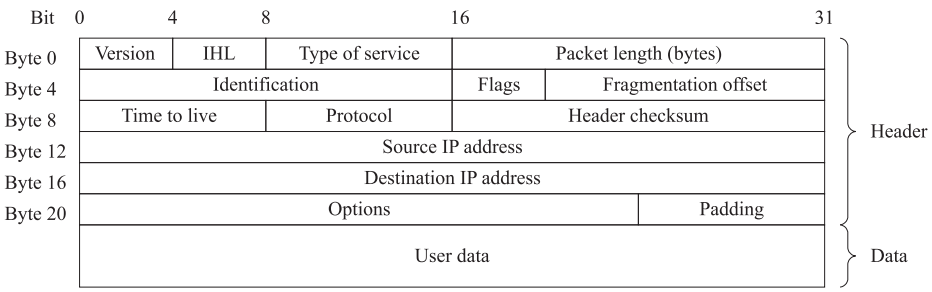
TCP/IP can be considered as a complete suite of protocols and consists of two parts. TCP stands for Transmission Control Protocol. This part of the protocol suite controls the transmission and thus the actual data transfer. The second part, the Internet Protocol (IP), is required in order to unequivocally address a computer in a network.

Internet protocol IP

The Internet protocol (IP) in the current version IPv4 allows the addressing and routing of data packets from the transmitter up to the receiver over several networks. IP is the addressing component of TCP/IP. Each station which wishes to communicate with another one is identified by an unequivocal IP address. This is comparable with an address on an envelope: using the address, the network recognizes the destination, and can then send the packet with the data to the correct receiver irrespective of the transmission path (Ethernet, token ring, ISDN).

The data packets with IP are called datagrams. The Internet protocol is a connectionless service with an Unreliable Datagram Service, i.e. neither the correctness of the data nor observation of the sequence, completeness and unambiguity of the datagrams is checked at the IP level. There are no acknowledgment mechanisms for IP. A reliable, connection-oriented service is implemented in the TCP level above this.

An IP datagram consists of a packet header followed by a data block which in turn is packed e.g. in an Ethernet frame. To implement its function, IP defines its own packet format which has a minimum length of 20 bytes.



Packet length: Total length of datagram including header (576-65,535 bytes).

Addresses: Transmitters and receivers in TCP/IP networks are identified by a 32-bit address which is unequivocal worldwide – the so-called IP address. The DENIC is the central authorized authority in Germany for assigning these addresses.

Source IP address: Internet address of source station

Destination IP address: Internet address of destination station

User data: This block of variable length finally contains the user data.

Fig. 2.3 Structure of an IP packet

Important blocks in the IP packet are shown in Fig. 2.3. Please refer to the relevant literature for the other blocks.

Format of IP addresses

The IP addressing defines logical network addresses for the TCP/IP protocol suite. The IP address is a fixed component of the Internet protocol (IP) and is independent of the hardware used, the vendor or the network medium used. These IP addresses are used as “Destination = receiver addresses” and “Source = transmitter addresses” in each data packet transmitted with the IP protocol. To ensure that there is always an unequivocal receiver for a packet, each station requires its own unequivocal address.

Each Profinet station connected over Ethernet must possess an IP address. As a protocol of layer 3 of the ISO/OSI reference model, the IP protocol is hardware-independent, permitting flexible assignment of the address. Contrary to level 2 communication, where a fixed MAC address is assigned to a device, it is necessary in the Ethernet to explicitly assign an address to a device.

The IP address consists of four bytes. Each byte has a decimal notation, and is separated from the previous one by a dot. This results in the following structure, where a number between 0 and 255 must be set for XXX: XXX.XXX.XXX.XXX e.g. 192.168.147.112

An IP address always consists of two (hidden) parts: a network ID and a station (host) ID, which together result in the actual IP address. The network ID is used to address the network, and the host ID to address the station within a network (see Fig. 2.4). This provides the advantage that many computers can be combined into groups, making it easier to find the actual computer. Telephone numbers have a similar structure. These also comprise an area code and an individual subscriber number.

The subnet mask was introduced to divide the IP address into the network component and the actual station component. This has the same structure as the IP addresses, but only marks the part of the IP address represented by the network number (network component). The standard subnet masks shown in Table 2.2 apply to the network classes A, B and C in line with the division of network and station addresses.

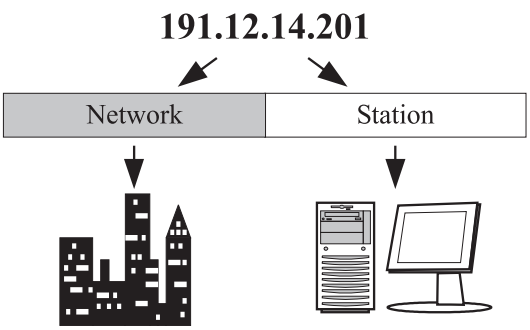


Fig. 2.4
Division of IP address into network and station components

Table 2.2 Summary of network classes

Network class	IP address ranges	Network ID	Host ID	Subnet mask
A	0.0.0.0 - 127.255.255.255	1 byte	3 byte	255.0.0.0
B	128.0.0.0 - 191.255.255.255	2 byte	2 byte	255.255.0.0
C	192.0.0.0 - 223.255.255.255	3 byte	1 byte	255.255.255.0

Please note: all devices connected via switches are in the same subnet. A subnet is produced by dividing all possible IP addresses into partial networks. The logical division of the network into subnets usually corresponds to the physical division into local partial networks. The division of a network class into further subnets using network masks is called subnetting. All devices in a subnet can directly communicate with one another. The subnet mask is identical for all devices in the same subnet. A subnet is physically limited by a router.

Classes of IP addresses

In order to provide this large number of addresses with an order and structure, they are divided into so-called network classes. IP addresses are divided into the five network classes A to E. This results in more efficient use of the IP addresses through definition of the stations which can be addressed in each class. The subnet mask determines which part of an IP address represents the network address (network ID) and which part the host address (host ID): the bits of an IP address belonging to the network ID identify the subnet mask with the value 1, those bits belonging to the host ID that with the value 0. Class D addresses are designed for multicast groups. The address range covers 224 to 239.x.x.x. Class E addresses are defined for future applications and are not currently in use. The address range in this case covers 240 to 255.x.x.x.

Before you commence configuration with assignment of addresses, you should have considered during the design phase which address area you wish to use for the Profinet devices in your network and how you wish to assign this address area. Subsequent changing of addresses resulting from an unfavorable assignment is extremely complex and therefore expensive. When selecting the address class and network address, you should ask the following questions:

- Is a connection planned to a public TCP/IP data network?
- How large will the TCP/IP data network be in the finally planned configuration?

One can basically say that almost any address from all address classes is a valid IP address which can be used in principle to configure a TCP/IP station. However, certain addresses in each network class are reserved for special services and should not be used.

Network address: If a station address only consists of zeros (e.g. 192.12.31.0 in a class C network), the address points to its own network and is therefore also referred to as the network address. In the case of this address, the IP protocol sends a wildcard address to the network. This means that all stations with a class C ad-

dress of structure 192.12.31.xxx are requested to send a reply. This results in the undesirable state of a “flooded” network with replies to non-existent computers. This address is not routed for this reason.

Default router address: Each subnet which communicates with other networks contains at least one router. According to the convention, this is always the first address following the network address. In a class C network, this is the address x.x.x.1. This is not a fixed and imperative rule, and can therefore be freely modified. However, it should be considered in the sense of the conventions for assigning IP addresses.

Local loopback address: The network address 127.0.0.1 identifies the respective local computer (loopback address or LOCALHOST). Packets with the address 127.0.0.1 immediately arrive back at the transmitter without ever having accessed the network. This is used to test the network in that stations can send messages to themselves for test purposes. The subnet mask in this case is 255.255.0.0. A network can therefore never have the address 127.x.x.x.

Broadcast addresses: The station address where all bits are set to “1” (e.g. 192.168.12.255 in a class C network) is used for broadcast messages in a subnet. Using this, data can be sent to all stations of the local network (subnet) or to all stations of the directly accessible networks.

IP addresses in public TCP/IP networks: If connection of a public TCP/IP data network is planned, you can no longer freely decide which IP address can be selected. The Internet is the largest example of a TCP/IP network. In this case, the addresses must always be unequivocal and therefore unique worldwide in order to guarantee correct functioning of such data networks. The assignment of the IP addresses is therefore regulated by a number of central authorities. Anyone wishing to connect a computer to the Internet must apply for one of these IP addresses depending on the planned network size. Responsible for the assignment of IP addresses on the Internet is the Internet Assigned Numbers Authority (IANA) in the USA. The local assignment authority for Germany is the Domain Verwaltungs- und Betriebsgesellschaft e.G. with the name DENIC. Each company or organization can apply here for an IP network address dependent on the planned network size.

IP addresses in a separate company network: If you design a company network without a connection to the Internet, you can theoretically select any network class with any valid station address.

To permit local networks without an Internet connection to be operated with TCP/IP, without having to apply for IP addresses, and in order to also test individual computer links, there is a range of addresses in each class (A, B, C) which has been released for “private” use. These addresses are not passed on externally by routers.

The IANA has defined the following IP addresses for this purpose:

- Class A networks: 10.0.0.0 - 10.255.255.255
- Class B networks: 172.16.0.0 - 172.31.255.255
- Class C networks: 192.168.0.0 - 192.168.255.255

Example: For a private class C network with only a few stations, the range of IP addresses from 192.168.0.0 to 192.168.255.255 released for a private network is sufficient. This means that the values for the network ID are fixed as 192 and 168. You can select any number between 0 and 255 for the third position of the network number. 101 has been selected in this example. The class C network address is therefore: 192.168.101.xxx.

Only the values from 1 to 254 for the fourth position of the IP address then remain for the actual stations (computers, Simatic CPs etc.) in the network, since the network address (x.x.x.0) and broadcast address (x.x.x.255) must not be used. All computers in your network therefore have the same IP address apart from the last position.

IP addresses of computers:	192.168.101.1 to 192.168.101.254
Network address:	192.168.147.0
Broadcast address:	192.168.147.255

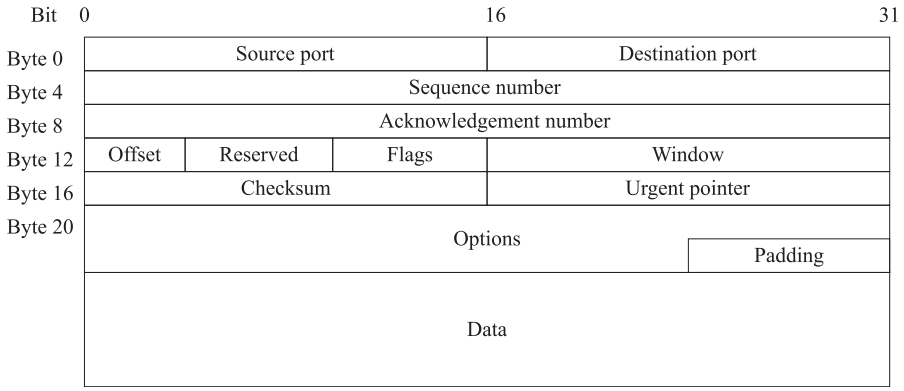
You can use these values for your own network. It is only important that each station is actually assigned an individual IP address which only differs in the last position (1-254). If you use a different network address in addition, the stations cannot normally communicate with one another since they assume that they are in a different network.

DHCP – dynamic IP addresses: Most problems occur in the addresses in IP-based networks when adding, deleting or modifying stations. To reduce the problem of reconfiguration, the protocol DHCP (Dynamic Host Configuration Protocol) has been provided. DHCP assigns dynamic IP addresses from a freely-available pool to a logical station for a certain fixed time. In this manner, DHCP permits a station to move from one subnet to another without being manually configured. Furthermore, only the actually required IP addresses are used. Vacant IP addresses are returned to the freely-available pool. A so-called DHCP server for the address output must be installed in the network to permit functioning of this service. At least one DHCP server is required in the network for administration of the configuration data for a defined IP address range. Only this single and fixed IP address of the DHCP server is known to the connected stations in the network configuration. The individual data terminals with DHCP capability register there during booting, and are assigned their IP address and the associated parameters (for example the subnet mask) by this server. Recent Simatic Ethernet components can handle DHCP.

TCP (Transmission Control Protocol = transport layer)

Data transmission over Ethernet with the IP is a very unreliable method. Data packets can be lost as a result of faults on the transmission medium or through network overloading. For example, they may arrive more than once or in a sequence different from the originally transmitted sequence.

Only provision of the transport layer above the Internet layer guarantees reliable and complete transmission of information between the transmitter and receiver in the correct sequence. TCP was specified in the RFC 793 in 1981 and is a connec-



Source port: Identifies the sending user program with a port number.

Destination port: Identifies the receiving user program with a port number.

Sequence number: TCP considers the data to be transmitted as a numbered byte stream. This byte stream is divided into blocks (TCP segments) during the transmission. The sequence number is the number of the first data byte in the respective segment. Through this, the correct sequence for segments arriving via different connections can be reestablished.

Fig. 2.5 The TCP data packet

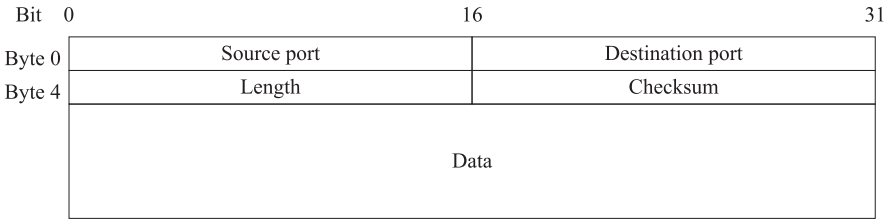
tion-oriented transmission protocol. This means that, when exchanging data between stations, the data of the sender are confirmed by the receiver. For these purposes, mechanisms are added for error checking, flow control and confirmation of transmission/reception. TCP establishes the connection between the communications channel and the host user program in the involved computers via so-called ports. These ports can also be considered as distributors to higher levels via TCP. Depending on which port is specified in the TCP protocol, the TCP packet is delivered by means of the protocol or user program assigned to the respective port. A TCP communications station is addressed using the combination of IP address and port number (example: 192.157.169.10: 80). The combination of IP address and port number is also referred to as socket. A range of port numbers has a fixed assignment, i.e. are assigned to fixed applications (Port 20/21 FTP, 23 TelNet, 25 SMTP (e-mail), 80 HTTP), and are known as so-called “Well Known Ports”. Each TCP packet contains a port number of the transmitter and one of the receiver.

The TCP header is 20 bytes long and is based directly on the IP header. A TCP packet has a structure as in Fig. 2.5. Please refer to the relevant literature for the other fields.

2.10.2 UDP/IP

Of course not all services at the transport level require a secure connection between two communications partners as with TCP. For example, if the network itself is secure enough, as is usually the case with local area networks (LANs), the transport protocol can be configured far more simply. The User Datagram Protocol (UDP) describes a minimalistic transport protocol for this which only provides

fundamental functions for data transport. It was specified in the RFC 768 in 1980. UDP offers a simple *connectionless* service which, compared to IP, only offers additional port numbers and a checksum. UDP can therefore be considered as a lightweight compared to TCP (Fig. 2.6).



Source port:	Source port number is the number of the transmitting protocol port.
Destination port:	Destination port number is the number of the receiving port.
Length:	The length corresponds to the size of the UDP packet in bytes including the UDP header.
Checksum:	The checksum checks the complete packet.

Fig. 2.6 UDP header

As a result of the desired minimalism, UDP does not work with a continuous connection at both ends. Both the establishment and clearance of the connection and also confirmation of the received packets are, for example, omitted.

Only a checksum is provided for checking the data transfer, and even this is optional. All other error handling mechanisms such as those existing with TCP are not present here. Therefore loss, duplication or errors in the sequence are possible for the data to be transmitted. All these possible errors must then be handled at the application level. The performance therefore largely depends on the application programming. Despite this deficiency, UDP has the advantage of speed. Compared to TCP, UDP exhibits approximately three times the transmission speed. As a result of its speed, UDP is used with Profinet for exception-based data exchange and system startup.

Sockets: At the beginning of the eighties, the so-called socket interface for communication between processes was introduced as BSD in UNIX systems. A socket is the name for the logical end points of a connection with TCP or UDP protocol. A socket consists of a network number, a computer number and a port number. Applications distributed over the network can be programmed via this socket interface. It provides a library with functions. A number of important socket primitives or system calls are:

- Generation of a socket: socket() for opening connection-oriented communication on the Internet
- Establishment of connection: bind() to connect the socket to the local end point address

- Communication: send = send() and receive = receive for writing to or reading from the virtual channel
- Clearance of connection: close()

Profinet also applies the socket interface such that user programs can open TCP connections in order to send and receive data.

2.10.3 Further Protocols of the Network Layer

The protocols of the network layer, i.e. the Address Resolution Protocol (ARP) and the Internet Control Message Protocol (ICMP), are essential components when applying TCP/IP. These are therefore briefly described below.

Address Resolution Protocol (ARP)

ARP is an Internet protocol that links an IP address to a physical address (normally Ethernet MAC address). This is important for transferring the IP packet to the corresponding LAN technology such as Ethernet, since stations are addressed using the MAC address at this level. ARP works fully automatically, and need not normally be explicitly used since the system manages this function itself. Each station with an IP address in the network manages a table for address resolution for this purpose. Already assigned pairs of IP and MAC addresses are implicitly stored in this table, the so-called ARP cache. This address table is not manually administered or created. The ARP protocol carries out the required entries and updating itself without the user noticing it.

How does the search for a MAC address associated with a defined IP address function? A station which does not know the hardware address of the destination station sends an ARP request as a broadcast datagram (i.e. to all stations of the network). This contains the Internet and hardware addresses of the source and the IP address of the destination station. All stations of the network now examine whether they are the destination of the request. Only the destination station replies to the packet with an ARP confirmation which it directly sends to the requesting station. This contains its hardware address which the requesting station can use to transmit the user data. This assignment is then entered in the ARP table. The complete procedure is invisible to the user. In order to be able to react to dynamic situations such as replacement of a network card and the associated MAC address, a timer controls deletion of the entries in the table.

Reverse Address Resolution Protocol (RARP)

The reverse case to ARP is also possible, where an unknown IP address is requested for a known MAC address. This occurs in so-called diskless computers which cannot save their own IP address. They must make contact with a computer which administers their IP address. Through a broadcast, the RARP determines the server which recognizes the source from the received MAC address and returns a reply package with the IP address.

Internet Control Message Protocol (ICMP)

The ICMP is used for transmitting status information and error messages between IP network nodes. The ICMP provides the network commissioning and servicing engineers with two important diagnostics tools:

- **ICMP "Echo Request" – Ping:** The most important type of ICMP packet is the Echo Request. The receiver of this packet must send it back, thus making it an Echo Reply. This mechanism permits checking of the availability of a certain address. This command provides users with a simple diagnostics aid. Depending on the replies or the absence of replies, it is possible to interpret whether a station is at all physically available, and within what time.
- **Traceroute:** The Traceroute command is usually referred to on Windows systems as trace. The IP header contains a TTL block (Time To Live) which is decremented by one by each intermediate station on the path of the packet through the network. The packet is rejected when it reaches a value of zero, and the source is informed by means of a "Time Exceeded" ICMP packet. This response is used by the Traceroute mechanism: a station which wishes to trace the route to a destination station sends data packets to a destination host, the first with a TTL of 1. This is therefore already rejected by the first intermediate station, and a Time Exceeded ICMP packet is returned. The IP address of this station is displayed, and a packet with a TTL of 2 is then sent. This is rejected by the second station, and so on. The TTL is large enough at some time or other, and the packet reaches its destination. The Traceroute command is then terminated. The result is a list of intermediate stations from the source to the destination. Note that routers always return the IP address of that interface via which the ICMP packet is sent to the requesting host.

3 Real-time Communication

Use of Ethernet technology with automation systems in the field must not only support the properties required for automation networks in the field, namely:

- efficient and high-frequency exchange of very small data quantities,
- real-time communication,
- synchronized actions between stations and
- design appropriate for fieldbus (e.g. line structures).

Even more is necessary: these properties of current fieldbus systems must be enhanced by the specific properties of 100-Mb Ethernet networks concerning bandwidth and range (Fig. 3.1).

Although the bandwidth of the 100-Mb Ethernet is an order of magnitude greater than Profibus, the actually usable bandwidth nevertheless largely depends on factors such as:

- type and manner of local implementation on the data terminals,
- network topology (line, star, etc.) and
- properties of the network components used, for example the switching procedure (cut-through or store&forward) or the priority assignment of protocols.

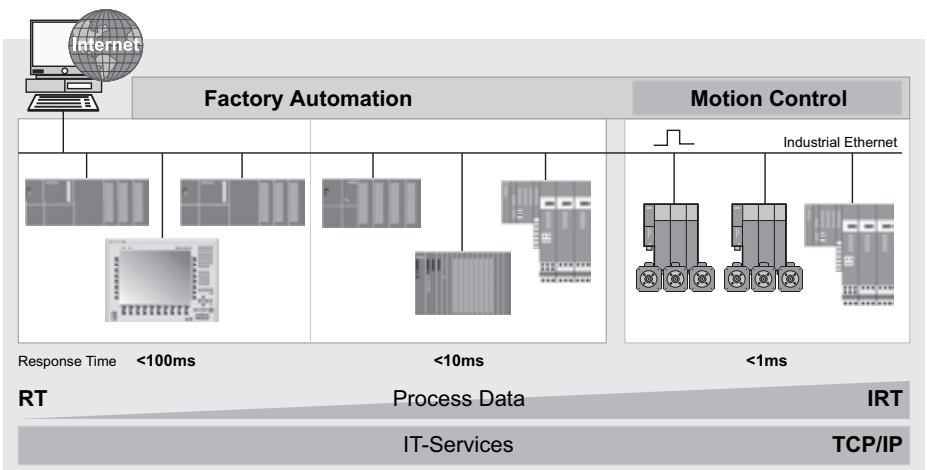


Fig. 3.1 The real-time concept with Profinet communication

To ensure that the regular Ethernet communications capability is completely retained and that the software based on it remains usable, this also particularly means that:

- the current Ethernet standard can be migrated into Ethernet with real-time capability,
- it must still be possible to use standard components such as switches, Ethernet controllers and protocol stacks, and
- the possibility exists for achieving a higher data transmission quality through expansion of the network component functions.

3.1 Requirements of Ethernet with Real-time Capability

A system can be considered as having a real-time capability with respect to an application if all time requirements of the application are fulfilled by it. A real-time response requires that a system has a clearly defined time response which is guaranteed under all operating conditions. A system must fulfill four criteria to this end:

- Runtime, cycle time, response time: a defined upper limit applies to these parameters which must never be exceeded.
- Jitter (cycle deviations): as the requirements for speed and precision increase, the time variation and the deviation from the setpoint must be smaller.
- Synchronism: this determines the simultaneity of actions. The highest possible accuracy is also required here.
- Throughput: it must be guaranteed that the defined data quantity can be transmitted within a time unit.

Transferred to the requirements of Ethernet for real-time capability, this must fulfill the following prerequisites:

- Segmenting/separation: using a specially designed network component, e.g. a router, it must be guaranteed that interfering traffic is kept away from the real-time network, since e.g. overload situations certainly result in a response which is not deterministic.
- Time slot procedure: systems with real-time capability are usually defined by sequences which occur at exact cyclic intervals. This can be achieved using a transmission with the time slot procedure. This guarantees that all required data are always transmitted at the right time.
- Time synchronization: many processes have to be triggered simultaneously in order to achieve the required synchronism. This means that all local clocks must operate synchronously within a defined tolerance.

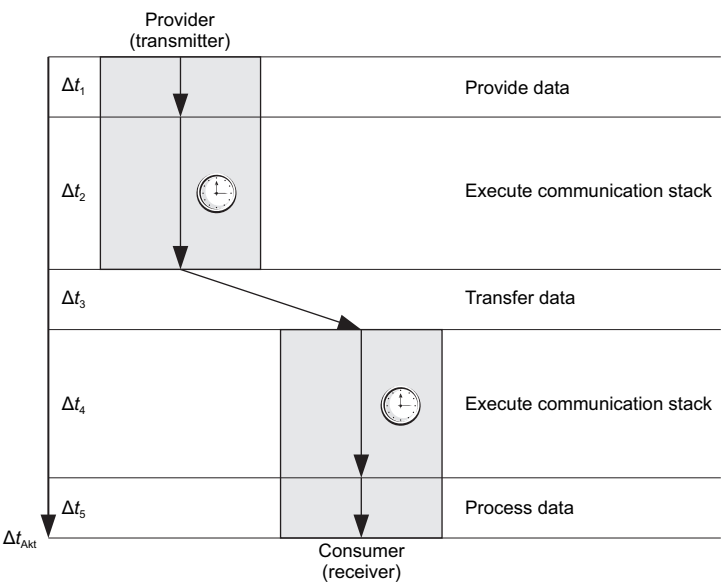
3.2 Real-time@Profinet

Real-time means that a system processes external events within a defined time. If the reaction of a system is predictable, one speaks of a deterministic system. The general requirements for real-time (RT) communication are therefore:

- deterministic response and
- defined response times, usually up to ð 5þms for standard applications.

Since the main task of the processor is execution of the user program and not the handling of data exchange, real-time communication over Ethernet must only result in insignificant loading of the processor. At the same time, the send cycle, i.e. the duration of a data transmission from the application of a device A to the application of a device B, should be as small as possible. Fig. 3.2 shows which factors are responsible for the send cycle.

One possibility for implementing real-time communication is the use of standard communication protocols such as TCP/IP or UDP/IP. However, their application is also associated with disadvantages: the frame overload increases the frame length, and therefore results in an increase in the transmission time on the line (Fig. 3.3). Furthermore, the corresponding communication stacks require a comparatively



Δt_1: Provision of variables in the application of the transmitter (provider)
Δt_2: Execution of communication stack, and sending of variables
Δt_3: Transmission on the line (including delay in the network components)
Δt_4: Receipt of variables in the partner device, and execution of communication stack
Δt_5: Provision of variables in the application of the receiver (consumer)

Fig. 3.2 Composition of the send cycle

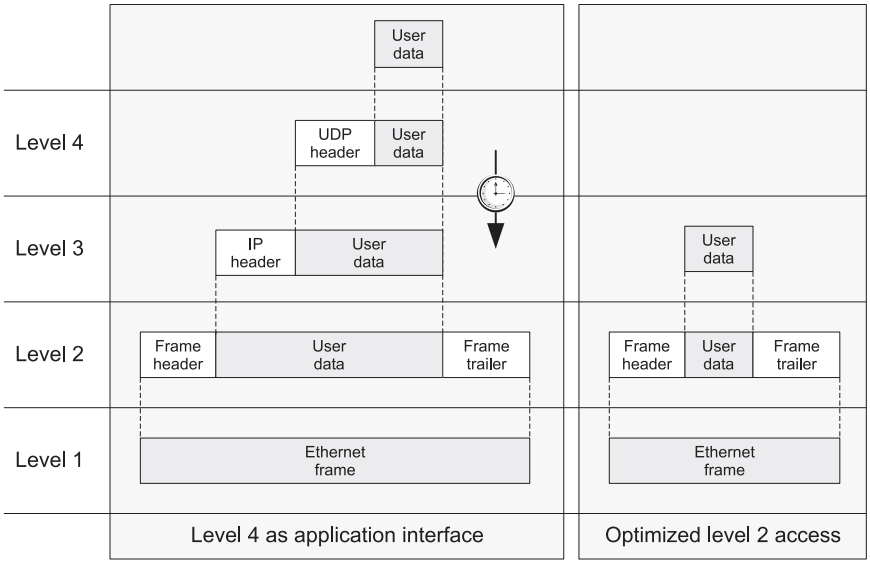


Fig. 3.3 Origin of overhead when "packing" process data

long computation time in the processor and therefore result in an increase in the send cycles.

Considerable improvements in the updating rate with an associated reduction in processor loading can be achieved through optimization of the communication stacks in the provider and consumer. However, optimization of the runtime of a communication stack also means that the resulting TCP/IP communication stack is no longer a standard product but a proprietary implementation. The same applies to the use of UDP/IP implementations.

Whereas level 3 and 4 protocols are only partially suitable for cyclic data exchange, it is recommendable to use an optimized layer 2 protocol conforming to IEEE 802.3 for this application. The only limitation: routing of user data is not possible since the level 3 protocol is missing.

Profinet uses an optimized communications channel for real-time communication, and thus guarantees the transmission of time-critical data between different stations over a network within a defined interval.

The real-time channel can be implemented on standard Ethernet controllers using a software solution executed on them, or in the form of special hardware. It is based on level 2 of the ISO/OSI reference model (see Table 3.1). Addressing of data packets is not carried out here using an IP address, but using the MAC addresses of the receiving devices. Real time permits exact determination (prediction) of the time of transmission, and guarantees that communication using other standard protocols such as TCP/IP can take place simultaneously in the same network without problem.

Table 3.1 Profinet communication protocols in the ISO/OSI reference model

Layer	Task	Standard communication	Real-time communication
7	Processing	ORPC/RPC	–
6	Presentation	–	–
5	Communication	Socket interface	–
4	Transport	TCP UDP	Real-time protocol (RTC 1) (RT over UDP)
3	Network	IP	IP (RT over UDP)
2	Data link	Ethernet drive	Real-time protocol (RTC 1-3)
1	Bit transmission	Ethernet network adapter	Ethernet network adapter

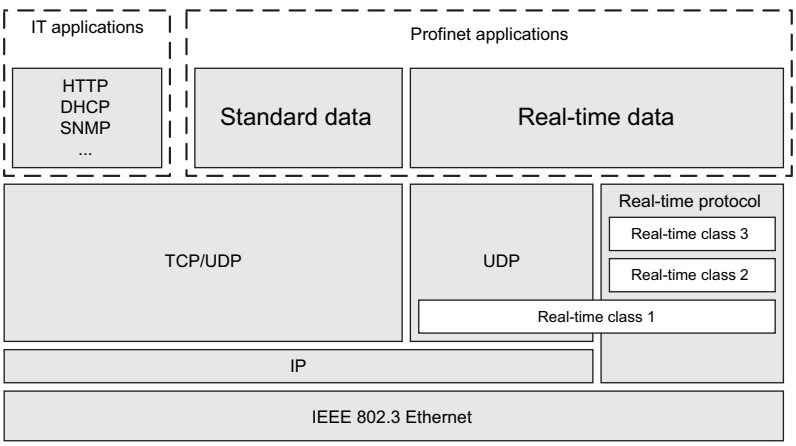


Fig. 3.4 Profinet communication protocols

The real-time protocol permits high-performance transmission of cyclic data and event-controlled messages (alarms). It is divided into three classes (RTC: real-time classes) (see Fig. 3.4):

- Real-time class 1 (RTC 1): suitable for transmission of cyclic and acyclic data. No special demands are placed on the switches used. Data transmission can be carried out using the real-time protocol or, with segmented networks, using UDP (RT over UDP).
- Real-time class 2 (RTC 2): suitable for transmission of interrupts and cyclic data. Special switches must be used in this case. However, it is not yet necessary to plan communication in the sense of configuring.
- Real-time class 3 (RTC 3): suitable for transmission of cyclic data with motion control applications. Special switches must also be used with RTC 3, and explicit communication planning must be carried out in advance.

Table 3.2 Profinet data channels

Standard channel	Standard data: – Device parameterization – Reading of diagnostics data – Loading of interconnections – Acyclic data exchange – Negotiation of communication channel for transmission of user data
Real-time channel	Real-time data: – Real-time classes 1 and 2 (RTC 1 and 2): High-performance transmission of user data Cyclic data exchange (RTC: Real-time cyclic) Event-controlled data exchange (RTA: Real-time acyclic) – Real-time class 3 (RTC 3): High-performance transmission Isochronous data Jitter < 1 µsec

Data whose transmission need not satisfy the real-time requirements, so-called non-real-time data (NRT), are exchanged on the standard channel (see Table 3.2).

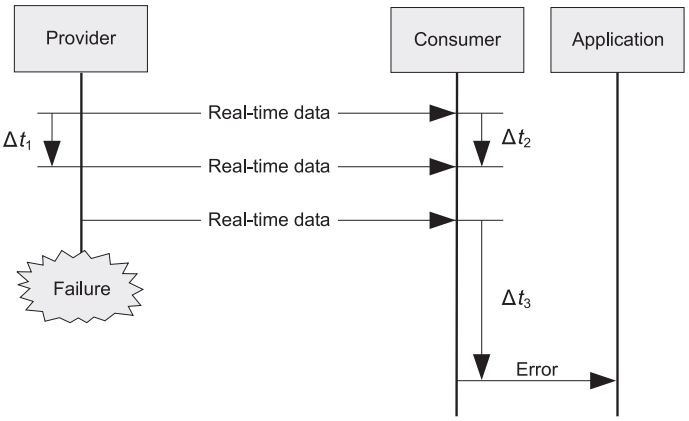
3.3 Real-time Communication

Real-time data transmission is carried out by Profinet real time according to a provider/consumer model. A consumer (receiver) corresponds to a data sink. Its pendant is the provider (transmitter). This corresponds to a data source. Cyclic data such as process values are transmitted at fixed intervals from the provider to the consumer unprotected and without acknowledgment.

Profinet devices can work simultaneously as consumers and providers according to the principle of cyclic exchange of user data (Fig. 3.5).

The following applies to execution of communication between consumer and provider:

- The cyclic exchange of data is carried out connection-oriented. Establishment and clearance of the connection are carried out using a higher-level protocol.
- The provider does not receive an explicit feedback (acknowledgment) on whether the consumer has received a sent data packet. in particular, it does not receive a corresponding. In order to send this information from the consumer to the provider (return channel), a further connection with reversed functions is required.
- The consumer monitors data receipt by means of a monitoring interval Δt_3. It usually applies that $\Delta t_3 = n \cdot \Delta t_2$.
- Only data packets whose length together with all protocol headers does not exceed the total length of an Ethernet packet can be transferred over the user in-



Δt_1: Updating interval (Profinet CBA: quality of service)
Δt_2: Provider control interval
Δt_3: Monitoring interval

Fig. 3.5 Principle of cyclic exchange of user data

terface between consumer and provider. The real-time protocol does not support segmenting and reassembling.

- The user interfaces for the data operate in buffered mode at the provider and consumer. If the updating rate of the provider application is greater than the updating interval Δt_1, not all values (statuses) written by the provider application into the transmitter buffer are sent to the consumer. If the updating rate at the consumer is smaller than the updating interval, the values are overwritten each time a real-time frame is received.
- An updating interval Δt_1 is specified for each provider. This interval must not be shorter, but can be exceeded by a value which has to be defined.
- A provider control interval Δt_2 is defined for each consumer. This interval may correspond, for example, to the updating interval Δt_1. The consumer monitors the provider for regular transmission of the previously defined data.
- A consumer uses an internal timer set to the value Δt_2 to monitor the send cycle of the provider.

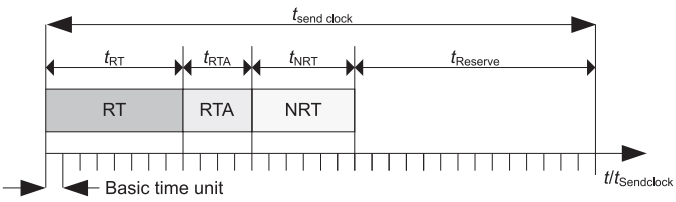
3.3.1 Send Clock Time and Bandwidth

The send clock time is the interval at which cyclic data are sent within an IO data CR. It is defined device-specific as an integral multiple of the basic time unit of 31.25 µs. The send clock time is usually defined during configuration, and therefore by the user.

Send clock time = Send clock factor · 31.25 µs

The send clock factor is between 1 and 128. A value of 32 corresponds to a send clock time of 1 ms.

The interval of the send clock time is divided into intervals for transmission of real-time data and acyclic protocols such as TCP/IP. The ratio of this division results in the respective bandwidth utilization in percent (Fig. 3.6).



Basic time unit:	31.25 µs
Send clock time:	$t_{send\ clock}$ = n · basic time unit; n: send clock factor
RT/RTA	Cyclic/acyclic real-time data $Bandwidth_{RT} = (t_{RT} + t_{RTA}) / t_{send\ clock}$
NRT	Non-real-time data $Bandwidth_{NRT} = t_{NRT} / t_{send\ clock}$

Fig. 3.6 Example of send clock time and division of bandwidth

3.3.2 Phase

Each send clock time represents a phase. Depending on the selected reduction, the cyclic data are distributed between different phases during configuration. Distribution is optimized for each communications station such that the best possible bandwidth is always used for transmission.

3.3.3 Reduction Ratio and Send Cycle

Since high-performance transmission of all data is not usually required, the configured transmission frequencies may differ for the communications stations. However, the “slowest” communications station must not determine the complete data throughput. For this reason, low-performance data are transmitted with reduction based on the send clock time:

Send interval = send clock time · 2^n

2^n: reduction, n: reduction ratio

The send cycle corresponds to the largest reduction of a communications station. In the context of Profinet IO, this specifically means that all I/O data exchanged between IO controller and IO Devices have been updated by the end of the send cycle.

3.3.4 Frame Send Offset

For further optimization, the sequence for assignment of a frame into the phases can be predefined. The frame send offset corresponds to the relative offset of the frame in 250-ns steps, referred to the start of the send clock time in which the frame is transmitted (Fig. 3.7).

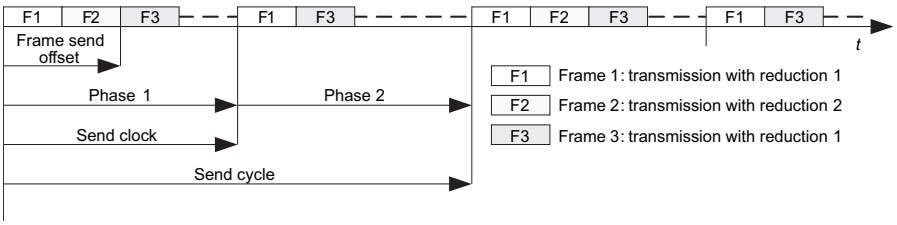


Fig. 3.7 Transmission of frames with Profinet IO

3.3.5 Real-time Connection Management

During the transmission of cyclic data, the connection management is handled by a higher-level protocol, for example TCP/IP.

An initiator, e.g. a Profinet controller, receives the information concerning the connections to be established from an engineering system, or from the saved configuration data following a warm restart. Using this data, the initiator automati-

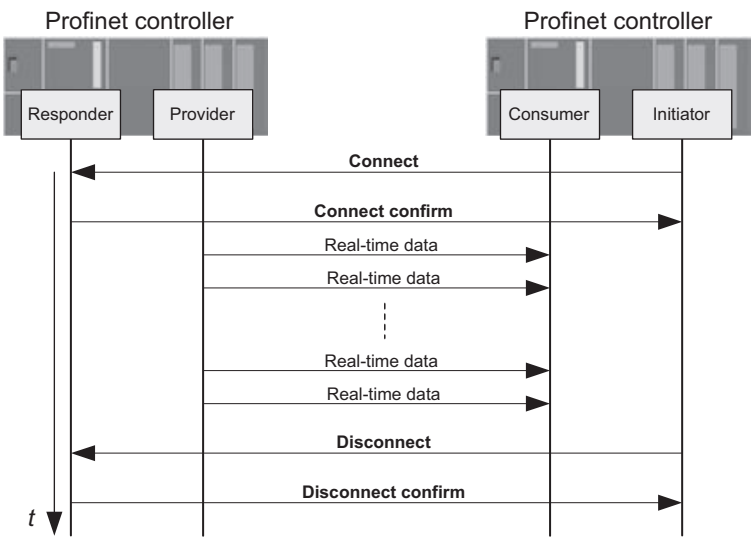


Fig. 3.8 Establishment and clearance of a cyclic connection with Profinet CBA

cally attempts to establish a connection to the responder. Following successful establishment of the connection, the provider commences with transmission of productive data to the consumer.

In the reverse case, the initiator provides the trigger for clearance of the connection. This is the case, for example, if a connection has been deleted by the engineering system. The initiator can be combined with both the provider and the consumer in one device.

Monitoring of the circuit is carried out by the data security properties of the real-time protocol and the higher-level protocols used as well as special monitoring mechanisms in the consumer and provider.

Fig. 3.8 shows the basic sequence for establishment and clearance of a connection with Profinet CBA.

3.4 Isochronous Real-time Communication

For high-performance motion control applications, Profinet with isochronous real-time (IRT) is a solution tailored to the most demanding real-time requirements.

Modern servo engineering allows the mechanical coupling of drive trains via a line shaft to be replaced by an electronic coupling. This electronic coupling is provided by means of the communication system. This system must satisfy the following requirements specific to motion control in addition to guaranteeing determinism:

- Isochronous operation of the communication system
- Cycle times equal to those of the drive controllers
- Direct data exchange between synchronously coupled axes.

With drive engineering, isochronous communication is the basis for drive synchronization. Not only is the frame transfer on the network implemented in an equidistant time frame, it is more important that the control algorithms in the drive are synchronized with the host motion controller.

It is necessary for typical drive applications that the maximum jitter is 1 µs. This is necessary in order to keep the control loops and the actual-value recording strictly synchronous, thus guaranteeing the control quality.

For performance reasons, electrically coupled axes must also directly exchange setpoints between the drives without a diversion through a motion controller. A typical application is the speed synchronism of several drives.

Transmission of the speed setpoints is carried out synchronous to the clock of the speed controller in the drives. The cycle time required is therefore defined by the control clock of the speed controllers, and is usually far shorter than required for typical I/O data transfer.

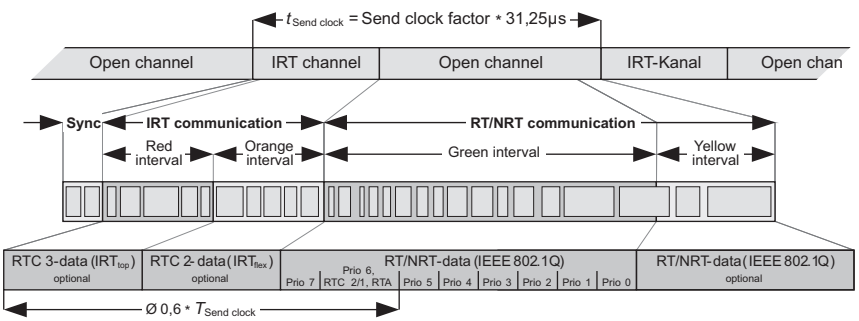
3.4.1 Isochronous Real-time Technology

The IRT technology works with hardware support in the form of a special communications ASIC. IRT permits communication with real-time capability under all conditions, i.e. even with:

- any load or overload situations in communication which is otherwise TCP/IP and
- any network topologies, i.e. also with many switches connected in series (linear topology).

This is achieved using a time-division multiplex procedure. A transmission cycle consists of intervals whose beginning is exactly monitored by the ASIC. Data are exchanged between an IRT channel and an open channel within this interval (Fig. 3.9).

Whereas the IRT channel is reserved for the transmission of isochronous, cyclic real-time frames, the transmission of real-time and non-real-time data (NRT data) is carried out in the open channel. For example, data exchange takes place here via TCP/IP (FTP, HTTP etc.).



Red interval: Optional interval for transmission of the IRT frames (RTC 3).
The size of the red interval results from the communications planning of the IRT-based application. Also considered are the number of communications stations, the cyclic data quantity, and the network topology.
NRT frames which arrive at a switch during the red interval are stored temporarily until the beginning of the green interval.

Orange interval: Optional interval for transmission of the IRT frames (RTC 2).
The interval is available for flexible extension of the IRT-based application by further communications stations. The size results from the number of stations and their cyclic data quantity.
NRT frames which arrive at a switch during the orange interval are stored temporarily until the beginning of the green interval.

Green interval: Interval for the transmission of RT frames (RTC 1 and RTC 2) and NRT frames with priority assignment according to IEEE 802.3Q.
The transmission duration of an NRT frame may extend into the yellow interval.
IRT frames which arrive at a switch during the green interval are rejected.
The total of the red and orange intervals as well as the period up to transmission of the IEEE 802.3Q priority 6 data should not exceed 60% of the send clock time on average.

Yellow interval: Optional interval during which only such NRT frames are sent whose transmission has actually been completed by the end of a transmission cycle. The yellow interval is only present in association with a red/orange interval.
The yellow interval must be large enough such that at least one Ethernet frame of maximum length can be transmitted completely.

Fig. 3.9 Example of division of transmission cycle into an IRT channel and an open channel

Send Clock Time and Phase

A send cycle can be divided into several intervals (phases). The duration of each phase is always the same over one send cycle, and corresponds to the send clock time. However, division of the intervals within the phases is flexible.

The reduction ratio specifies after how many send clock times a phase is repeated (Fig. 3.10). At least one NRT phase must be present within a send cycle.

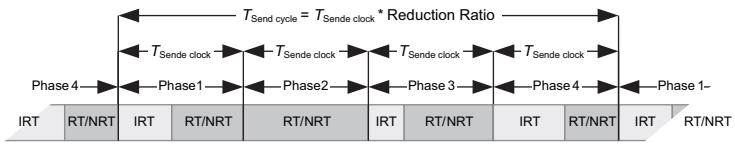


Fig. 3.10 Example of division of the IRT send cycle into several phases

The send clock time is calculated as with RT communication as:

Send clock time = Send clock factor · 31.25 µs

The send clock factor has different minimum values depending on the composition of a phase (Table 3.3).

Table 3.3 Values of the send clock factor with IRT

Interval	Min. send clock factor	Send clock factor
IRT	1	31.25 µs
NRT	5	125 µs
IRT + NRT	6	156.25 µs

3.4.2 Configuration of IRT Applications

IRT as a transmission concept necessitates explicit planning of communication. Planning of IRT communication is an optimization task based on a planning algorithm. This algorithm requires the following main input parameters:

- The network topology
- The performance data of communication nodes present in the transmission path
- Source and destination nodes
- The data quantity to be transmitted
- The properties of the connection path (redundant transmission etc.)
- The configuration of the response for time synchronization (primary/secondary clock master or clock slave).

Configuration of the topology information is omitted for IRT applications. Once the corresponding automation plant has been assembled, the devices participating in the IRT communication collect information on the respective physical neighbors during startup by means of the LLDP (Link Layer Discovery Protocol). This topology information can be downloaded to the engineering tool and processed further. The offline configuration of the automation plant which is usually required is no longer necessary.

3.5 Time Synchronization

Wherever network synchronization is required, Profinet uses an automatic function which exactly records all time parameters of the transmission link: the Precision Transparent Clock Protocol (PTCP) in accordance with IEC 61158. The establishment of a synchronous network is one of the basic functionalities of the Profinet ASIC (Application Specific Integrated Circuit).

PTCP is similar to the Precision Time Protocol (PTP) specified by IEEE 1588, but is located in layer 2 of the OSI reference model and therefore not capable of routing. The main difference between PTCP and IEEE 1588 is the application of so-called transparent clocks which directly pass on the synchronization frames of the clock master to the clock slave. The cascading effects which inevitably occur during synchronization with boundary clocks disappear almost completely when using transparent clocks. The synchronization accuracy is therefore significantly better than with the procedure used in IEEE 1588 (Fig. 3.11).

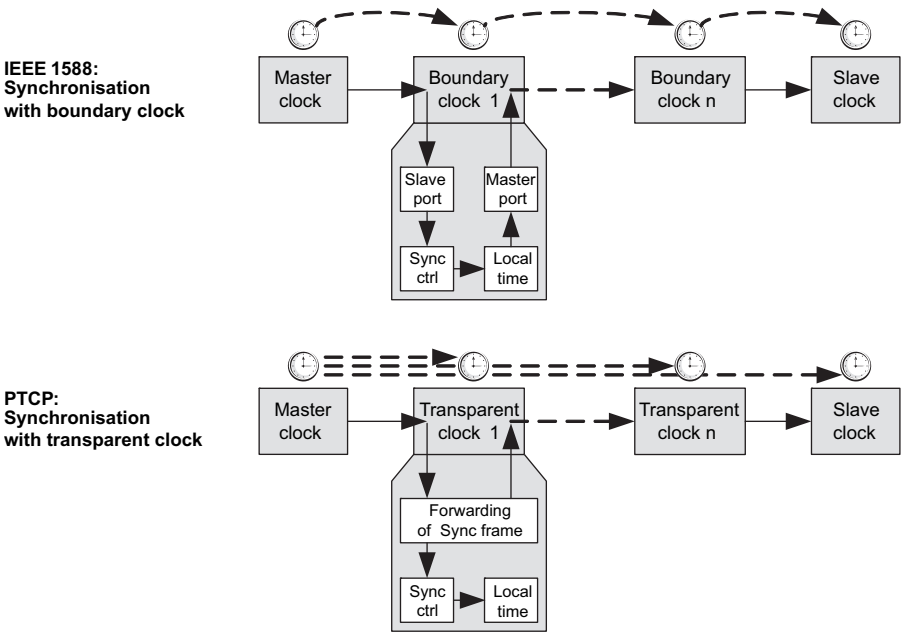


Fig. 3.11 Comparison of time synchronization with IEEE 1588 and PTCP

PTCP serves for time synchronization in the microsecond and submicrosecond range between a PTCP master (clock master) and the PTCP slaves (clock slaves) of the same PTCP subdomain. A PTCP subdomain comprises all communication participants which are synchronized with the same clock in a subnet. PTCP supports the best master model with up to 32 different clocks.

The most important properties of the PTCP are:

- Synchronism in the microsecond and submicrosecond range
- Low use of resources
- No special requirements for memory and CPU performance of the network components
- Minimum use of bandwidth
- Low administration requirements.

In the context of IRT, a PTCP subdomain corresponds to an IRT domain which in turn can comprise several IO Systems.

3.5.1 Time Synchronization Sequence

The basic function is that the network node with the most exact clock (master clock) synchronizes the local clocks of the other network nodes (slave clocks). The functionality of the clock master can, if supported by the device, be carried out by an IO controller or an IO Device. The synchronization is carried out cyclically by exchanging a sequence of synchronization frames between two network nodes (Fig. 3.12).

All frames in a sequence have the same sequence number. This is incremented by each new sequence. The synchronization procedure is divided into two phases.

- Measurement of the delay on the transmission link between two ports communicating with each other
- Synchronization of the clocks of the clock master and clock slaves.

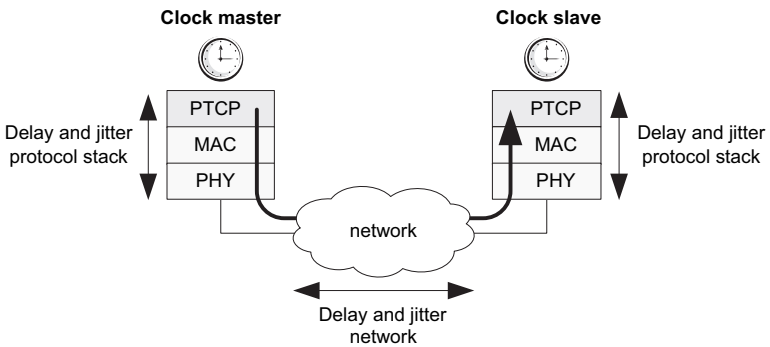


Fig. 3.12 Simple configuration with clock master and slave clock

Delay measurement

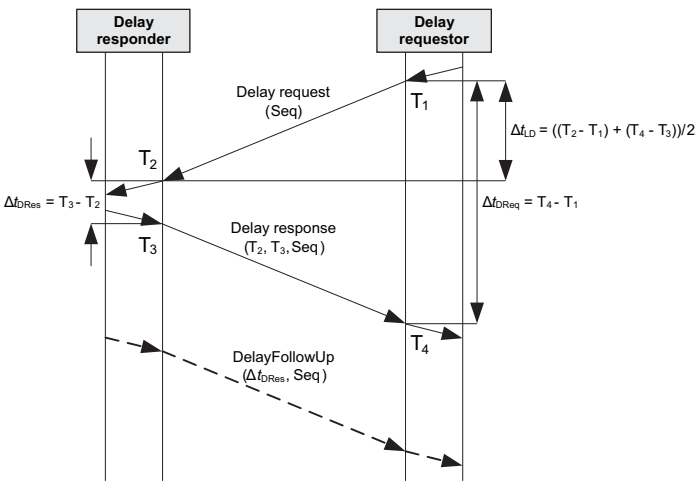
The first phase of the synchronization procedure is measurement of the delay between the delay requester and the delay responder.

The delay consists of three periods:

- Local delays in the delay requester
- Local delays in the delay responder
- The delay of a frame on the transmission path.

Four time stamps are necessary to determine the delay. The measurement (see Fig. 3.13) commences with transmission of a delay request from the delay requester to the delay responder. The exact transmission time of the frame is stored in the intermediate memory by the delay requester. The delay responder signals receipt of the delay request by means of a delay response. Transmitted in this are the receive time of the delay request as well as the send time of the delay response. Following receipt of the delay response, the delay requester then possesses all four time stamps and can calculate the transmission time.

If the delay responder does not possess the functionality for entering the receive time of the delay request and the send time of the delay response into the delay response frame, it transmits its local delay time $\acute{y}t_{\mathrm{DRes}}$ in a delay follow-up response.



Seq: Sequence number ($Seq_{\mathrm{Req(new)}} = Seq_{\mathrm{Req(old)}} + 1$)
Δt_{DReq}: Transmission time of delay request and delay response sequence
Δt_{DRes}: Local delay time of delay responder
Δt_{LD}: Delay time of cable between delay requester and responder (line delay)
Δt_{D}: Delay time of complete transmission link

Fig. 3.13 Example: measurement of delay

Synchronization

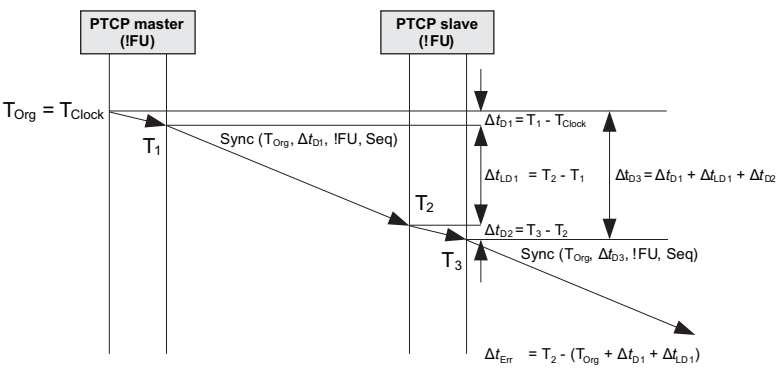
Time synchronization within a PTCP subdomain begins with the clock master sending a synchronization frame to defined multicast addresses. The following are transmitted in the process:

- Value of the master clock
- Local delay time of the clock master.

Using the information transmitted in this manner, the clock slaves synchronize their local clocks.

However, each PTCP network node in the transmission link between clock master and clock slave generates an additional runtime delay. This runtime delay must be taken into consideration by correction of the delay time transmitted in the synchronization frame. The correction is carried out by the PTCP network node itself before the frame is passed on. PTCP network nodes are called !FU nodes (non-FU nodes) if they:

- Carry out delay time measurements
- Carry out measurements of the local delay time
- Carry out correction of the delays transmitted in a PTCP frame and
- Provide mechanisms for the use of PTCP with media redundancy.



Δt_{LD1}: Delay time of cable between PTCP master and slave (line delay)
Δt_{D1}: Local delay time of PTCP master
Δt_{D2}: Local delay time of PTCP slave (internal bridging delay)
Δt_{D3}: Delay time of previous transmission link
Δt_{Err}: Time difference between the value of the PTCP master clock and the actual starting time of the synchronization transmission

Fig. 3.14 Example: synchronization without follow up

Since they are not visible for a clock slave in the transmission path to the clock master, they are referred to as transparent clocks. Both the clock master and clock slaves can work as transparent clocks.

If the transparent clock functionality is not supported (FU nodes), or if the modification of frames in the transmission path is not permissible for implementation reasons, transmission of the additive local delays of a PTCP network node is carried out by a follow up frame (Fig. 3.14).

Accumulation of delay times on a transmission link

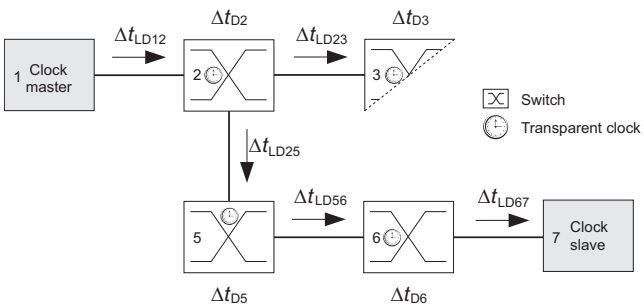
A prerequisite for exact synchronization is determination of the exact delay times. These times result through delays in the data transmission on the cable and in the devices (see Table 3.4).

A PTCP network node is responsible for only passing on those synchronization frames in which all previous delay times have been recorded. Accumulation of the delay times is carried out in two steps (see also Fig. 3.15):

- Adding of line delay to predecessor when receiving
- Generation of difference between transmitter and receiver time before forwarding

Table 3.4 Typical delay times in a transmission link

Component	Delay
Cable	5 ns/m
Transmitter/receiver	100-300 ns
Switch	10 µs



Δt_{LDxy}: Delay time of cable (line delay)
Δt_{Dz}: Local delay time of device (internal bridging delay)

Fig. 3.15 Delay times in a transmission link

Recognition of synchronization errors

If the time synchronization has been carried out completely once, a renewed offset measurement can determine a possible deviation between the slave clock and the master clock. Such a deviation can occur as a result of:

- Errors in the transmission equipment when entering the time stamp of the transmitter or receiver time (jitter)
- Differences in the crystal frequencies of the master clock and slave clock.

A simple correction possibility is to adjust the slave clock. However, the occurrence of reverse jumps in the time must be avoided in such a case since this may lead to repeated execution of local actions. Special control algorithms which successively eliminate the calculated errors are highly suitable for correction of the time.

3.6 Profinet Protocol Elements

The real-time protocol applies the Ethernet II protocol which is almost exclusively used nowadays for data transmission (Fig. 3.16 and Table 3.5).

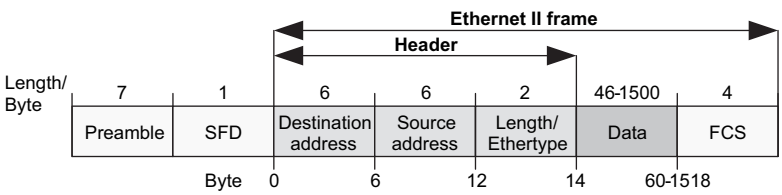


Fig. 3.16 Structure of the Ethernet II frame for Profinet communication

Table 3.5 Protocol elements of an Ethernet II frame for Profinet communication

Protocol element	Meaning
Preamble	Introduction of data packet. Seven bytes comprising an alternating sequence of "1" and "0" for synchronization of the receiver.
SFD	Start of frame delimiter (10101011). The double "1" at the end of the byte identifies the beginning of the destination address of the data packet.
Destination Address	Unicast: Destination address of data packet. The first three of the six bytes usually identify the vendor, the others are assigned by the vendor as desired. Siemens: "08.00.06..." Multicast: DCP (Discovery & Configuration Prot.) 01-0E-CF-00-00-00 MRP (Media Redundancy Protocol) 01-15-4E-00-00-00 - ...FF-FF-FF MRRT (Media Redundancy Real-Time) 01-0E-CF-00-05-00

Table 3.5 Protocol elements of an Ethernet II frame for Profinet communication

Protocol element	Meaning
Destination Address *(continued)*	PTCP: DelayReq/DelayRes/FollowUpRes 01-80-C2-00-00-0E FollowUp: Clock synchronization 01-0E-CF-00-04-20 Time synchronization 01-0E-CF-00-04-21 Synchronization 01-0E-CF-00-04-22 - ...00-04-3F RTA Sync and Announce Clock synchronization 01-0E-CF-00-04-00 Time synchronization 01-0E-CF-00-04-01 Synchronization 01-0E-CF-00-04-02 - ...00-04-1F RTC Sync (clock synchronization) 01-0E-CF-00-01-02 Reserved: 01-0E-CF-00-00-01 - ...00-01-01 01-0E-CF-00-01-03 - ...00-03-FF 01-0E-CF-00-04-40 - ...FF-FF-FF
Source Address	Source or sender address of data packet.
Length/ Ethertype	Length block or type ID of data packet. < 0x0600: IEEE802.3 length block 0x0600: Ethernet II type block 0x0800: IP 0x0806: ARP 0x8100: Tag Control Information; data packets with VLAN-TPID 0x8892: Profinet 0x88E3: MRP 0x88CC: LLDP
Data	User data component within the Ethernet II frame. Ethertype: 0x0800: UDP, RPC, SNMP, ICMP 0x0806: ARP 0x8100: VLAN TPID 0x8892: RTC, RTA, DCP, PTCP, MRRT 0x88E3: MRP 0x88CC: LLDP If the user data length is < 46 bytes, additional padding bytes are added to extend the frame to the minimum length of 64 bytes.
FCS	Frame Check Sequence: 32 Bit checksum. Cyclic Redundancy Check (CRC) for the complete Ethernet frame.

In order to keep the jitter (maximum cycle deviation) during the frame runtime within switches as small as possible the transmission of all cyclic and acyclic real-time services are assigned priorities through application of the VLAN frame format (VLAN tagging). Using the protocol element “User priority”, the switches control the data flow between the devices during runtime. The “User priority” can have values between 0 (lowest priority) and 7 (highest priority). Profinet real-time frames are sent with priority 6 or 7.

In the receiver, the Ethernet controller initially evaluates the 6-byte long destination address. Assignment of the frame to a communications channel is subsequently carried out in the Profinet protocol stack using Ethertype and FrameID (Fig. 3.17 and Table 3.6).

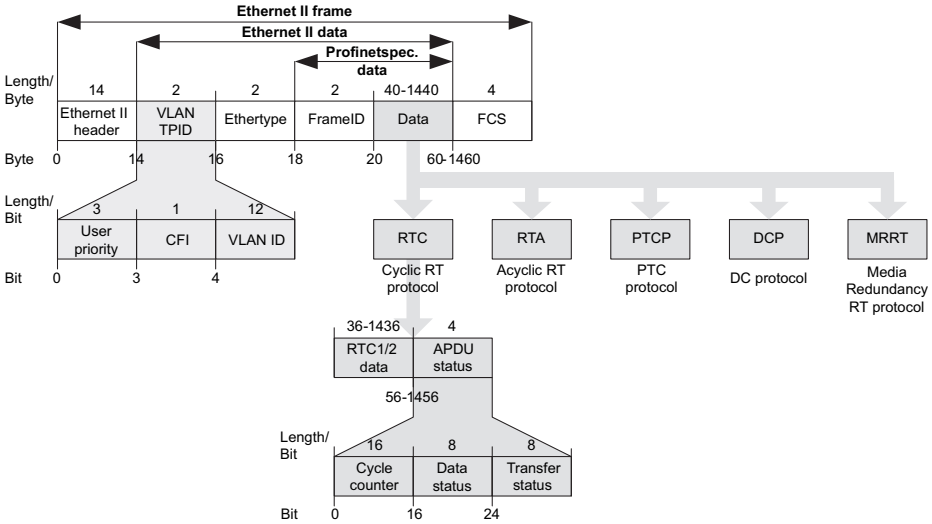


Fig. 3.17 Structure of the data component of an Ethernet II frame with RT communication

Table 3.6
Protocol elements of the data component of an Ethernet II frame with RT communication

Protocol element	Meaning
Ethernet II header	Header of the Ethernet II frame
VLAN TPID	VLAN Tag Protocol Identifier: User Priority: 0x00: IP, DCP 0x01 - 0x04: Reserved 0x05: RTA low-priority or UDP RTA low-priority 0x06: RTC 1/2, UDP RTC (RT over UDP), RTA high-priority or UDP RTA high-priority 0x07: PTCP, MRP, MRRT CFI (Canonical Format Indicator): 0: Ethernet 1: Token Ring VLAN ID: 0x000: Transmission of data with priority 0x001: Standard setting 0x002-0xFFE: For free use 0xFFF: Reserved
Ethertype	Type identification for the network protocol following in the data component: 0x8892: Profinet
FrameID	Identification of frame type: PTCP: 0x0000: RTA Sync without FollowUp (clock and phase synchronization) 0x0001: RTA Sync without FollowUp (time synchronization) 0x0020: RTA Sync with FollowUp (clock and phase synchronization) 0x0021: RTA Sync with FollowUp (time synchronization) 0x0080: RTC Sync (RTC3 synchronization) 0xFF00: Announce (Best Master Algorithm: clock and phase synchronization) 0xFF01: Announce (Best Master Algorithm: time synchronization)

Table 3.6
Protocol elements of the data component of an Ethernet II frame with RT communication

Protocol element	Meaning
FrameID *(continued)*	0xFF20: FollowUp (clock and phase synchronization) 0xFF21: FollowUp (time synchronization) 0xFF40: DelayReq (delay measurement) 0xFF41: DelayResp (delay measurement with FollowUp) 0xFF42: DelayFuResp (delay measurement with FollowUp) 0xFF43: DelayResp (delay measurement without FollowUp) RTC2: 0x8000 – 0xBBFF: Unicast frames 0xBC00 – 0xBFFF: Multicast frames RTC1, UDP RTC: 0xC000 – 0xF7FF: Unicast frames 0xF800 – 0xFBFF: Multicast frames RTA and UDP RTA: 0xFC01: Alarm high 0xFE01: Alarm low DCP: 0xFEFD: GetReq, SetReq, GetResp, SetResp 0xFEFE: IdentifyReq 0xFEFF: IdentifyResp MRRT: 0xFF60: Protocol for smooth activation of media redundancy
Data	RTC, RTA, DCP, PTCP or MRRT data. With RTC1/2: Profinet CBA: Linking data of same QoS value as byte stream Profinet IO: I/O data APDU Status (Application Protocol Data Unit Status): Cycle counter: The counter is incremented by the provider with each send clock. A consumer can detect overtaking processes using the counter value. A bit increment represents a time increment of 31.25 µs in the Big Endian format. Data status: Bit 0: (State): 0: Backup; identification of secondary channel with redundant operation 1: Primary; identification of primary channel with redundant operation Bit 1: 0 Bit 2 (DataValid): 1: Data valid 0: Data invalid Bit 3: Reserved Bit 4 (ProcessState): 0: Process which has generated the data is inactive 1: Process which has generated the data is active Bit 5 (ProblemIndicator): 0: Problem present. Diagnostics was signaled or is ongoing 1: No problem detected Bit 6: 0 Bit 7: 0 Transfer status: Bit 0 - 7: 0
FCS	Frame Check Sequence: 32 Bit checksum. Cyclic redundancy check (CRC) for the complete Ethernet frame.

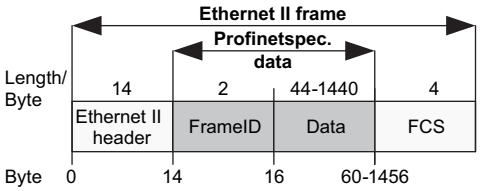


Fig. 3.18 Structure of the data component of an Ethernet II frame with IRT communication

Table 3.7
Protocol elements of the data component of an Ethernet II frame with IRT communication

Protocol element	Meaning
Ethernet II Header	Header of the Ethernet frame
Ethertype	Type of the protocol: 0x8892: Profinet: RTC
FrameID	Identification of frame type: RTC3: 0x0100 – 0x7FFF: Unicast and Multicast frames RTC2: 0x8000 – 0xBBFF: Unicast frames 0xBC00 – 0xBFFF: Multicast frames
Data	RTC2/3 data
FCS	Frame Check Sequence: 32 Bit checksum Cyclic redundancy check (CRC) for the complete Ethernet frame

As a result of the time-based communication, an isochronous real-time frame (Fig. 3.18) has a defined transmission instant. An IRT frame is unambiguously specified by its position within a transmission cycle, the FrameID and the Ethertype 0x8892. In contrast to a real-time frame, it is not necessary to have a VLAN tag for priority assignment (see Table 3.7).

3.7 Profinet ASIC

After the software-based real-time communication with Profinet was made available for factory automation, the next stage was development of the ERTEC 400 and 200 (Enhanced Real Time Ethernet Controller) ASICs by Siemens AG, into a high-performance, equidistant communications solution for use in motion control applications (Table 3.8).

The ERTEC 200 is envisaged for implementation of Profinet devices with RT and IRT functionalities. It possesses an integral ARM946 processor, a 2-port Ethernet switch with integral PHY, and a facility for connecting an external host processor system to a local bus interface.

Table 3.8 Properties of ERTEC 200 and ERTEC 400

Property	ERTEC 200	ERTEC 400
Field of application	Single drives Comparable field devices (IO Devices)	Pure switching functionality 10/100 Mb/s Ethernet. Interface for high-precision drive control. Distributed I/O with real-time Ethernet link. Control systems with own host processor or PC system.
ASIC technology	0.15 µm technology	
Housing	Fine Ball Grid Array (FBGA), 304 pins, pin spacing: 0.8 mm, housing size: 19 mm x 19 mm	
Processor	ARM 946E-S 50/100/150 MHz	
Operating conditions	Temperature range: -40°C to +85°C Power supply for core: 1.5 V ±10% Power supply for I/O: 3.3 V ±10% Power consumption: 0.4 W at 1.5 V, 0.5 W at 3.3 V	
Functionality	IRT communication RT communication NRT communication	PCI interface V2.2, 32 bit, 66 MHz IRT communication RT communication NRT communication
Switch	2-port switch 10/100 Mb/s half/full duplex Autonegotiation Broadcast filter IEEE802.1Q VLAN tagging and identification IEEE802.1D bridge Cut through (IRT) Store and forward	4-port switch 10/100 Mb/s half/full duplex Autonegotiation Broadcast filter IEEE802.1Q VLAN tagging and identification IEEE802.1D bridge Cut through (IRT) Store and forward

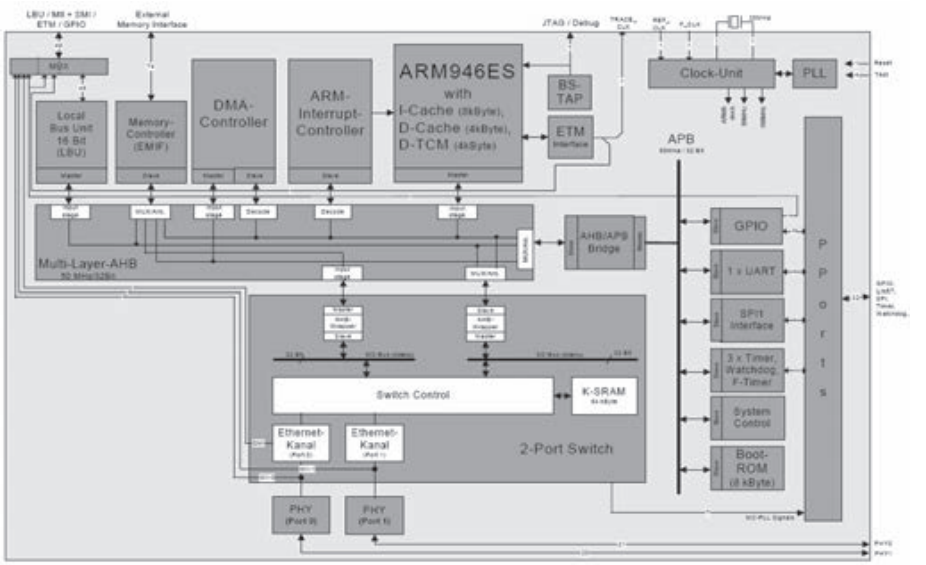
As a result of the integral ARM946 processor, integral 4-port Ethernet switch, and the various possibilities for connecting external host processor systems to a selectable bus system (PCI or LBU), the ERTEC 400 complies with the trend toward open communication to all automation components (Fig. 3.19). For complex applications, the ASIC can also be used to design bumpless, redundant solutions.

The ASICs are designed for use in:

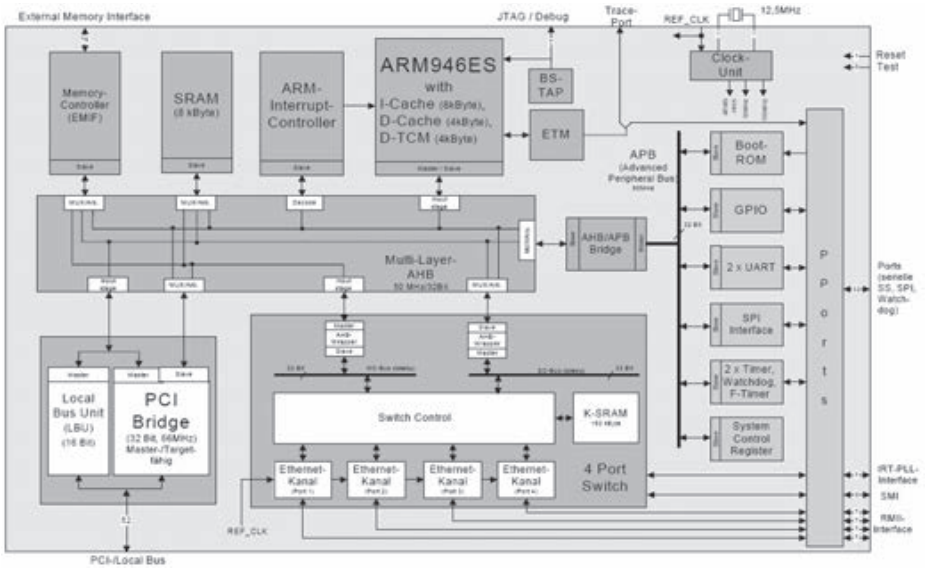
- Interface modules for high-precision drive controls
- Distributed I/O Devices with real-time capability Ethernet interface
- Devices with Profinet RT and IRT functionality.

3.7.1 Application

Based on the IEEE 802 transmission procedure, both ASICs offer real-time communication in that they combine the switching mechanisms “Cut through” and “Store and forward”. Uniform plant and machine solutions are therefore possible compatible with the Ethernet standard.



ERTEC 200



ERTEC 400

Fig. 3.19 Block diagram of ERTEC 200 and 400

The destination systems of both ASICs are PLCs which, on the basis of the Switched Fast Ethernet, increase the previous automation performance and simultaneously offer a link to the IT world. The destination hardware of the ERTEC 400 is in the environment of single controller implementations and multi-processor solutions, whereas the focus of the ERTEC 200 is to be found in the sector of individual drives or field devices. Figs. 3.20 and 3.21 show two application examples.

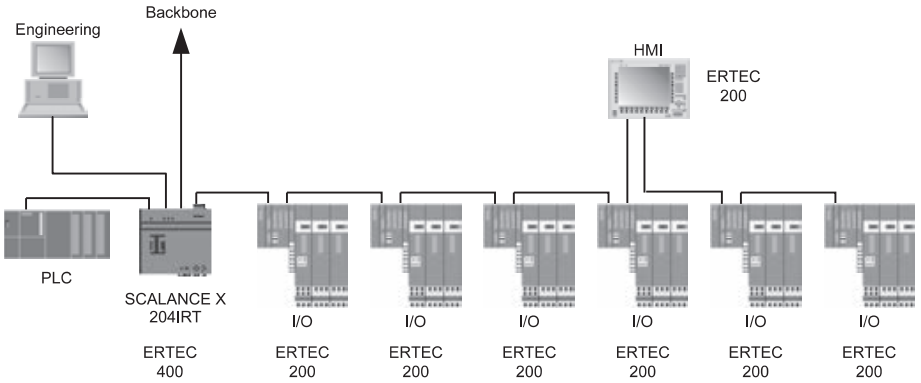


Fig. 3.20 Application example: devices with ERTEC 200/400 in Profinet IO application

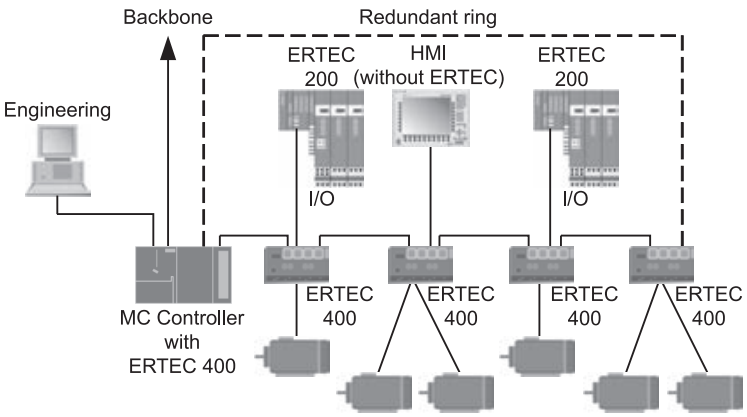


Fig. 3.21 Application example: combination of ERTEC 200/400 with isochronous drives and isochronous I/O

3.7.2 Development of Profinet IO Devices

Using the Development Kit DK-ERTEC 400 PN IO, Siemens provides engineers with a platform for development and testing of the hardware and software functionalities of IO-Devices. The Development Kit comprises the required hardware, drivers, configuration software, demonstration programs and documentation.

The software stack included in the Development Kit supports users in the generation of the complete communications software, and permits low-cost creation of IO Devices. The following functionalities are supported:

- Cyclic data exchange with an IO controller
- Transmission and receipt of process diagnostics interrupts, plug and pull interrupts
- Assignment of IP addresses and device names over Ethernet.

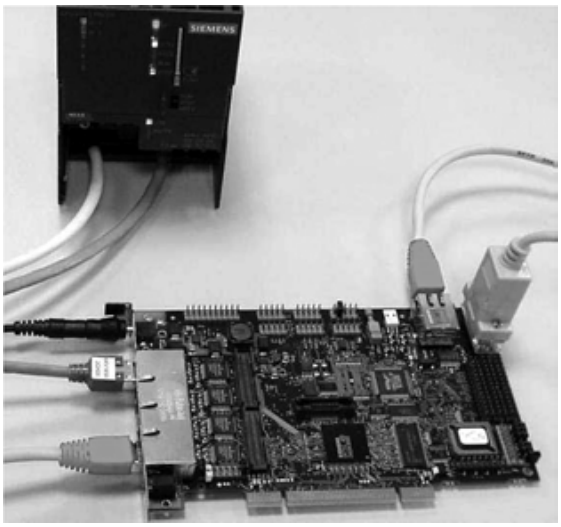


Fig. 3.22
IO Device with ERTEC 400 evaluation board in a minimum configuration

The PC cards and accessories supplied allow fast design of an application with two communication partners and application of the specific automation functions using the demonstration software (Fig. 3.22). The configuration software which is also supplied demonstrates the simple integration into the Siemens automation landscape.

3.8 Protocol Analyzer for Profinet

Wireshark is a software program for analyzing network protocols. It was developed as open source software by a team led by Gerald Combs under the GNU General Public License (GPL). Following protocolling of the data traffic, the tool presents the data in the form of individual packets. The hexadecimal data are decoded and analyzed in a manner which is clearly understandable for users. Protocols can be presented in different colors to facilitate the readability of a protocol recording (Fig. 3.23).

Wireshark is being continuously developed further, and today permits the analysis of more than 700 different protocols, including

- Profinet CBA
- Profinet IO
- Profinet PTCP
- Profinet MRP
- Profinet MRRT
- Profinet RT

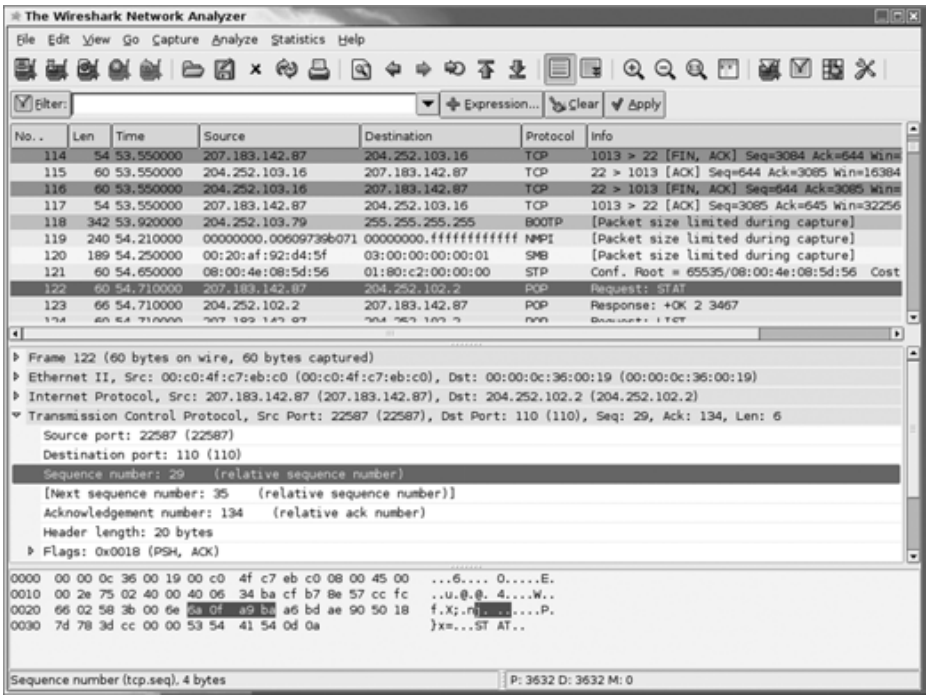


Fig. 3.23 Example of a protocol listing with Wireshark

Wireshark is available for various operating systems and languages, and can be downloaded free of charge at the Internet address www.ethereal.com. A good introduction to working with Ethereal can be found at http://www.wireshark.org.

4 Profinet IO – Distributed I/O

In the context of Profinet, Profinet IO is the communications concept for implementing modular, distributed applications on the Industrial Ethernet. Distributed I/O and field devices are integrated into the Ethernet communication by means of Profinet IO.

In addition to the star, tree and ring network topologies, Profinet IO also supports the line topology characteristic of fieldbuses. This is implemented by a switch functionality integrated in the Profinet IO devices. Existing fieldbus systems such as Profibus DP or Interbus can be integrated into Profinet IO applications using proxies.

Cyclic data exchange between an IO Controller and an IO Device (field device) is based on a provider/consumer model. With up to 1440 bytes per transmission cycle and field device, Profinet IO significantly exceeds the data quantities which could previously be transmitted over fieldbuses. The assignment between provider and consumer is defined during system configuration.

The look & feel of the Profinet IO engineering is oriented according to that of Profibus DP. Programming of the user program for an IO Controller is equivalent to the procedure with Profibus DP. In addition, new blocks and system status lists are available for Profinet IO.

Since only the interface to the transmission medium is replaced, the previously installed Profibus I/O can be used further. The I/O view known from Profibus DP is retained. IO Devices are described unambiguously in GSD files. The user data from the field devices are transmitted cyclically in a real-time channel to the process image of an automation system. Table 4.1 compares various features of Profinet IO and Profibus DP.

4.1 The Profinet IO Concept

Distributed field devices, so-called IO Devices, are assigned during configuration to a programmable controller, the IO Controller. If a IO Controller also has a Profibus interface, it can simultaneously be the DP master of a subordinate Profibus. If it additionally possesses the Profinet CBA functionality, it can be used to implement technological modules within a distributed automation system.

With Profinet IO, the master/slave principle known from Profibus DP has been converted into a provider/consumer model. From the point of view of communication, all Profinet devices have equal privileges on the Ethernet. However, a type is

Table 4.1 Comparison between Profinet IO and Profibus DP

Feature	Profinet IO	Profibus DP
Line-based transmission system	Industrial Ethernet via twisted-pair cable and fiber-optic cable (FOC).	Profibus via copper cable and FOC.
Cable-free transmission system	Radio transmission using Industrial Wireless LAN (IWLAN).	Infrared transmission
Transmission rate	100 Mb/s, full duplex.	Max. 12 Mb/s
Number of stations	Defined by the network class.	Max. 126
Topology	Standard: star and tree Optional: line and ring	Standard: line Optional: tree and ring
Implementation as star	A maximum of one station is connected to each port of a switch.	–
Implementation as tree	The switches are interconnected.	Profibus DP is looped through as standard from station to station.
Implementation as line	Profinet devices are connected together via integral switches.	
Implementation as ring	Closing of the two open ends of a line into a ring by means of a redundancy manager.	
Address assignment	Assignment of IP address to IO Devices and Controller in the Profinet IO engineering tool.	Coding of Profibus address using a DIP switch or configuration in the Profibus DP engineering tool.
	Assignment of IP addresses to IO-Devices by the IO Controller. Assignment of device names to IO-Devices in the Profinet IO engineering tool. Assignment of IP addresses to switches or CPs using the primary setup tool (PST). Configuration of the IP address using integrated Web sites is possible as an option.	
Data exchange	Autonomous data transmission of IO Device following parameterization.	Data transmission by DP slave following request.
Interrupts and diagnostics	Transmission with assigned priorities.	Transmission with equal priorities.
I/O data	Priority adjustable using the updating rate.	Transmission with equal priorities.
Slot model	Slot 0: Profinet IO interface Slot >0: Modules	Slot 0: Profibus DP interface Slot >0: Modules
	Granularity: Slot/subslot/channel	Granularity: Slot/channel
Importing of device data	GSD file in XML format	GSD file in ASCII format
GSD file	Description of several devices of a device family is possible.	Description of one device.
Host device	IO Controller	DP master class 1
	IO Supervisor	DP master class 2
Subordinate device	IO device	DP slave
Network address	IP address	Profibus address

assigned to each device during configuration, and this defines the type and manner of communication according to the provider/consumer model.

4.1.1 Profinet IO Device Classes

Profinet IO differentiates four device classes (see Fig. 4.1 and Table 4.2).

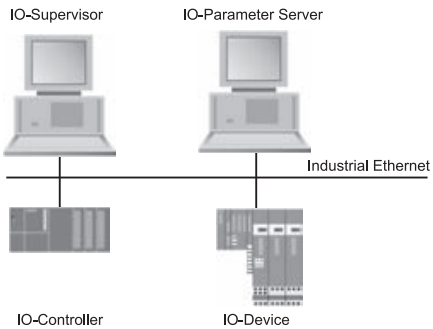


Fig. 4.1
Profinet IO device classes

Table 4.2 Description of device classes

Device class	Function
IO Supervisor:	The IO Supervisor is an engineering device, usually a PC, HMI or programming device (PG), used for commissioning and diagnostics of IO Controllers and IO devices. It is connected during runtime, and usually only temporarily for commissioning or troubleshooting. The IO Supervisor functions correspond to those of a Profibus class 2 master.
IO Controller:	An IO Controller is a programmable controller, typically a PLC, in which an automation routine is executed. A Profinet IO configuration contains at least one IO Controller. The IO Controller functions correspond to those of a Profibus class 1 master.
IO Device:	An IO Device is a distributed field device which exchanges data with one or more IO Controllers using Profinet IO mechanisms. A Profinet IO configuration contains at least one IO-Device. The IO Device functions correspond to those of a Profibus slave.
IO Parameter Server:	An IO Parameter Server is a server station, usually a PC, for loading and saving the configuration data (records) of IO Devices. The IO Parameter Server functions have no corresponding pendant with Profibus.

Data exchange between the devices is carried out over data channels. A separate channel is available for the transmission of real-time data (see Fig. 4.2 and Table 4.3).

4.1.2 Device Model of an IO Device

A uniform device model is specified for structuring an Profinet-IO device, and permits the modeling of modular and compact Profinet-IO devices (Fig. 4.3 and Table 4.4). This module is oriented according to the essential features of Profibus DP.

Definition of submodules is new, and takes into account the flexibility of modern field devices.

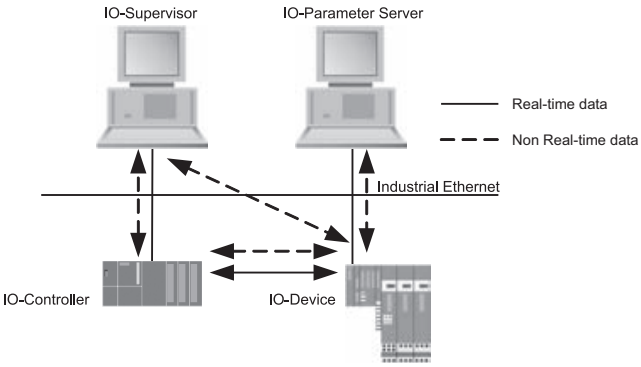


Fig. 4.2
Data flow between Profinet IO devices

Table 4.3 Profinet IO data channels

Channel	Protocol	Service/function
Standard	ARP	Mapping of IP addresses to the respective corresponding MAC addresses ("Ethernet" addresses).
	DCP	Name assignment for Profinet IO devices.
	DHCP	Central and automatic assignment of IP addresses within a network.
	DNS	Administration of logical names in an IP-based network.
	ICMP	Transmission of information and diagnostic error reports.
	IP	Transmission of data in interconnected networks.
	LLDP	Neighbor recognition. Exchange of own MAC address, device name and port number with direct neighbor.
	MRP/MRRT	Protocols for administration of media redundancy in network components.
	PTCP	Time and clock synchronization.
	SNMP	Administration of network nodes (servers, routers, switches, etc.). This includes e.g. the reading of status and statistics information or the detection of communications errors.
	RPC	Calling of device-specific functions. General administration functions.
	UDP	Connectionless data transmission.
Real-Time	Acyclic real-time protocol	Transmission of alarms. General administration functions.
	Cyclic real-time protocol	Cyclic data exchange.

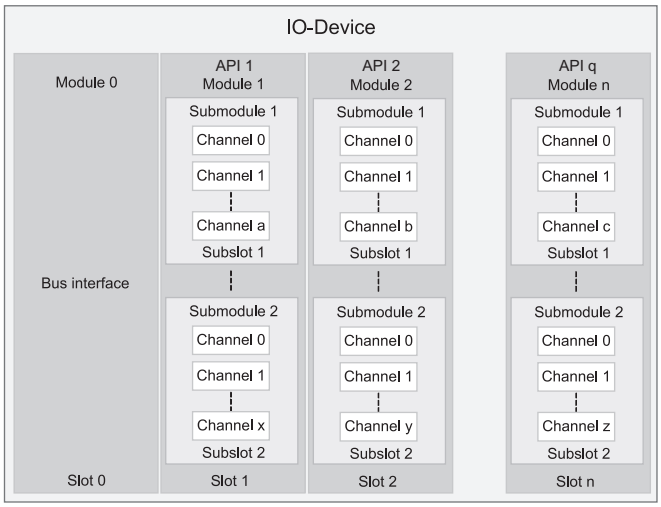


Fig. 4.3 Device model of an IO Device

The modules are positioned in slots, the submodules in subslots. Hot swapping of both modules and submodules is possible. The difference between a "modular" and "compact" device is merely that the slots/subslots with their modules/submodules have a fixed definition in a compact device (virtual module/submodule). The device/slot/subslot address levels can be applied to any physical implementation of devices.

The I/O data are defined within a slot/subslot. Competing values may result when defining the Profinet profile of an IO fevice. This is the case, for example, if an IO device supports different profiles during runtime, e.g. PROFIsafe and PROFIdrive. These profiles are implemented using instances of different applications (Application Process Instances) within the IO device. An Application Process Instance is unambiguously identified by the Application Process Identifier (API), and represents the highest address level.

Channels can be split in an application in two ways:

- All channels can be considered as an entity, and are assigned to one IO Controller.
- The respective channels can be operated independent of each other, and assigned in bit-granular mode to different IO Controllers.

Profinet profiles

Transmitted data are usually interpreted application-specific in the user program of the respective automation system. However, there are applications where the data interpretation is standardized, e.g. in drive engineering or safety-related data transmission. The significance of application-based parameters is defined unambiguously using profiles defined for this purpose.

Table 4.4 Elements of the device model

Element	Function
Application Process Instance	Application within a Profinet IO Device. An Application Process Instance is addressed by the API. The default value of the Application Process Identifier is 0. Valuesþ>þ0 are reserved for Profinet profiles, and are defined by the PNO.
Slot	A slot describes the structure of components or functions, for example hardware modules or logical units within an IO Device. The configuration of the hardware module/logical unit is defined by the vendor. The technical data are defined in the GSD file. The slots are numbered from 1 to 32767, and gaps are permissible. A slot may have several subslots.
Subslot	A subslot describes the structure of components or functions, for example hardware modules or logical units within a slot. The granularity (bit/byte/word/etc.) is vendor-specific. The slots are numbered from 1 to 32767. Subslot number 0 is used to address the slot itself. In addition, subslots in the range from 32768 to 36863 are possible for addressing special applications. A subslot may have several channels.
Channel	Channels represent the actual structure of the input and output data.

A profile is characterized by a profile identifier (profile ID). This profile ID is represented in Profinet IO by the API through which a specific application (Application Process Instance) can be unambiguously identified and addressed within the Profinet IO Device. IO Devices support one or more profiles, but at least the profile of a general Profinet IO Device with the API = 0 (see Table 4.5).

Table 4.5 Examples of Profinet profiles and their applications

Application	Profile	Profile ID/API
Profinet	General device	00000000h
Drive engineering	PROFIdrive	00003A00h-00003AFFh
Safety technology	PROFIsafe	00003E00h-00003EFFh
Conveyor technology	Intelligent pumps	00005D00h-00005DFFh

4.1.3 Data Objects

IO Data Objects are used for cyclic exchange of input/output data. An I/O data element is referenced by specifying the device, slot and subslot.

Record Data Objects are transmitted acyclic to an IO Device, and contain parameterization, configuration, status and diagnostics information.

The event-based transmission of data is carried out using Alarm Data Objects. These include both system-defined events such as hot swapping of modules and user-defined events such as diagnostics or process alarms which have already been detected by the control system.

4.1.4 Context Management (CM)

An IO Device delivers input data from the automated process to the IO Controller, and receives output data for controlling the process. An IO Supervisor can also communicate simultaneously with an IO Device. To permit data exchange to occur at all, it is necessary for application and communication relations to exist. The task of the context management (CM) is to manage the application and communication relations. Details:

- Initialization of application relations
- Initialization of communication relations
- Setting of relevant communication parameters for communication relations, e.g. timeouts and operating modes
- Implementation of unambiguous identification of data exchange
- Parameterization of the Ethernet device driver (EDD)
- Distribution of parameters described in the GSD (general station description) file.

4.1.5 Application Relations (AR)

Applications wishing to exchange data must be related to one another. The actual data exchange over communications channels and the connections established there is only possible if an application relation has been established (see Fig. 4.4). Several application relations can be established to an IO Device from different IO Controllers. IO Devices support at least one IO AR, a supervisor AR and an implicit AR (see Table 4.6).

Table 4.6 Application relations with Profinet IO

Type	Function
IO AR	Cyclic exchange of I/O data over Unicast (1:1) or Multicast connection (1:n) Acyclic exchange of data using read/write services Sending of alarms
Supervisor AR	Data exchange between IO Supervisor and IO Device Take control of one or more submodules of an IO Device by IO Supervisor
Implicit AR	Reading of cyclic or acyclic data by an IO Supervisor out of an IO Controller or IO-Device.

An application relation (AR) is a logical, virtual element which permits data exchange between two devices on communication channels. The actual data transmission takes place within these channels by means of one or more communication relations (see Fig. 4.4).

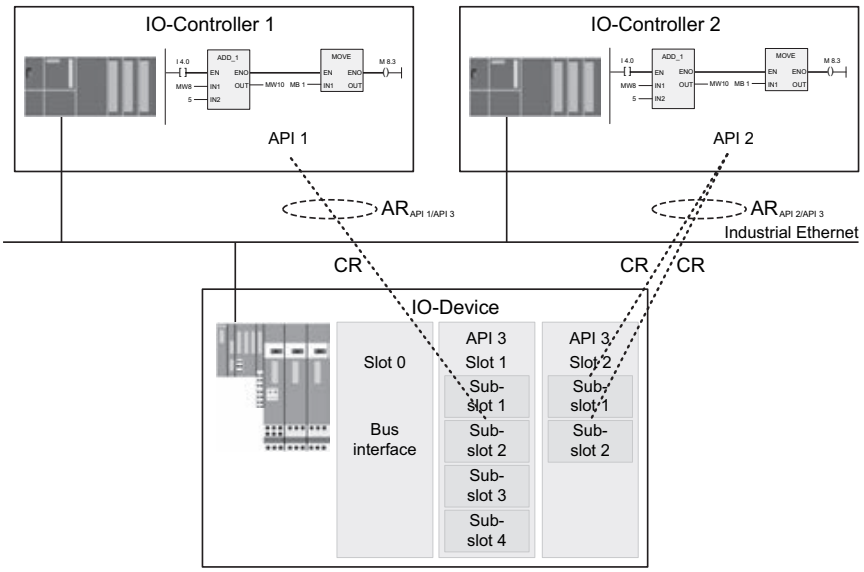


Fig. 4.4 Application relations (AR) and connections between IO Controller and IO Device

IO Devices have a passive response, i.e. establishment of communication using Profinet IO is always initiated by an IO Controller or IO Supervisor.

Establishment of application relations

Establishment of application relations is carried out implicitly during the system startup through establishment of the first communication relation between an IO Controller/IO Supervisor and an IO Device. The following data are transmitted to the IO Device in the process:

- General communication parameters of the AR
- Modeling of the device
- IO Data CR to be established including its parameters
- Event CR to be established including its parameters.

The received data are checked by the IO Device and the requested CR is initialized. Any errors are signaled back to the IO Controller/IO Supervisor.

Clearance of application relations

The clearance of an application relation is implicitly associated with the clearance of all communication channels present within this AR and the corresponding communication relations.

4.1.6 Communication Relations (CR)

Several communication relations (CR) can be established within an AR. The following types of CR exist (see Fig. 4.5):

- The Record Data CR for acyclic transmission of records, e.g. for startup parameterization, diagnostics, etc.
- The IO Data CR for cyclic transmission of I/O data.
- The Alarm CR for acyclic transmission of events.

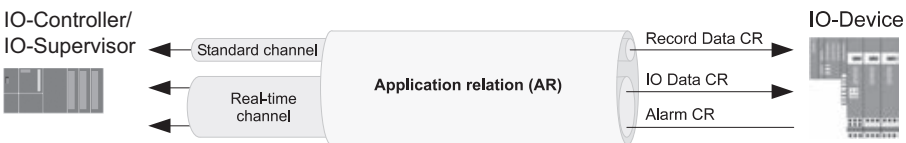


Fig. 4.5 Data traffic with application and communication relations

During establishment of a CR, the context management uses the Profinet IO device model for addressing IO Data Objects.

Since all subsequent subslot parameter settings are handled via this CR, the establishment of the Record Data CR is always carried out first (Table 4.7).

Record Data CR

The Record Data CR is established from the Record Data client (typically an IO Controller) to the Record Data server (typically an IO Device). Since all subsequent

Table 4.7 Data and objects transmitted within a Record Data CR

Data type	Contents	Read/write (R/W)
Record Data Objects	Records	R/W
Diagnostic Data Objects	Diagnostics data	R
IO Data Objects	I/O data	R
Identification Data Objects	Identification data (I&M)	R
AR-Data	AR-specific data	W
Log Data	Log data	R
Physical Device Data	Device data	R/W
Configuration Data	Configuration data	W
Differences between expected and inserted modules	Differences between correct configuration and actual configuration	R

subslot parameter settings are handled via this CR, the establishment of the Record Data CR is always carried out first (Table 4.7).

IO Data CR

The task of the IO Data CR is to transmit I/O data. Data exchange is according to a provider/consumer model as with Profinet CBA. The following parameters are transmitted during establishment of an IO Data CR by the consumer:

- A list of I/O data objects to be transmitted as well as their structure
- The parameters of the send interval (send clock time, scaling, phase and sequence)
- The transfer frequency.

The number of IO Data CRs to be established is defined in the device configuration. Two “opposite” IO Data CRs are always established, thus permitting bidirectional data exchange between IO Controller/IO Supervisor and IO Device.

The data are sent cyclically from the provider to the consumer in line with the configured transfer frequency. Explicit acknowledgment of transmitted data is not carried out. Nevertheless, the data are acknowledged implicitly by means of the simultaneously established “opposite” IO Data CR (IOCS). I/O data are transmitted unformatted, and contain submodule-granular status information. Communication is monitored by the consumer, also through evaluation of the cycle counter element in the RT frame.

The transmitted value of an I/O data object has a consistent length. Consistency of values over several I/O data objects is not supported. The maximum possible consistent length of an I/O data value is 240 bytes.

Alarm CR

An IO Device transmits alarms to the IO Controller by means of an Alarm CR. Alarms are acyclic data which have to be acknowledged within a defined time at both the protocol and user levels. It is possible to set how many alarms can be sent before an acknowledgment must be explicitly carried out. Since the acyclic services do not support segmenting, all alarms must be transmitted within one frame.

When configuring an Alarm CR, the end for the alarm source and the end for the alarm sink are defined. Both the IO Controller and IO Device can work as an alarm source or sink.

The IO Controller defines the priority with which alarms are to be transmitted. Exactly one low-priority alarm and one high-priority alarm can be transmitted simultaneously in one Alarm CR (see Table 4.8). High-priority alarms must always be processed as fast as possible. Low-priority alarms must not significantly delay a high-priority alarm.

Table 4.8 Profinet IO alarms and their mapping in a Simatic S7 user program

Alarm priority	Alarm	Simatic S7 alarm type	Organization block
High	Process	Process interrupt	OB 40-47
Low	Diagnosis (appears/disappears)	Diagnostics interrupt (UP/DOWN)	OB 82
	Pull	Remove module interrupt	OB 83
	Plug	Insert module interrupt	
	Plug_wrong	Insert module interrupt	
	Return of submodule	Insert module interrupt	
	Controlled	Control interrupt	
	Released	Release interrupt	
	–	Station failure interrupt	OB 86
	–	Station return interrupt	
	Status	Status interrupt	OB 55
	Update	Update interrupt	OB 56
	Manufacturer-specific	Manufacturer-specific interrupt	OB 57
	Profile specific	Profile-specific interrupt	
	Redundancy	I/O redundancy error	OB 70

4.1.7 Services and Protocols

The various services used with Profinet IO are described below. A detailed description of the protocol structure will not be provided here. In this context, the book from Manfred Popp [16] is recommended.

Cyclic I/O data

Following the system startup, I/O data are exchanged cyclically between IO Controller and IO Device. Each item of I/O data contains two attributes, the IOPS (IO Provider Status) and IOCS (IO Consumer Status), which permit the IO Controller and IO Device to evaluate the quality of the transmitted value (Fig. 4.6).

The IOPS is transmitted by the provider simultaneously with the data, and is therefore consistent with the data value. On the other hand, the IOCS can only be returned from the consumer to the provider following the receipt of data. The IOCS and the data value are therefore inconsistent (see Table 4.9, Fig. 4.7).

IOCS and IOPS can have the values GOOD and BAD, where different values are defined for BAD specific to the fault (BAD_BY_CONTROLLER, BAD_BY_DEVICE, ...).

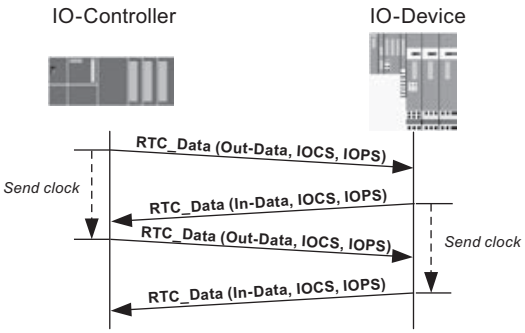


Fig. 4.6
Sequence of cyclic data transmission with RT protocol for Profinet IO

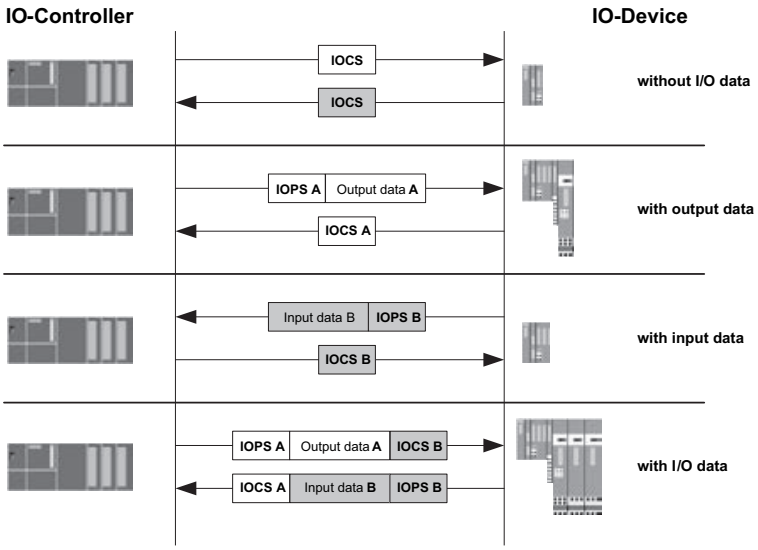


Fig. 4.7 IOPS and IOCS with IO Controller and IO Device

Table 4.9 Significance of IOPS and IOCS with IO Controller and IO Device

Data	IOPS	IOCS
Input	The IOPS describes the provider status of the input data, and is transmitted by the IO-Device together with the actual data to the IO Controller. The IOPS provides the instances in the transmission path, e.g. submodule, module, IO-Device or the IO Controller itself with a facility for identifying invalid input values. The control application of the IO Controller may only process values with IOPS = GOOD. Values with IOPS = BAD must be replaced by a corresponding default value, and the submodule can be marked as being faulty.	The IOCS describes the consumer status of the input data, and is transmitted from the IO-Controller to the IO Device. It helps the IO Device to recognize communication problems, and provides information on whether the IO Controller is currently processing the delivered input values or not (example: IO Controller in STOP state). The response of an IO Device to IOCS = BAD is vendor-specific.

Table 4.9 Significance of IOPS and IOCS with IO Controller and IO Device *(continued)*

Data	IOPS	IOCS
Output	The IOPS describes the provider status of the output data, and is transmitted by the IO-Controller together with the actual data to the IO Device. It helps to recognize communication problems, and provides information to the IO-device on whether the IO Controller can currently set the delivered output values or not (example: IO Controller in STOP state). The IO Device may only process values with IOPS = GOOD. Values with IOPS = BAD must be replaced by a corresponding default value.	The IOCS describes the consumer status of the output data, and is transmitted from the IO Device to the IO Controller. It helps the IO Controller to recognize communication problems, and provides information on whether the IO Device can currently pass on the delivered output values to the process or not (example: if a module has been removed from a modular IO Device). The IOCS can be set by all instances in the transmission path, e.g. submodule, module, IO Device or the IO Controller itself. The response of an IO Controller to IOCS = BAD is vendor-specific. With Simatic S7 CPU, the submodule is marked as being faulty.

Alarms

All process events must be signaled within a Profinet IO configuration by means of alarms (see Tables 4.10 and 4.11 as well as Fig. 4.8). The transmission is carried out using the acyclic real-time protocol (RTA: real time acyclic). An IO Device transmits alarms with priority as real-time messages. Both UP and DOWN alarms must be acknowledged by the IO Controller.

Table 4.10 Alarms

Alarm type	Triggering events
Process alarm	The alarm signals the occurrence of an event from a process, e.g. a temperature violation.
Diagnosis appears	The alarm signals the appearance of a fault or diagnostics event within an IO Device in conjunction with the connected components, e.g. an open-circuit.
Diagnosis disappears	The alarm signals the disappearance of a fault or diagnostics event within an IO Device in conjunction with the connected components, e.g. an open-circuit.
Pull	With modular IO Devices, the alarm signals the removal of a module/submodule.
Plug	With modular IO Devices, the alarm signals the insertion of a module/submodule. Following insertion, the parameters of the corresponding module/submodule are loaded again.
Plug Wrong	The alarm signals that an incorrect module/submodule has been inserted.
Status	The alarm signals a change in status of a module/submodule.
Update	The alarm signals changes in the parameters of a module/submodule.
Redundancy	The alarm signals to a secondary IO Controller that the primary IO Controller has failed.
Controlled by Supervisor	The alarm signals that an IO Supervisor has taken over control of a module/submodule.
Released by Supervisor	The alarm signals the release of a module/submodule from control by an IO Supervisor, IO Controller or the local access of an IO Device. This is followed by the same protocol sequence as with a plug alarm.

Table 4.10 Alarms *(continued)*

Alarm type	Triggering events
Return of Submodule	The alarm signals that: – an IO Device delivers valid data again for a particular input element without having been reparameterized or – an output element can process the received data again. The alarm signals the change in status of the input or output data of a provider or consumer submodule from invalid (BAD) to valid (GOOD).
Profile specific	The alarm signals agreement of an IO Device with specific profiles of the PNO profile guidelines.
Multicast Provider Communication Stopped	The alarm signals a timeout during the multicast transmission of I/O data by the provider.
Multicast Provider Communication Running	The alarm signals resumption of the multicast transmission of I/O data by the provider.
Port Data Changed Notification	The alarm signals a change in Ethernet port data.
Sync Data Changed Notification	The alarm signals a change in time synchronization.
Isochronous Mode Problem Notification	The alarm signals a problem in applications working in isochronous mode.
Manufacturer Specific	The alarm signals a vendor-specific alarm type.

Table 4.11 Services for alarm transmission

Service	Function
RTA_DATA Request (Alarm)	Alarm notification from an IO Device to the IO controller. The following are transmitted: – Alarm identification (diagnostics, process etc.) – Address information (API, slot, subslot, module ID) – General parameters – With channel diagnostics: channel number, channel type, fault type
RTA_DATA Request (Alarm_Ack)	Alarm acknowledgement of IO Controller at the application level: From the view of the IO Device, the alarm is only safely saved following receipt of this acknowledgment.
RTA_ACK	Acknowledgement of an RTA_DATA frame at the protocol level: The RTA_DATA frame has been received, and resources are available for receipt of a further frame. Frame repetition is unnecessary.

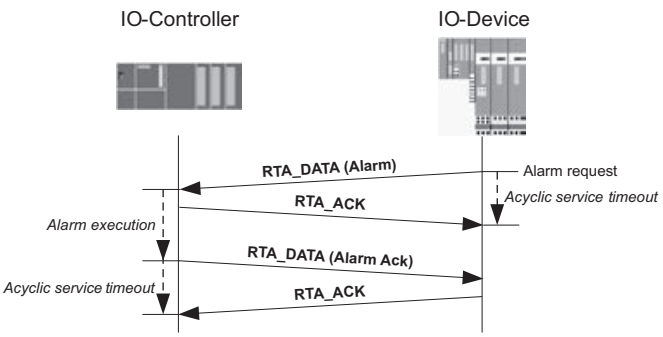


Fig. 4.8
Alarm processing sequence with Profinet IO

Acyclic data transmission

Acyclic data transmission serves to exchange data which are not time-critical. Read and write services are used. Acyclic data exchange takes place within the NRT communication channel (NRT: non-real-time) using remote procedure calls (RPC), based on UDP/IP.

Read/write services always consist of a request and a subsequent response (see Fig. 4.9 and Table 4.12). Write requests are only permissible within an established IO Data CR, read requests can also be carried out without an explicit IO Data CR.

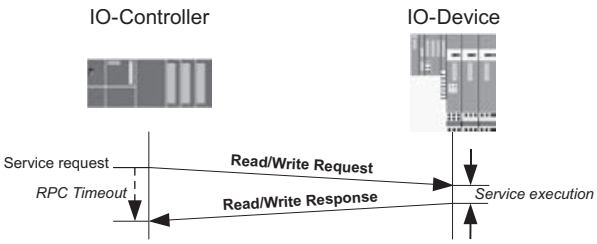


Fig. 4.9
Sequence of acyclic read/write services with Profinet IO

Table 4.12 Read/write services

Service	Function
Read Request	Data request from an IO Controller to an IO Device.
Read Response	Transmission of requested data to the IO Controller.
Write Request	Data transmission from an IO Controller to an IO Device.
Write Response	Acknowledgment of data transmission by the IO Device.

Assignment of name to an IO Device

IO Devices are assigned a name prior to the actual establishment of a connection. The name is assigned by an IO Supervisor and saved in retentive mode in the IO

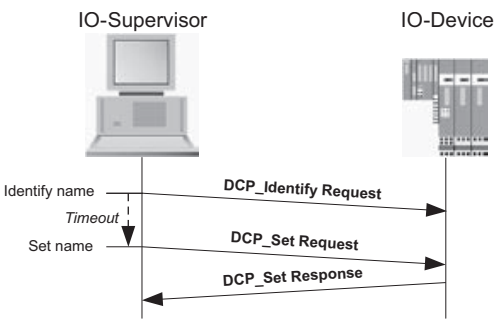


Fig. 4.10
Sequence for assignment of name to an IO Device

Table 4.13 Services for assignment of a name to an IO Device

Service	Function
Identify Request	Request to IO Devices for a certain search criterion (device name in this case) by IO-Supervisor or IO Controller.
Set Request	Writing of a parameter (device name in this case) into an IO Device: Device names must comply with the DNS conventions, i.e.: – Limited to 240 characters (letters, digits or hyphen) – No special characters
Set Response	Acknowledgment of Set Request.

Device (see Fig. 4.10 for sequence). The name is used for unambiguous identification of an IO Device during runtime, and can be freely selected by the user within the DNS name conventions (DNS: domain name services). The name is assigned in the first version of Profinet IO by means of the DCP (discovery and basic configuration protocol) (Table 4.13).

Assignment of IP address to an IO Device

An IO Device is assigned its IP address which is valid during runtime from the IO Controller during the system startup. In addition to the ARP service (ARP: address resolution protocol) known from the IT world, also uses DCP services (see Fig. 4.11 and Table 4.14).

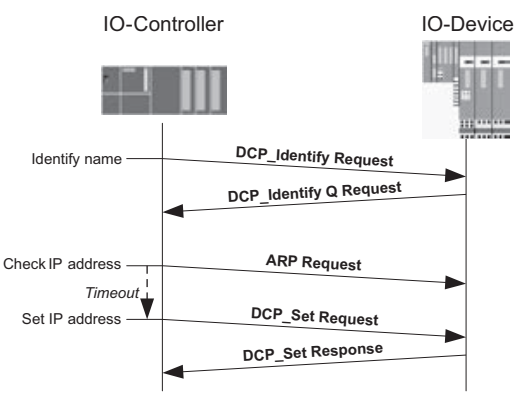


Fig. 4.11 Sequence for assignment of the IP address to an IO Device using DCP

Table 4.14 Services for assignment of the IP address to an IO Device using DCP

Service	Function
Identify Request	Request to IO Devices for a certain search criterion (device name in this case) by IO-Supervisor or IO Controller.

Table 4.14 Services for assignment of the IP address to an IO Device using DCP *(continued)*

Service	Function
Identify Q Request	Response to Identify Request: The object searched for has been found (device name in this case).
ARP Request	Determination of the MAC address (Ethernet address) corresponding to an IP address: The ARP is a protocol from the IT world, and is a typical component of the TCP(UDP)/IP protocol suite. An ARP Request is sent as a broadcast to all devices within an Ethernet subnet and is used with Profinet IO to search for IP addresses. If no response is provided to the ARP Request, no device with the requested IP address is existent or active in the corresponding Ethernet subnet.
Set Request	Writing a parameter (IP address in this case) to an IO Device.
Set Response	Acknowledgment of Set Request

Address assignment using DHCP

Profinet IO optionally supports the assignment of IP addresses to IO Devices using DHCP (DHCP: dynamic host configuration protocol) (see Fig. 4.12 and Table 4.15). When using DHCP within a network, a separate DHCP server manages the assignment of IP addresses. In this case, an IO Device actively requests the assignment of an IP address from the server.

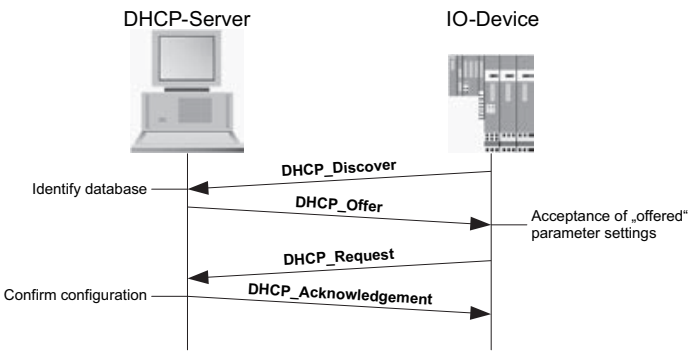


Fig. 4.12 Sequence for assignment of the IP address to an IO Device using DHCP

Table 4.15 Services on assignment of IP address to an IO Device using DHCP

Service	Function
Discover	Request of a device to all DHCP servers in the Ethernet subnet for assignment of an IP address.
Offer	Transfer of an IP address from the DHCP server to the requesting device: In addition to the actual IP address, the frame contains further IP address parameters such as the subnet mask etc.

Table 4.15 Services on assignment of IP address to an IO Device using DHCP *(continued)*

Service	Function
Request	Feedback of device to DHCP server: With this frame, the device confirms the IP address parameters selected by it. The IP address is marked in the DHCP server as being assigned.
Acknowledgement	Confirmation of the IP address and parameters selected by the device by means of the DHCP server: The device can now be accessed using the IP address.

Establishment of connection

An IO Data CR is established through a Connect sequence between IO Controller and IO Device. The subsequent Write Request initiates its parameterization, which is terminated by the subsequent DControl Request. Following the positive response to the CControl Request sent by the IO Device, establishment of the IO Data CR is complete.

Fig. 4.13 shows the basic establishment of a connection between IO Controller and IO Device, Table 4.16 explains the corresponding sequences.

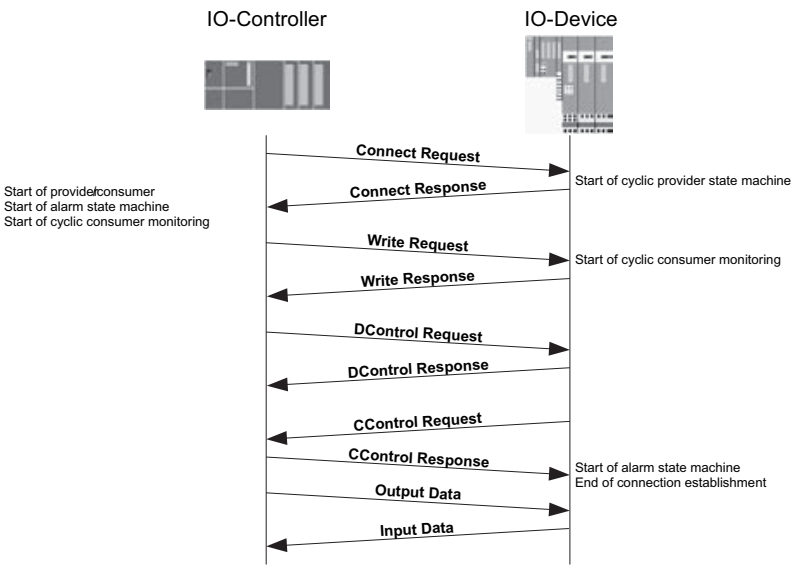


Fig. 4.13 Basic sequence for establishment of connection with Profinet IO

Profinet IO Device identification

A IO Device is unambiguously identified by a device identification (see Table 4.17). During the system startup, the IO Device checks the device identification sent by the IO Controller with its own, fixed parameter ID.

Table 4.16
Services for establishment of connection between IO Controller and IO Device

Service	Function
Connect Request	Initiation of establishment of connection: Establishment of all required ARs and CRs. Establishment of connection is always necessary except with services which can only read data.
Connect Response	Reply of IO Device to request for establishment of connection: The response is only sent when it has been guaranteed that the connection can be established.
Write Request	Data transmission from an IO Controller to an IO Device: Transmission of parameter data for the individual submodules to the IO Device. A separate record is defined for each module/submodule, and is transmitted in its own Write Request.
Write Response	Acknowledgment of data transmission by the IO Device: Further data can be transmitted following the Write Response.
DControl Request	Signaling of end of parameter transmission by the IO Controller.
DControl Response	Acknowledgment of DControl Request by the IO Device. Establishment of the connection is completed following this frame.
CControl Request	Confirmation of establishment of connection by the IO Device.
CControl Response	Acknowledgment of CControl Request by the IO Controller.
Input/Output Data	Cyclic I/O data transmitted by real-time protocol.

Table 4.17 Structure of device identification

Device identification	Vendor_ID (16 bit)	Device_ID (2 byte)
Meaning	Identification assigned by the PNO as unambiguous reference to the vendor. For example, the Vendor_ID of Siemens is 42 (0x2A).	ID defined vendor-specific for detailed differentiation of IO Devices.

4.1.8 From Configuration to Up-and-Running System

An IO Device does not have a device name when delivered. An IO Device is only addressable for an IO Controller when a device name has been assigned by the IO Supervisor. Fig. 4.14, 4.15 and Table 4.18 show and explain the steps which are implemented when using Simatic together with Step 7.

4.1.9 Proxy Functionality with Profinet IO

In a manner similar to Profinet CBA, field devices can be integrated into the cyclic Profinet IO communication by means of a so-called proxy on the Ethernet. From the viewpoint of communication, a proxy makes a field device appear like an IO Device, and corresponds to an Ethernet/fieldbus gateway from the viewpoint of the process data.

Data exchange with the field device is then via the proxy which passes on the data by means of the respective fieldbus protocol to the field device or fetches them

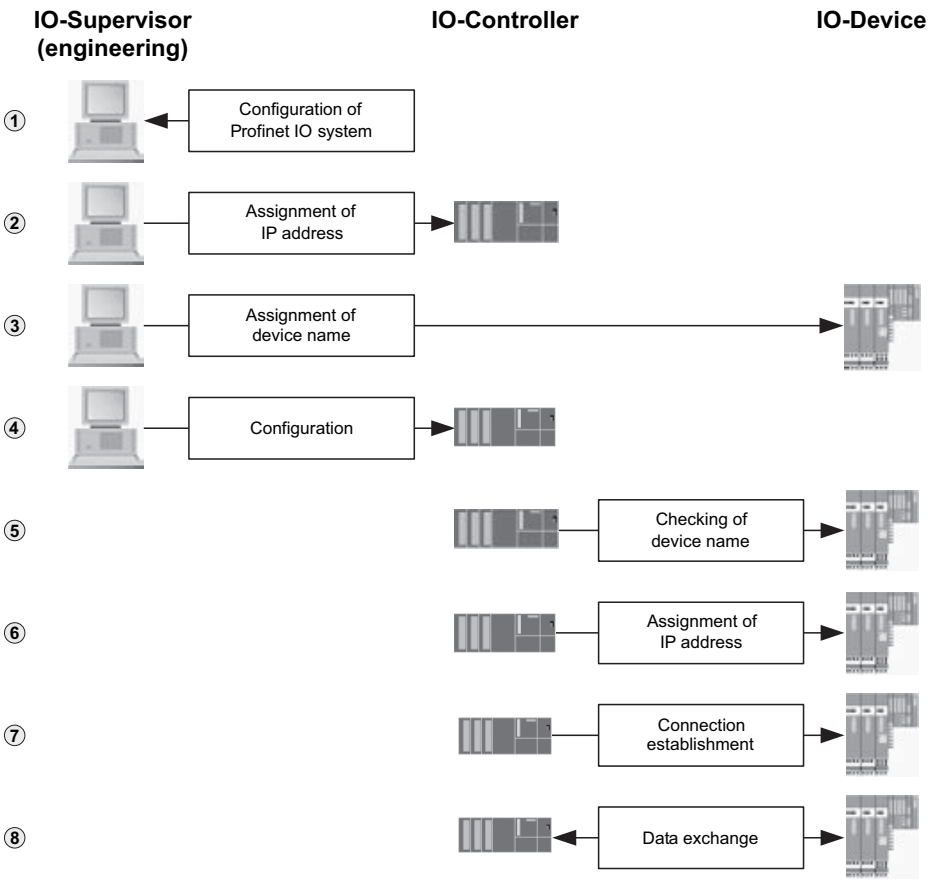


Fig. 4.14 Steps from configuration up to system startup

Table 4.18 Steps from configuration up to system startup

Step	Function
1	Configuration of Profinet IO System in HW-Config.
2	Assignment of an IP address to the IO Controller.
3	Assignment of device names to the configured IO Devices.
4	Transmission of Profinet IO configuration to the IO Controller.
5	Checking of names of configured IO Devices.
6	Assignment of configured IP addresses to the configured IO Devices.
7	Initiation of establishment of connection between IO Controller and the configured IO Devices.
8	Exchange of cyclic I/O data between IO Controller and the configured IO Devices.

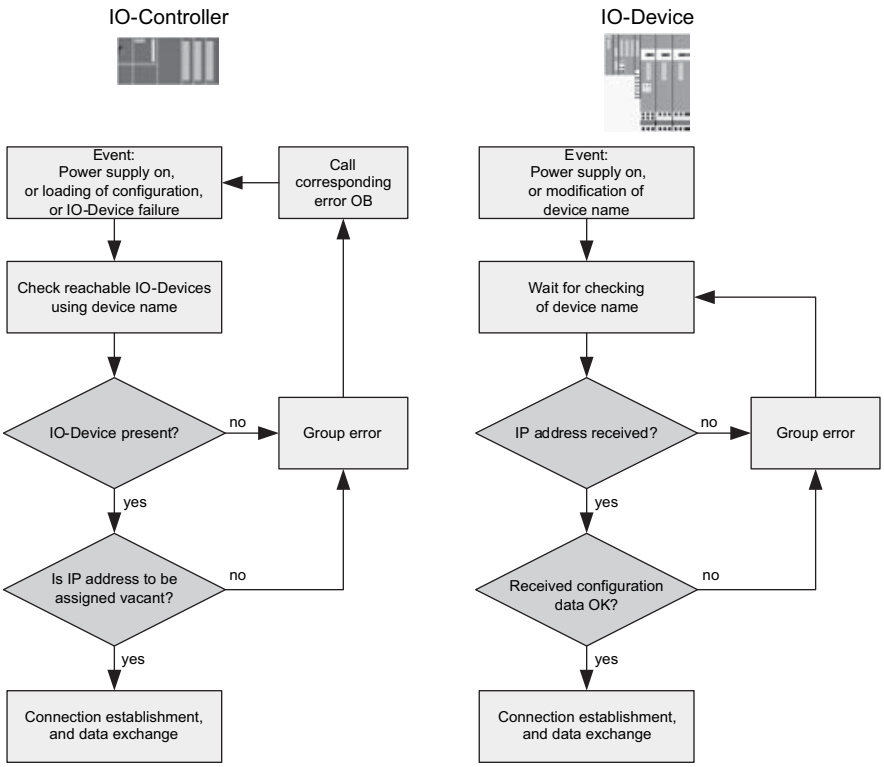


Fig. 4.15 Startup response of Simatic Profinet IO devices

from there. The proxy functionality in the sense of Profinet IO is a property of Profinet IO Controllers with additional fieldbus functionality, for example with Profibus DP master functionality.

Profinet CBA and Profinet IO proxies basically fulfill the same task through integration of field devices, but do not have compatible functions because of the different communications services used on the Ethernet (see Fig. 4.16).

4.1.10 Profibus Integration

IO Controllers with DP master functionality support simultaneous operation of Profibus and Profinet IO systems. Alternatively, it is possible for Profibus DP slaves to integrate them as an IO Device via a Profinet IO device with proxy functionality. Fig. 4.17 and Table 4.19 show and explain which configurations are supported.

In addition to the guideline for integration of Profibus slaves, guidelines for integration of field devices for the Interbus, AS-I (actuator/sensor interface), DeviceNet and HART (Highway Addressable Remote Transducer) fieldbus systems are available.

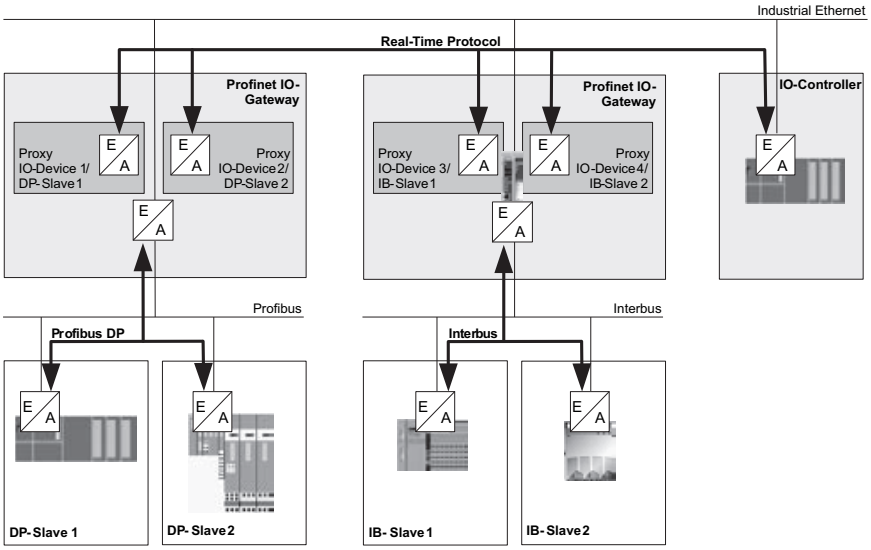


Fig. 4.16 Principle of proxy functionality with Profinet IO

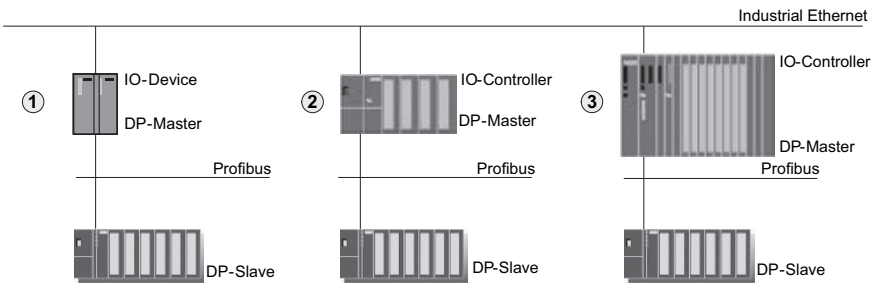


Fig. 4.17 Integration of Profibus with Profinet IO

Table 4.19 Configurations with Profibus integration in Profinet IO

Profinet IO device	Configuration
1	Profinet IO Link Simatic Net IE/PB-Link PN IO as proxy for Profibus DP slaves.
2	Simatic S7 CPU 31x-2PN/DP as IO Controller with simultaneously used Profibus subnet.
3	Simatic S7 CPU 41x with Simatic Net-CP 443-1 Advanced as IO Controller with Profibus subnet simultaneously used by the CPU.

4.2 From Planning to Operation of a Plant

Engineering of Profinet IO Systems is similar to that with Profibus DP. Profinet IO devices are configured using the Simatic Step 7 engineering tool (see Table 4.20). They are selected in HW-Config from the central data management, the module catalog. Devices which are not present there can be added by importing a GSD file. Coupling to a Profinet IO System and parameterization with an IP address are carried out graphically in HW-Config or Netpro.

Step 7 automatically checks whether all quantity frameworks defined by the hardware have been observed in the project and that the configuration is consistent and free of errors. Following loading of the configuration into the PLCs, online access to process data is possible at any time using variables tables, HMI applications such as Simatic ProTool/ProRT and Simatic WinCC flexible or other OPC-based client programs. During commissioning and operation, an online/offline comparison of the device configurations can be made for Profinet IO devices, the current device status can be displayed, and online data can be scanned for test and diagnostics purposes. Simatic Net switches are integrated in the Profinet IO diagnostics concept, and can be configured and diagnosed as IO Devices. Documentation of the completely configured plant including all devices and connections can be carried out automatically by Step 7 as the last step.

The process from planning to operation of a Profinet IO-based automation solution with Simatic Step 7 is carried out in the steps according to Table 4.21.

Table 4.20 Comparison of Profinet IO and Profibus DP in Step 7

Feature	Profinet IO	Profibus DP
Subnet name	Ethernet	Profibus
Name of subsystem	Profinet IO system	DP master system
Hardware catalog	Profinet IO	Profibus DP
Number assignment	Device number	Station number (corresponds to Profibus address)
Device parameter/diagnostics address	Can be set using the object properties of the interface module in slot 0.	Can be set using the object properties of the station.

Table 4.21 Plant engineering sequence with Profinet IO

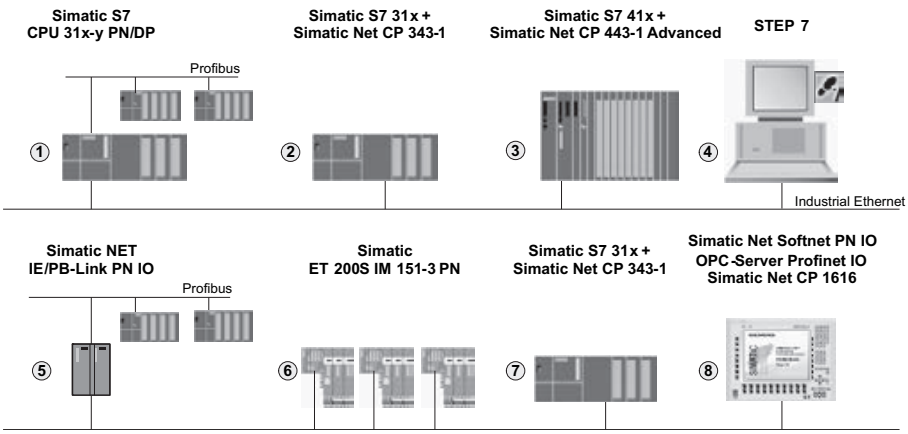
Step	Activity
1	Planning the plant.
2	Configuration of plant with Simatic Step 7.
3	Commissioning of plant.
4	Operation of plant.
5	Maintenance and modification work.

4.2.1 Planning the Plant

Prior to the actual plant engineering, the plant planner first clarifies the fundamental questions regarding the plant architecture (see Table 4.22). The result is a plant plan which serves as the basis for further procedures (Fig. 4.18).

Table 4.22 Procedure when planning the plant

Step	Activity
1	Definition of required functions
2	Definition of used PLCs and field devices



Profinet IO device	Type	Function
1	IO Controller	The Simatic S7 31x-2 PN/DP CPU works as an IO Controller and DP-Master.
2	IO Controller	The Simatic Net CP 343-1 Advanced works as an IO Controller.
3	IO Controller	The Simatic Net CP 443-1 Advanced works as an IO Controller.
4	IO Supervisor	The PC works with the Simatic Step 7 engineering tool as an IO Supervisor.
5	IO Device	The Simatic Net IE/PB Link PN IO gateway works as a proxy for the connected DP slaves. Each DP slave is visible for the IO Controller as an IO Device.
6	IO Device	The Simatic ET 200S IM 151-3 PNs work as IO Devices.
7	IO Device	The Simatic Net-CP 343-1 works as an IO Device.
8	HMI	The PC works as a Profinet IO OPC server, and reads data from an IO Controller.

Fig. 4.18 Example of a plant configuration with Simatic devices for Profinet IO

4.2.2 Configuration of Plants with Simatic Step 7

The task of the configuration engineer is to completely configure the plant in Step 7. This commences with creation of a project, and ends with plant commissioning, subsequent documentation, and archiving of the project data (see Table 4.23).

Table 4.23 Basic procedure for configuration of a plant with Step 7

Step	Activity
1	Creation of a new Profinet IO project, or opening an existing one.
2	Option: Importing of IO Devices using GSD file.
3	Insertion of Profinet IO Devices into a project.
4	Configuration of the IO Controller.
5	Configuration of the Profinet IO System.
6	Configuration of IO Devices and Profinet IO gateways.
7	Option: Configuration of a sync domain.
8	Option: Definition of IRT topology.
9	Assignment of an IP address to the IO controller.
10	Assignment of device names to the configured IO Devices.
11	Generation of the user program.
12	Downloading of the configuration and user program.

Creation of a new Profinet IO project, or opening an existing one

A Simatic 300 station is initially inserted as a new object in the Simatic Manager. Alternatively, the station is opened which is to be expanded by a Profinet IO System (see Fig. 4.19).

Fig. 4.19 Creation of a new Profinet IO project

Importing of IO Devices using GSD file

Analogous to the importing of DP slaves with Profibus, IO Devices are also imported using a device description (device master data, GSD) into the Step 7 module catalog (see Fig. 4.20). If several GSD files exist for a IO device, the latest version of the GSD file is always considered. The GSD file contains all information required for device configuration.

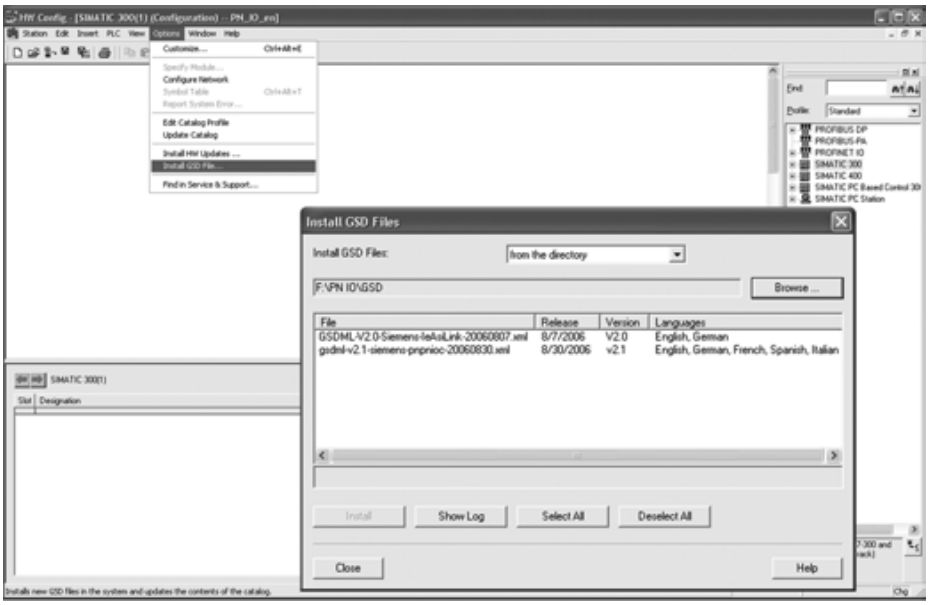


Fig. 4.20 Importing of IO Devices using GSD

GSD file

Every vendor of an IO device must provide an associated GSD file. This file describes the properties of the IO devices similar to Profibus DP. Contrary to this, however, the file is not present in a keyword-based text file but as an XML file. In association with Profinet IO, the term Generic Station Description Markup Language (GSDML) is therefore also used.

XML is a metalanguage defined by the World Wide Web Consortium (W3C), and permits the definition of markup languages. The structure of the GSD conforms to the ISO 15745 “Open Systems Application Integration Framework”, and is based on the device profile defined there.

The structure and rules of a GSD file are defined by the GSDML schema. This schema describes the structure of a GSD file and contains the validity rules which permit, for example, checking of a GSD file syntax. GSDML schemas are administered by Profibus International. Checking can be carried out using an XML parser. Sche-

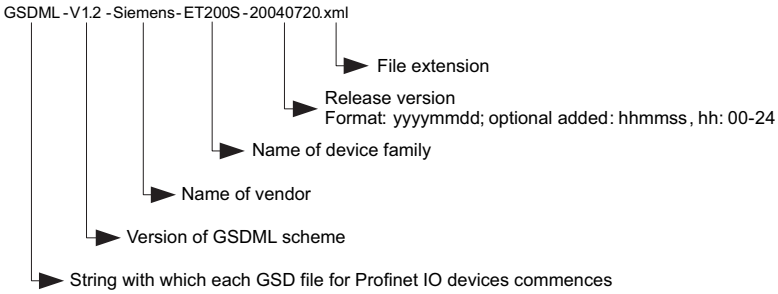


Fig. 4.21 Name schema of a GSD file

ma files have the extension ".xsd". The specification for generation of an XML schema has been published on the Internet at http://www.w3.org/XML/Schema.

Function expansions in the environment of Profinet IO always have effects on the GSDML specification and the associated scheme, and necessitate a new version of the specification and scheme (see Fig. 4.21).

The version of a GSD file contains two items of information:

- The version of the GSDML scheme used: this defines which language scope is used by a GSD file.
- The version date: the date is updated if e.g. a fault has been eliminated or the functions have been extended.

Configuration of the IO Controller

The following can be used as IO Controllers:

- Simatic S7 CPU 31x-y PN/DP
- Simatic S7 CPU 41x-y PN/D
- Simatic S7 CPU 31x together with a Simatic Net Profinet CP (e.g. CP 343-1)
- Simatic S7 CPU 41x together with a Simatic Net Profinet CP (e.g. Simatic Net CP 443-1 Advanced) or
- PC station (e.g. with Simatic Net CP 1616)

The IO Controller is selected from the hardware catalog for this purpose, and positioned as usual in a permissible tier of the subrack using drag&drop.

Configuration of PN IO interface of an IO Controller

A Profinet IO System connected to the PN IO interface of the IO Controller similar to a Profibus configuration. Configuration of the PN IO interface is carried out first (see Figs. 4.22 to 4.26 and Tables 4.24 to 4.26).

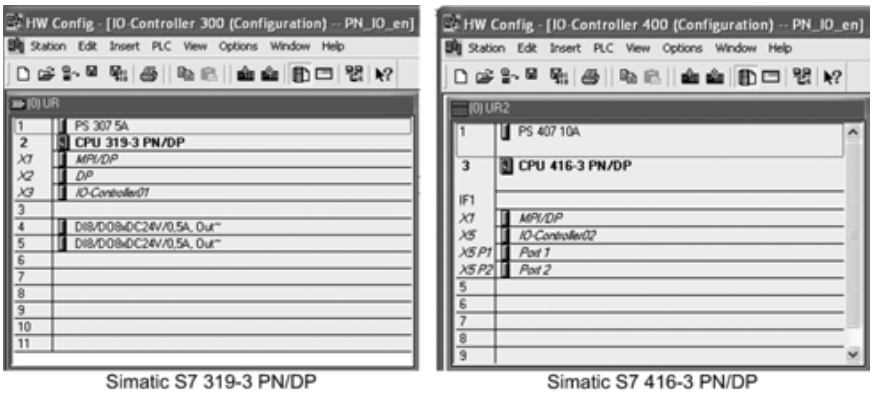


Fig. 4.22 Example of PN IO interface with Simatic S7

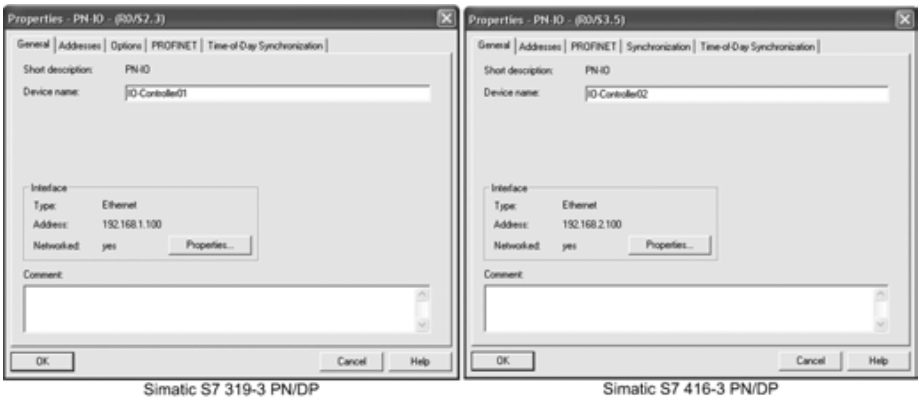


Fig. 4.23 General settings of the PN IO interface

Table 4.24 Parameters in the tab “General”

Parameter	Meaning
Short designation	Designation of IO Controller. The abbreviation is always “PN-IO” in the case of an integral Profinet interface.
Device name	Unambiguous device name on the Ethernet subnet which complies with the DNS conventions. With integral Profinet interfaces, the device name is derived from the short description.
Interface	“Interface” contains the type and address of the interface for a subnet. With Ethernet, this is the IP address. “Networked” (yes/no) indicates whether the module is connected to a configured subnet. The button “Properties” can be used to change the properties of the subnet, to generate a new subnet, or to select a different subsystem.
Comment	Comment on the Profinet IO interface.

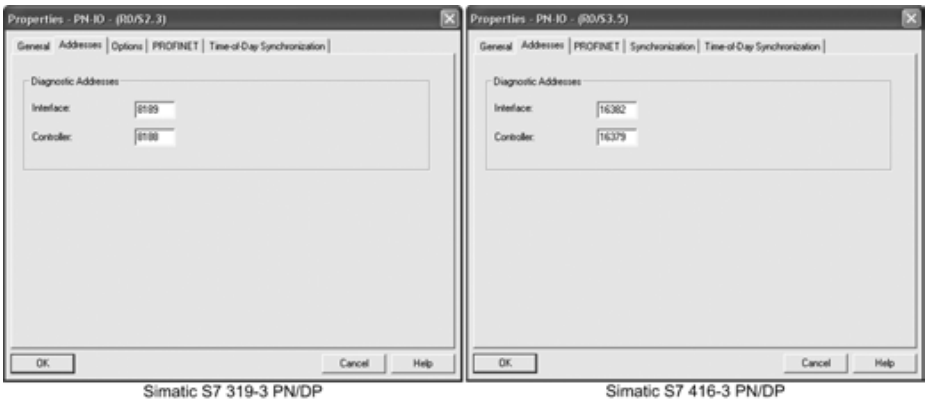


Fig. 4.24 Setting the addresses of PN IO interfaces with Simatic S7

Table 4.25 Parameters in the tab "Addresses"

Box	Meaning
Diagnostic addresses	Interface: By means of this diagnostic address, the CPU signals e.g. synchronization errors or media redundancy errors of the IO Controller, providing the IO Controller supports this function. Controller: By means of this diagnostic address, the CPU signals e.g. a failure/return of the Profinet IO System. On failure of an IO Device, the associated IO System is also identified by this address.

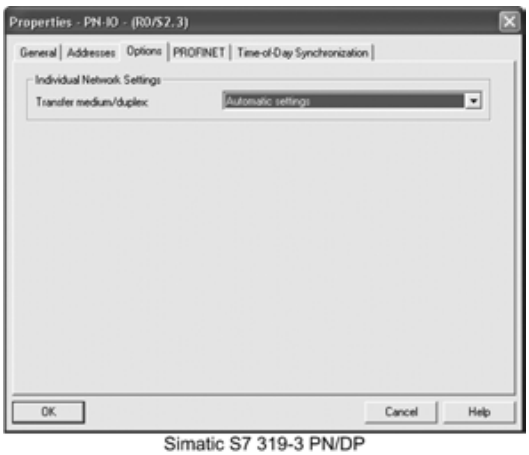


Fig. 4.25 Setting of options for PN IO interfaces with Simatic S7

Table 4.26 Parameters in the tab “Options”

Box	Meaning
Individual network settings	Transfer medium/duplex: Automatic or TP/ITP with 100 Mb/s full duplex A fixed network setting can be made here if required. “Automatic settings” is standard, and guarantees problem-free communication in the standard case. If problems occur during communication (connections are not established, frequent occurrence of network faults), it could be the case that the selected or automatic network setting is inappropriate. Module-dependent: Port: Activated/deactivated By selecting one of these possibilities, an unused port can be deactivated, for example for safety reasons. TP: Twisted-pair cables ITP: Industrial twisted-pair cables

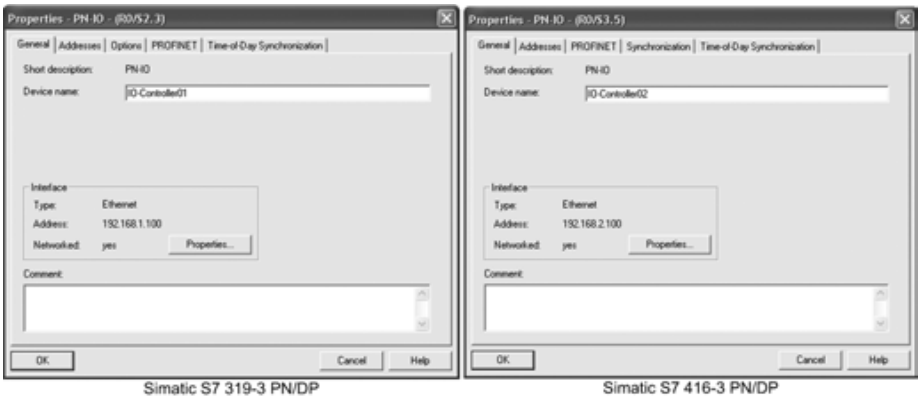


Fig. 4.26 Setting of Profinet properties of PN IO interfaces with Simatic S7

Configuration of a Profinet IO System

The designation of the Profinet IO Systems has a similar structure to that with DP master systems. The first part of the name identifies the Ethernet subnet, followed by a colon. The second part of the name consists of the designation “IO System” followed by the number of the IO System in brackets. Whereas the numbers commence with “1” for DP master systems, Step 7 assigns numbers starting at “100” to Profinet IO Systems. See Figs. 4.27 to 4.32 and Tables 4.27 and 4.31.

Table 4.27 Parameters in the tab “Profinet”

Parameter/box	Meaning
Send clock	The send clock is the period between two successive intervals for IRT or RT communication. The send clock is the smallest possible send interval for data exchange. The calculated updating times are a multiple of the send clock. If the IO Controller is working as a sync slave or sync master, Step 7 indicates the send clock which has been selected in the dialog “Domain Management” (tab “Sync-Domain”). If the IO Controller is not working as a sync slave or sync master, the send clock is set here.

Table 4.27 Parameters in the tab "Profinet" *(continued)*

Parameter/box	Meaning
IO communication	If cyclic data exchange over Profinet IO and Profinet CBA takes place on the same Ethernet subnet, the percentage share of Profinet IO in the total communication (Profinet IO + Profinet CBA) must be defined. Communication component (Profinet IO): If the module is to be used simultaneously for cyclic data exchange over Profinet IO and Profinet CBA, the share of Profinet IO communication in the total communication is defined here. With a setting of 100%, the available capacity is reserved exclusively for Profinet IO data exchange. The communication component for acyclic data exchange (e.g. PG access/IO Supervisor) need not be explicitly considered at this point since a sufficiently large time share is already reserved for the system.
CBA communication	This module is used for Profinet CBA communication: If this option is selected, a Profinet component can be created from the module for use with Profinet CBA. Communication component (Profinet CBA): Calculated share of Profinet CBA communication in total communication.
OB 82 / Fault task call with communication alarms	If this option is selected, all diagnostic events result in calling of the OB 82 as well as an entry in the diagnostics buffer. If this option is deactivated, calling of the OB 82 is suppressed for certain diagnostic events. Such events are information from the Profinet interface, for example maintenance information specifying the necessity for preventive maintenance (maintenance request or maintenance requirement).

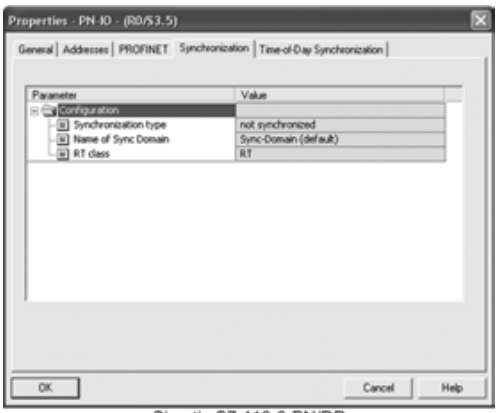


Fig. 4.27
Setting and display of the synchronization settings of PN IO interfaces with Simatic S7

Table 4.28 Parameters in the tab "Synchronization"

Parameter	Meaning
Synchronization type	Not synchronized: The device does not participate in the synchronized data exchange. If this option is selected, no further settings can be made for the synchronization. Sync master: The device is working as sync master. Sync slave: The device is working as sync slave.

Table 4.28 Parameters in the tab “Synchronization” *(continued)*

Parameter	Meaning
Name of sync domain	If the synchronization type “Sync master” has been selected, the name of the sync domain in which the device is working as sync master is displayed here. The name of the sync domain can be changed in the context menu under “Profinet IO Domain Management...”.The default name of the sync domain is “Sync domain”.
RT class	Selection/display of the real-time class with which the cyclic data are to be transmitted. RT: RT protocol (RTC 1) IRTflex: IRT protocol (RTC 2) IRTtop: IRT protocol (RTC 3)

Table 4.29 Parameters in the tab “Time-of-Day Synchronization”

Box	Meaning
NTP procedure	The Network Time Protocol (NTP) is the implementation of a TCP/IP protocol for time synchronization in networks. The NTP procedure uses hierarchical time synchronization. In this case an external time source, for example a PC in the network, is used for synchronization. With the NTP procedure, the module sends time queries to all configured NTP servers at regular intervals. The most reliable and exact time is determined using the responses from the servers, and the module time synchronized. The advantage of this procedure is that time synchronization is possible beyond the limits of subnetworks. Switch on time synchronization in NTP procedure: If this option is selected, the time is synchronized using an NTP server specified under NTP addresses. NTP server addresses: The addresses of previously configured NTP servers are displayed in this box. The output is as an IPv4 or IPv6 address or as a DNS name. Use the “Add” button to add the addresses of up to four NTP servers. Use the “Edit” button to change a selected address. Use the “Delete” button to delete a selected address. Updating interval: The updating interval for time synchronization is specified in this box.

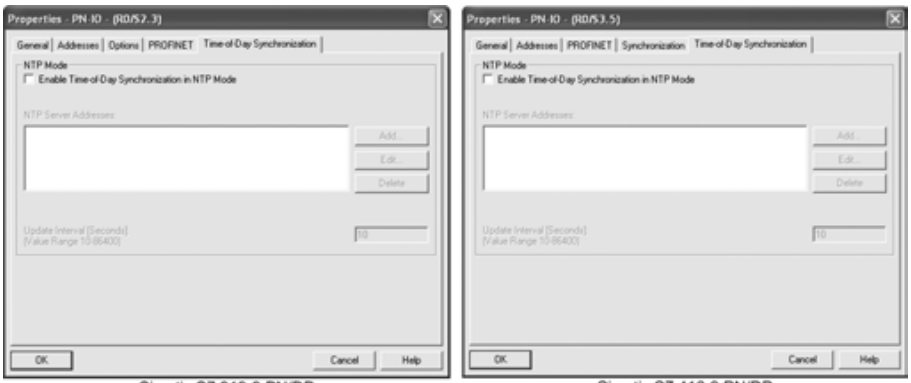


Fig. 4.28 Setting of Time-of-day synchronization with Simatic S7

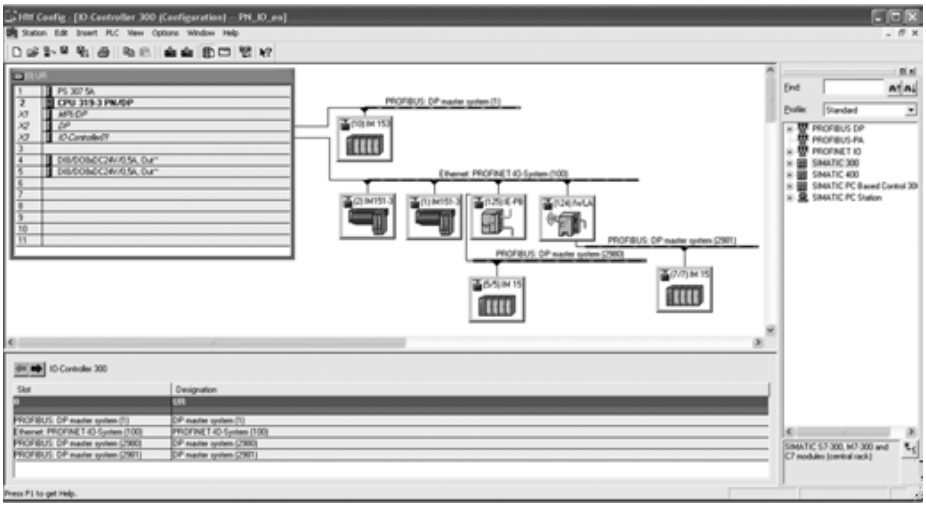


Fig. 4.29 Profinet IO System in HW-Config

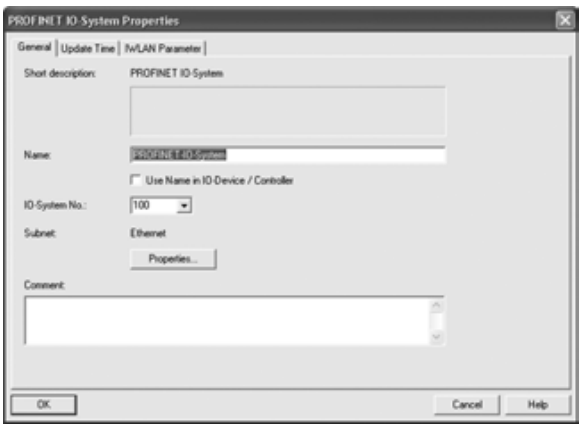


Fig. 4.30
General settings of Profinet IO Systems

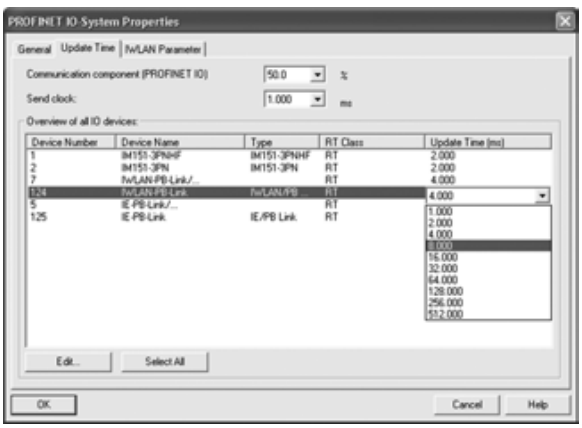


Fig. 4.31
Setting the update time with Profinet IO Systems

Table 4.30 Parameters in the tab “General”

Parameter	Meaning
Short Designation	Preset short designation for Profinet IO Systems.
Name	Configurable name of Profinet IO System.
Use Name in IO Device/Controller	Optional possibility for automatic extension by the engineering system of the name of the Profinet IO System as a component of the device name. The device name of the IO Controller, for example, has the format: [Name from short designation].[Name of IO System]
IO System No.	Number of Profinet IO System. The permissible numbers commence at 100 since smaller numbers are used as range identifications, e.g. with SFC 71 “LOG_GEO”.
Subnet	Name of subnet to which the Profinet IO System is assigned. Using the button “Properties”, it is possible to modify the subnet properties, to create a new subnet, or to select a different subsystem.
Comment	Comment on the Profinet IO System.

Table 4.31 Parameters in the tab “Update Time”

Parameter/box	Meaning
Communication Component (Profinet IO)	If the module is to be used simultaneously for cyclic data exchange over Profinet IO and Profinet CBA, the share of Profinet IO communication in the total communication is defined here. With a setting of 100%, the available capacity is reserved exclusively for Profinet IO data exchange. The communication component for acyclic data exchange (e.g. PG access/IO Supervisor) need not be explicitly considered at this point since a sufficiently large time share is already reserved for the system. This setting can also be made in the context menu of the IO Controller.
Send clock	The send clock is the period between two successive intervals for IRT or RT communication. The send clock is the smallest possible send interval for data exchange. The calculated updating times are a multiple of the send clock. If the IO Controller is working as a sync slave or sync master, Step 7 indicates the send clock which has been selected in the dialog “Domain Management” (tab “Sync-Domain”). If the IO Controller is not working as a sync slave or sync master, the send clock is set here. This setting can also be made in the context menu of the IO Controller.
Overview of all IO Devices	The update times of the IO Devices are calculated from the hardware configuration, the resulting quantity of cyclic data, the module properties and the communication share for Profinet IO. An IO Device is provided with new data by the IO Controller within the updating time, and sends its updated data to the IO Controller. Updating times can only be configured in specific intervals. The possible values are defined in the GSD files of the IO Devices. Device number: Display of configured device number of an IO Device. Device name: Display of configured device name of an IO Device. Type: Display of device type of an IO Device. RT class: Display of configured real-time class (RTC) for cyclic data transmission. Update time: Display of calculated or configured update time.

Table 4.31 Parameters in the tab "Update Time" *(continued)*

Parameter/box	Meaning
Overview of all IO Devices *(continued)*	IO Devices without user data (example: Simatic Net IE/PB Link) are identified by an asterisk (*). It is possible that no updating time could be calculated. This is the case, for example, if the limits for the number of cyclic user data/frames or the available time intervals have been exceeded, or if no common basis could be found for the send/receive interval. In such cases, the updating time is not displayed.

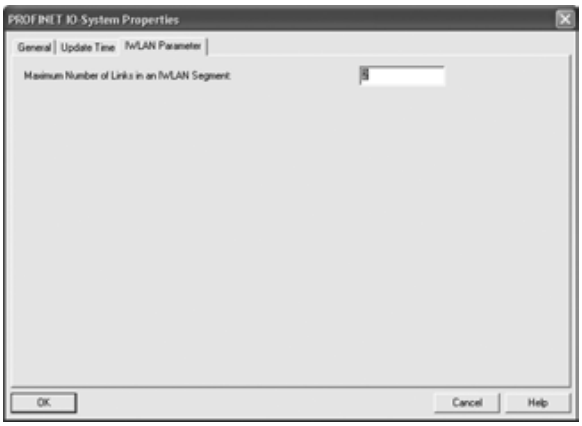


Fig. 4.32 Setting of IWLAN parameters with Profinet IO Systems

Table 4.32 Parameters in the tab "IWLAN Parameters"

Parameter	Meaning
Maximum Number of Links in an IWLAN Segment	If part of the Ethernet subnet consists of a radio network (IWLAN: Industrial Wireless LAN), the cyclic data exchange between IO Controllers and IO Devices takes place over a radio link. Fixed access points are installed at one end of the radio link, and mobile stations at the other (example: Simatic Net IWLAN/PB Links with DP slaves). If the radius of action of the mobile stations is large, it may be necessary to install several access points. Each access point with its radio range constitutes a segment, and an IWLAN can be designed using a number of segments. If several mobile stations are present within a segment, they must share the bandwidth available for radio transmission. The update time is increased in such a case.

Configuration of IO Devices

Selection and arrangement of IO Devices in HW-Config is carried out similar to Profibus DP. Prior to insertion, a Profinet IO System must be present and visible in the station window.

IO Devices process the section "Profinet IO" in the hardware catalog (see Fig. 4.33). They are coupled to an IO System using drag&drop or a double-click. If a

modular IO Device is involved, the required modules must be subsequently configured into the IO Device.

The symbolic representation of IO Devices in the station window is oriented according to the representation of DP slaves on the Profibus. The symbol displays the device number and name (possibly shortened).

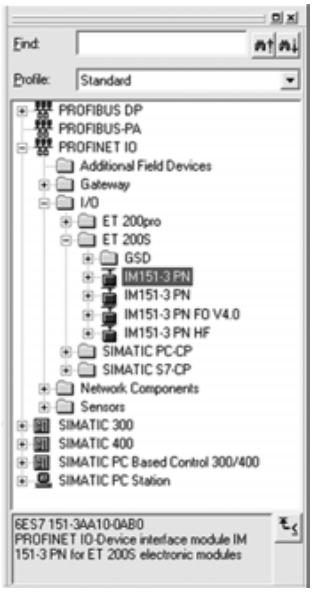


Fig. 4.33 IO Devices in the hardware catalog

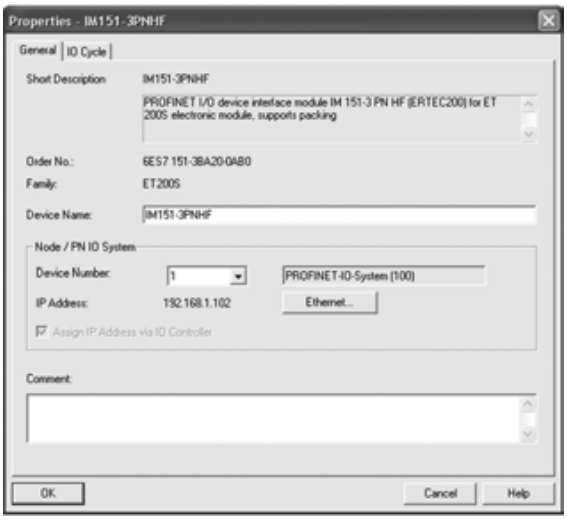


Fig. 4.34
General settings of an IO device

Table 4.33 Parameters in the tab “General”

Parameter	Meaning
Short Description	Short designation of the IO Device.
Order No.	Order No. of device.
Family	Name of device family.
Device Name	Unambiguous device name on the Ethernet subnet which complies with the DNS conventions. Device names are assigned to the Profinet IO Devices during the commissioning phase. The default setting is the name from the GSD file (see “Short description”). With integral Profinet interfaces, the device name is derived from the short description. If several devices of the same type are arranged in the same Profinet IO System, Step 7 automatically supplements the name from the GSD file with a serial number. The second device is assigned the extension “-1”, the third device the extension “-2” etc.
GSD file	Optional: Name of GSD file used by Step 7 to represent the IO Device and its properties. If several GSD files with different versions or releases are present in the Step 7 data management, the device with the latest GSDML schema version or the latest release is always embedded in the hardware catalog. Using the button “Change release number” it is possible to interactively access other versions or releases of the GSD files, permitting e.g. configuration of “preceding devices”.
Node/PN IO system	Device number: Unambiguous number of the IO Device which, in contrast to the device name, is visible in the user program. It can be applied there (e.g. with SFC 71 “LOG_GEO”) to identify the device. The associated IO System is displayed in addition to the device number. The name and number of the Profinet IO System can be modified using the properties dialog of the Profinet IO System. IP address: The IP address for the IO Device is usually assigned automatically by Step 7, based on the IP address of the IO Controller. This implicitly configured IP address is downloaded to the IO Controller together with the hardware configuration. The IO Controller assigns this IP address to the IO Device during startup. Assign IP address via IO Controller:Activated: the IO Device is assigned its IP address by the IO Controller during startup. Not activated: the IO Device must obtain its IP address from a device other than the IO Controller, for example from a DHCP server. Both the IO Controller and the IO Device must support this mechanism. Ethernet: This button is used to call the dialog for parameterization of the Ethernet interface. The IP address of the IO Device can also be changed here.
Comment	Comment on the IO Device.

Table 4.34 Parameters in the tab “IO cycle”

Parameter	Meaning
Update time	Display of calculated or configured update time.
Number of accepted update cycles with missing IO data	Violation of the watchdog time results in a fault reaction similar to that with a Profibus system (switching of outputs to safe state). To allow adaptation in problematical cases, the default number of accepted update cycles with missing IO data can be changed. This can make sense, for example, during the commissioning phase.
Watchdog time	The watchdog time is calculated from “Update time” × “Number of accepted update cycles with missing IO data”. The maximum watchdog time is 1.92 seconds.

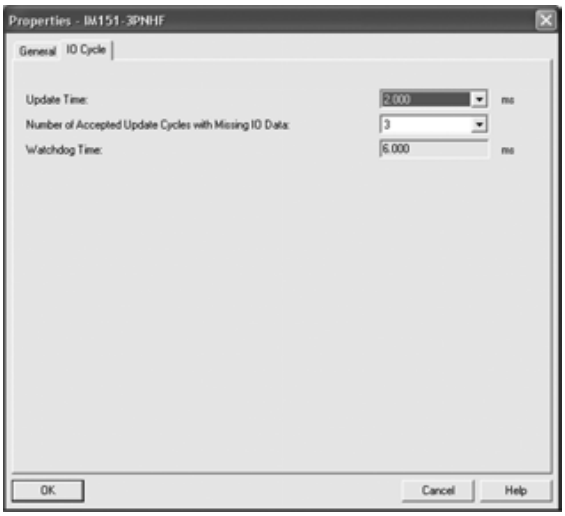


Fig. 4.35
Setting the IO cycle of an IO Device

Configuration of the Simatic Net IE/AS-I Link PN IO gateway and the Simatic PN/PN Coupler

Configuration of the Simatic Net IE/AS-I Link PN IO gateway and Simatic PN/PN coupler parameters which are relevant to Profinet is basically carried out as with an IO Device.

Configuration of the Simatic Net IE/PB Link PN IO and IWLAN/PB Link PN IO gateways

A gateway allows integration of distributed I/O devices of other fieldbus systems. It works as a router between two types of network, and allows these I/O devices to appear like an IO Device to the IO Controller.

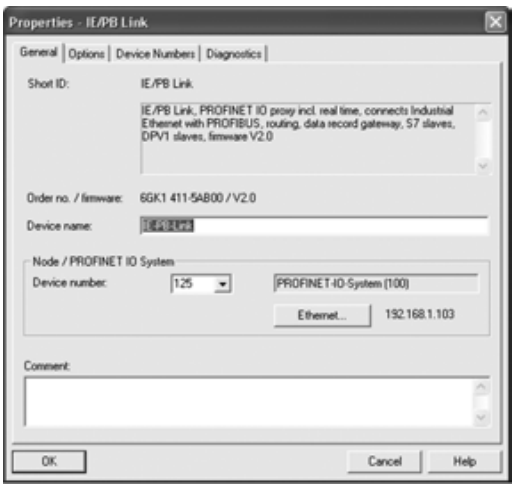


Fig. 4.36
General settings of the Simatic Net IE/PB Link PN IO and IWLAN/PB Link PN IO gateways

Table 4.35 Parameters in the tab "General"

Parameter/box	Meaning
Short ID	Short description of the gateway.
Order No./firmware	Order No. and firmware of the gateway.
Device name	Unambiguous device name on the Ethernet subnet complying with the DNS conventions.
Node/Profinet IO System	Device number: Unambiguous number of the IO Device which, in contrast to the device name, is visible in the user program. It can be used there (e.g. with SFC 71 "LOG_GEO") to identify the device. The associated IO System is displayed in addition to the device number. The name and number of the Profinet IO System can be changed in the properties dialog of the Profinet IO System. Ethernet: This button is used to call the dialog for parameterization of the Ethernet interface. The IP address of the gateway can also be entered here.
Comment	Comment on the gateway.

The DP slaves are addressed by the IO Controller like an IO Device using the Profinet IO device number. The device numbers, which are initially assigned automatically, can be changed in the tab *Device Numbers*.

When positioning DP slaves on the DP master system, Step 7 attempts to assign the same value to the device number and the Profibus address. If an identical assignment is not possible, a value which is still vacant is assigned to the device number. It may be the case that device numbers are occupied by further IO Devices connected on the PN IO System.

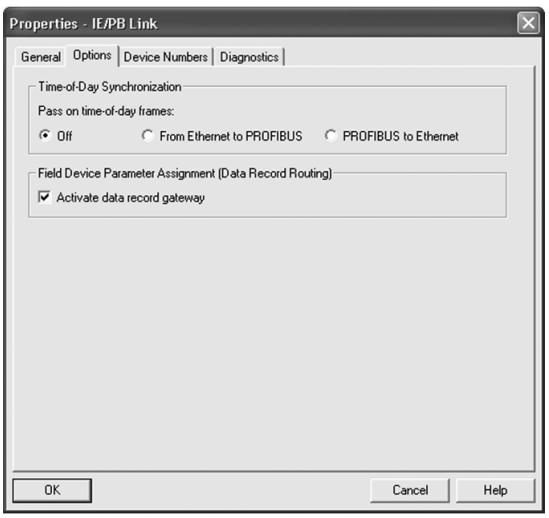


Fig. 4.37
Setting the options of the Simatic Net IE/PB Link PN IO and IWLAN/PB Link PN IO gateways

All assigned device numbers must be unambiguous within a Profinet IO System. Repeatedly used device numbers may occur, for example, if a Profibus address is reassigned and if automatic tracking of the device number is activated. Unambiguous assignment of numbers can be guaranteed by using the consistency test provided by HW-Config.

Table 4.36 Parameters in the tab "Options"

Parameter	Meaning
Time-of-Day Synchronization	Possibility for setting whether the IE/PB-Link is to pass on time-of-day frames from a clock transmitter or not. Possible directions: Off: Time frames are not passed on From Ethernet to Profibus: Passing on of time frames from Ethernet to Profibus. Profibus to Ethernet: Passing one of time frames from Profibus to Ethernet. If this option is switched on, IE/PB-Link also accepts the time sent by the clock transmitter for time stamping of entries in the diagnostics buffer. An internal system clock is otherwise used.
Field Device Parameter Assignment (Data Record Routing)	The IE/PB-Link can be used as a router for records directed to field devices (DP slaves). This means that tools or devices which are not directly connected on the Profibus can nevertheless transmit records to the Profibus field devices. The Simatic PDM (Process Device Manager) is an example of a tool which generates such records for parameterization of field devices. The function is switched on as standard, but requires additional memory resources. The option can be switched off if the resources of the IE/PB-Link are already under high load because of the configuration (connections etc.) or if data record routing is not required.

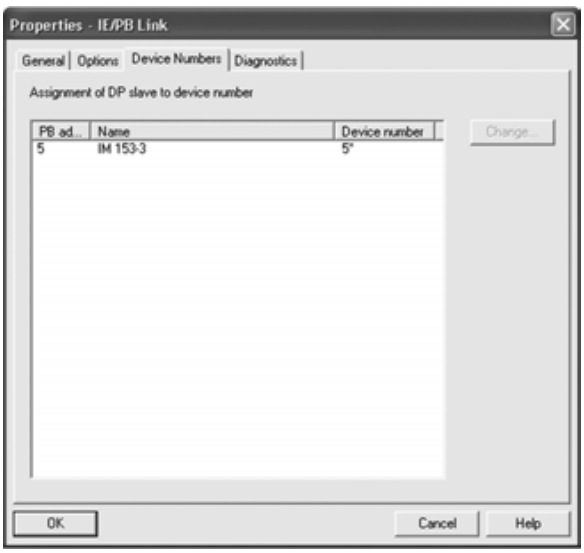


Fig. 4.38
Settings of device numbers of DP slaves with the Simatic Net IE/PB Link PN IO and IWLAN/PB Link PN IO gateways

Table 4.37 Parameters in the tab "Device Numbers"

Parameter	Meaning
Assignment of DP slave to device number	PB adr.: Profibus address which was defined in the properties dialog of the DP slave. Name: Device name which was defined in the properties dialog of the DP slave. The device name for the DP slaves has no further significance for the identification as a Profinet IO Device. The device number is decisive. Device number: Device number of Profinet IO Device, in this case of the DP slave as Profinet IO Device. "*" means that tracking of the device number on the basis of the Profibus address has been preset for this DP slave. A change to the Profibus address of the DP slave thus automatically results in adaptation of the device number to the new Profibus address.

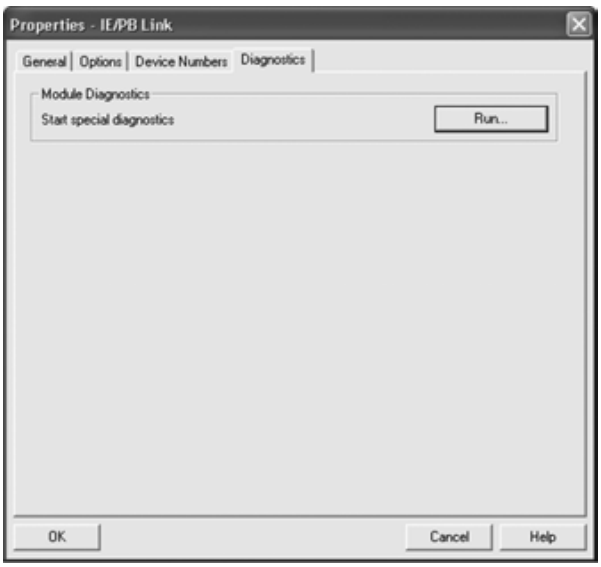


Fig. 4.39
Calling the special diagnostics of the Simatic Net IE/PB Link PN IO and IWLAN/PB Link PN IO gateways

Table 4.38 Parameters in the tab "Diagnostics"

Parameter	Meaning
Module Diagnostics	Starting of diagnostics: The NCM-S7 diagnostics for the Simatic Net IE/PB-Link PN IO is called by clicking the button "Execute". The NCM S7 diagnostics provides dynamic information on the status of the communications functions of modules connected online. In order to carry out the diagnostics, it must be guaranteed that the Simatic Net IE/PB-Link PN IO is accessible to the engineering PC via the network.

Assignment and checking of IP addresses

In addition to the automatic assignment of IP addresses, Step 7 also supports manual assignment. It is therefore meaningful to check all assigned IP addresses at the end of the configuration procedure. It is important that each IP address is unique. Furthermore, it must be present within the permissible IP addresses band.

A window can be called in the context menu of the Profinet IO System under “Edit Profinet IO System IP addresses...” in which Step 7 provides an overview of all configured IP addresses of a Profinet IO System. Duplicate IP addresses are marked in color, and can then be changed.

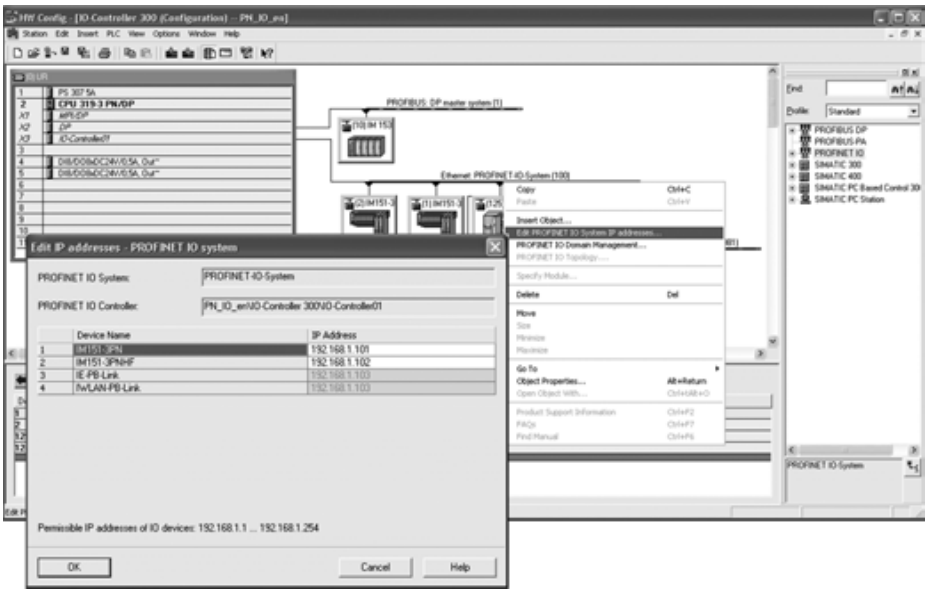


Fig. 4.40 Assignment and checking of IP addresses

Configuring a sync domain

A sync domain (PTCP subdomain) is a group of Profinet devices synchronized to a common clock. One device has the role of the sync master (clock master), all other devices have the role of a sync slave (clock slave).

Table 4.39 Parameters in the tab "Sync domain"

Box	Meaning
Sync Domain	Sync-Domain: Selection of the sync domain to be edited. New/delete/edit: Create/delete/edit a sync domain. The sync domain (default) cannot be deleted. Send clock (µs): Setting of the send clock for the selected sync domain. The send clock is the period between two successive intervals for IRT or RT communication, and thus the smallest possible send interval. The calculated update times for Profinet devices are a multiple of the send clock. From the Profinet devices connected to the Ethernet subnet, Step 7 automatically determines all possible send clocks supported by the Profinet devices. Details: Display of reserved bandwidths for the various communication components within a send clock and facility for adjusting the ratio IRT_{top}/IRT_{flex} within the IRT channel.
Nodes	Station/IO System: Display of all stations within the selected sync domain as well as the relative Profinet IO System. Add/remove: Add/remove stations to/from the selected sync domain. All stations which are not used anywhere else are assigned to the sync domain (default), and cannot be deleted from the sync domain. Station/device name: Display of all Profinet IO Devices within the selected station. Synchronization type: Display of synchronization mode configured for the Profinet IO Device. RT class: Display of RT class configured for the Profinet IO Device. Device Properties: Display/modification facility for synchronization settings of the selected Profinet IO Device.
Modules	If the selected sync domain is an IRTtop sync domain, the objects which can be addressed within the sync domain (e.g. modules or areas for direct data exchange) are displayed following clicking of the button.

Table 4.40 Parameters in the window "Details", tab "Sync Domain"

Box	Meaning
IRT_{top}/IRT_{flex}	Reserved share: Share of IRT communication in total communication. The reserved share may be greater than the calculated share. Calculated share IRT_{top}: Time for IRT_{top} communication calculated by Step 7. Calculated share IRT_{flex}: Time for IRT_{flex} communication calculated by Step 7.

Table 4.40 Parameters in the window "Details", tab "Sync Domain" *(continued)*

Box	Meaning
RT/NRT	Reserved share: Share of RT/NRT communication in total communication. The reserved share may be greater than the calculated share. Calculated share RT: Time for RT communication calculated by Step 7. Bandwidth NRT: Time for NRT communication (TCP/IP) calculated by Step 7.

Fig. 4.41 Parameters in the window "Device properties", tab "Synchronization"

Table 4.41 Parameters in the window “Device properties”, tab “Synchronization”

Box	Meaning
Parameter	Name of sync domain: Name of sync domain to which the Profinet device is assigned. The assignment can be changed here if the Profinet device is a sync master. Device name: Name of Profinet device. Station: Station name in the Step 7 project in which the Profinet device is configured. IO System: Name of Profinet IO System to which the Profinet device is assigned. Synchronization type: Not synchronized The device does not participate in the synchronized data exchange. If this option is selected, no further settings can be made for the synchronization. Sync master: The device is working as sync master. Sync slave: The device is working as sync slave. RT class: Selection/display of real-time class with which the cyclic data are to be transmitted. RT: RT protocol (RTC 1). IRTflex: IRT protocol (RTC 2). IRTtop: IRT protocol (RTC 3).

Definition of the IRT topology

The extremely exact synchronization intervals when using IRT necessitate consideration of the line lengths between the communication partners and the associated delay times. These delays can be determined using the IRT Topology Editor.

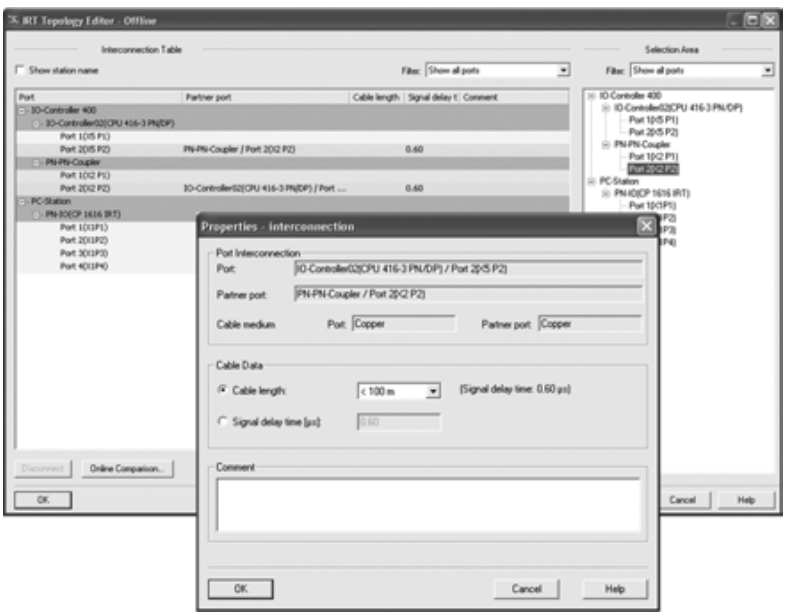


Fig. 4.42 IRT Topology Editor

Table 4.42 Parameters in the window "Properties – interconnection"

Box	Meaning
Port Interconnection	Port: The name of the local port in the format Station/Device/Port. Partner port: The name of the remote port in the format Station/Device/Port. Cable medium: Port: Copper or fiber-optic Partner port: Copper or fiber-optic
Cable Data	Cable length: Length from which the signal delay time is calculated. Copper: 20 m / 100 m Fiber-optic: 100 m / 500 m / 1000 m / 2000 m Calculation of the signal delay time from the cable length is only possible if the cable media of the communicating ports are identical. Otherwise the signal delay time must be specified. Signal delay time: Signal delay time between two communicating ports. Value range: 0.01 ... 99999.99 s Input of the signal delay time is necessary, for example, if a media converter is used or if cable lengths exist other than those selectable.
Comment	Comment on the interconnection

One possibility for accessing the editor is by using the menu item "Profinet IO Topology"; it is called in the context menu of the Profinet IO System.

The editor allows clear linking of the ports of Profinet IO Devices of the Profinet IO System with IRT capability. The line data can subsequently be specified in the properties dialog of a link. The data present following completion of the topology configuration flow together with the configuration data of the total plant into the calculation of the update time.

Assignment of IP address to an IO Controller

Prior to the first loading, an IO Controller does not generally possess an IP address. In order to be able to access it on the network, it must therefore be initially assigned an unambiguous IP address as well as IP parameters (Fig. 4.43).

Fig. 4.43
Assignment of PG/PC interface

In order to make these assignments, the IO Controller must be accessible online, in other words:

- The Ethernet interface of the Step 7 engineering computer must be accessible to Step 7/NCM PC. For this purpose, the access point for the IE module must be set to S7ONLINE in the window “Assign PG/PC interface”.
- The IO Controller and the Step 7 engineering computer must be connected to the Ethernet.
- The IO Controller must be connected to the same Ethernet subnet as the Step 7 engineering computer.

The assignment of an IP address can also be carried out in HW-Config using the menu item “Assign Ethernet address”.

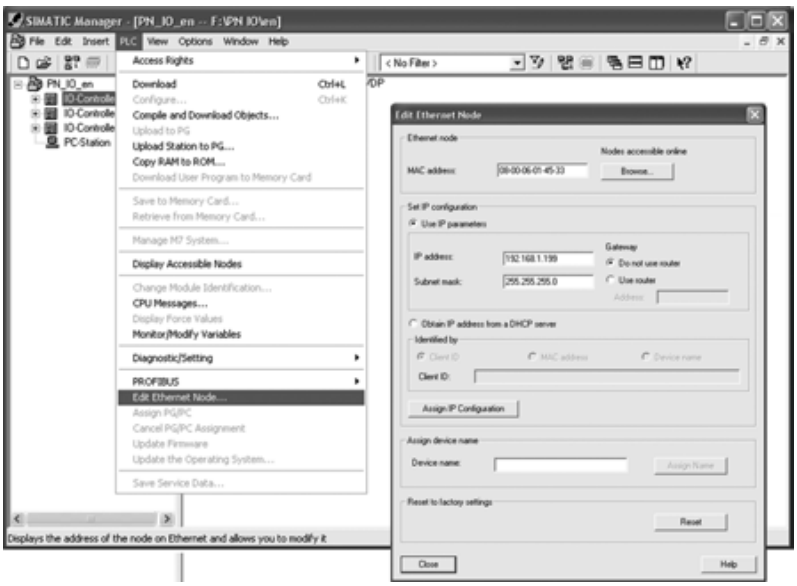


Fig. 4.44 Assignment of IP address in the Simatic Manager

Table 4.43 Parameters in the dialog “Edit Ethernet Node”

Parameter	Meaning
Ethernet node	MAC address: The Ethernet address of the device to be set is entered in the format aa-bb-cc-dd-ee-ff. Nodes accessible online: If the Ethernet address is unknown, the Ethernet subnet connected to the engineering computer can be searched for accessible stations by clicking the button “Browse”. Note: If switches with VLAN capability are present in the communications path to the Ethernet nodes, it must be guaranteed that frames with the VLAN tag = 0 are actually passed on and not rejected. In the latter case, an existing Ethernet node is not recognized.

Table 4.43 Parameters in the dialog "Edit Ethernet Node" *(continued)*

Parameter	Meaning
Set IP configuration	Use IP parameters: If the dialog has been selected in the context of a selected module, the IP address is preassigned the values configured for the module. Otherwise the IP address and subnet mask are entered here. Gateway: Do not use router: select this option if device communication is only to be carried out in the own IP subnet. Use router: Select this option if the device communicates with devices (also engineering) in IP subnets other than the own IP subnet. In this case, "Address" must be the IP address of the network card of the router which is in the same IP subnet as the device. Obtain IP address from a DHCP server: If this option is selected, the device obtains its IP address from a DHCP server. Depending on the selected option, the DHCP server is provided with the MAC address of the CP, the device name or the client ID for this purpose. The client ID is a string with a maximum of 63 characters. If the IP address is to be determined by the DHCP server using the device name, a name must have been previously assigned to the device. Assign IP Configuration: By clicking this button, the IP configuration is transmitted to the Ethernet node. If the Ethernet subnet has previously been browsed using "Nodes accessible online", a warning is output prior to assignment of the configuration if the assigned IP address already exists in the Ethernet subnet.
Assign device name	Device name: Unique device name on the Ethernet subnet complying with DNS conventions. Assign name: By clicking this button, the specified device name is transmitted to the Ethernet node.
Reset to factory settings	Reset: By clicking this button, the device is reset to the factory settings. The IP address and the configuration data are then deleted. Further information on resetting/overall resetting can be found in the device manual.

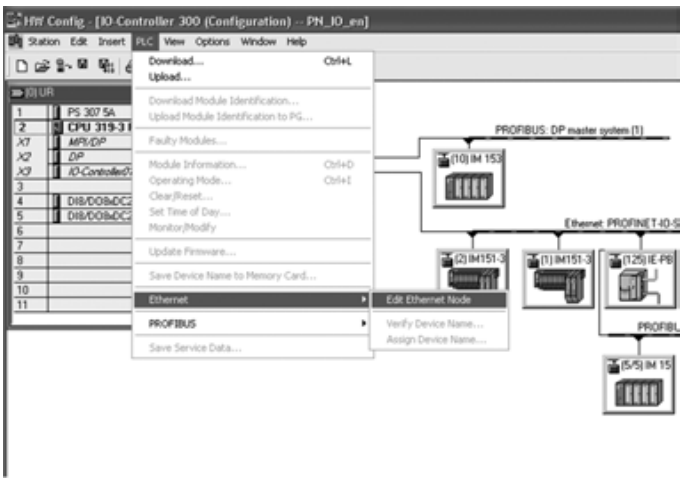


Fig. 4.45 Assignment of IP address in HW-Config

Assignment of device name

To permit IO Devices to be parameterized by an IO Controller during the system startup, they require an unambiguous device name. This name is assigned during configuration of the IO Devices in HW-Config and transferred from there to the IO Devices. Fig. 4.46 and Table 4.44 clarify the sequence for assigning a name.

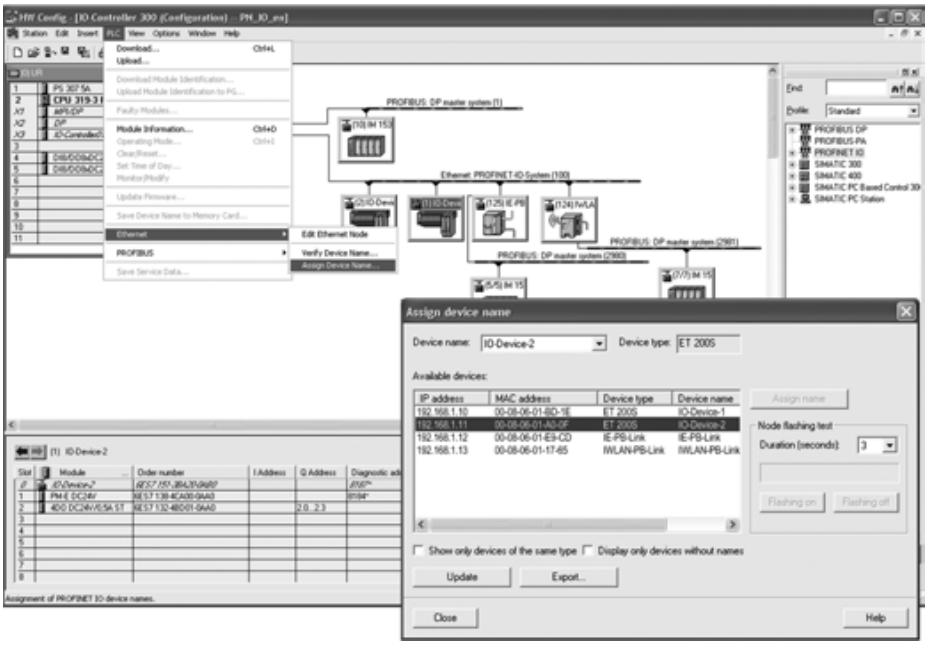


Fig. 4.46 Assignment of device name in HW-Config

Table 4.44 Parameters in the dialog window “Assign device name”

Parameter	Meaning
Device name	Name to be assigned to the selected device.
Device type	Type of IO Device
Available devices	IP address: IP address of device, if already assigned. MAC address: MAC address of device. This is usually already assigned by the vendor. Device type: Type of device, e.g. ET 200S Device name: Name of device, if already assigned.
Display only devices of the same type	Filter facility for suppressing certain types of device.
Display only devices without names	Filter facility for suppressing already named devices.

Table 4.44 Parameters in the dialog window “Assign device name” *(continued)*

Parameter	Meaning
Node flashing test	The flashing test permits identification of a reachable device provided the device supports this function. The corresponding device can be recognized by the flashing LINK LED. Duration (seconds): Duration of flashing (3 s to 60 s, adjustable in 3-second steps). “Flashing on”/“Flashing off”: The function is triggered by clicking the button “Flashing on”. The LED then flashes, and can be stopped using “Flashing off”.
Assign name	On clicking the button, the selected device name is transmitted to the IO Device.
Update	On clicking the button, the Ethernet subnet is searched again, and the list “Available devices” updated.
Export	Saving of list of “Available devices” as CSV file (CSV: character separated values).

Verification of device names

If a device name has been assigned to the IO Devices, correct assignment of the names can be subsequently verified using the function “Verify Device Name” (see Fig. 4.47 and Table 4.45).

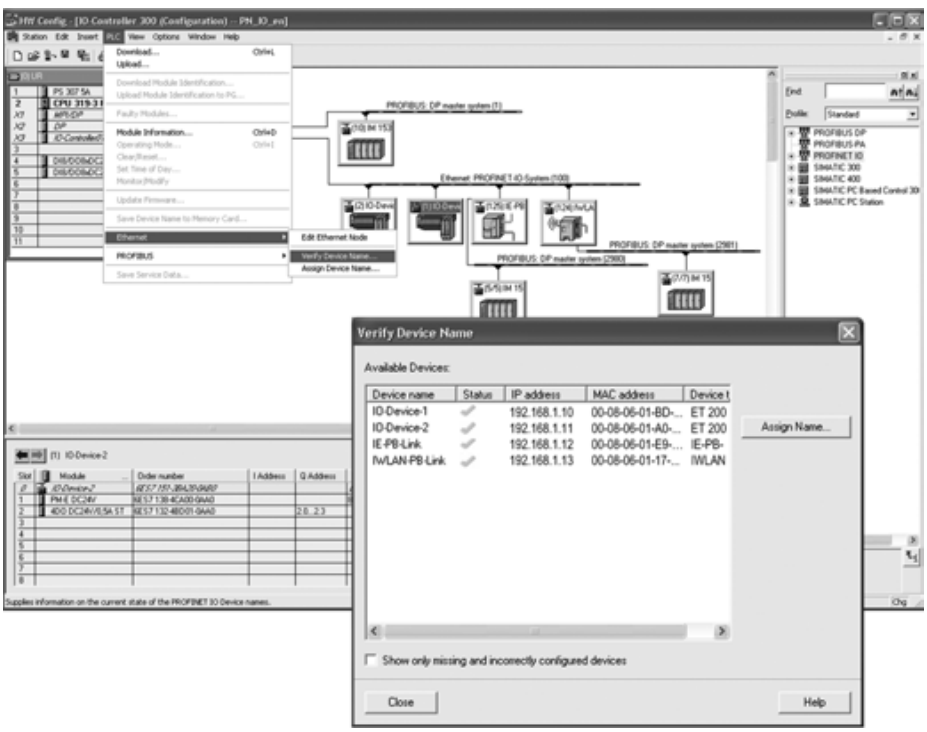


Fig. 4.47 Verification of device names in HW-Config

Table 4.45 Parameters in the dialog window "Verify Device Name"

Parameter	Meaning
Available Devices	The device names are displayed together with additional information of all IO-Devices which were previously selected in HW-Config. Device name: Name of device, if already assigned. Status: Green tick: a device with the configured name exists, and the type corresponds to the configured IO Device. Red cross: a device with the configured name exists, but the type does not correspond to the configured IO Device. In this case, the type determined online is also displayed. If no device with the configured name has been found, only the status (X) is displayed for the device name. IP address: IP address of device, if already assigned. MAC address: MAC address of device.
Show only missing or incorrectly configured devices	Filter facility for suppressing correctly configured devices.
Assign Name	Clicking this button starts the dialog "Assign device name".

Generation of the user program

The distributed I/O connected to a Simatic S7 system is handled like centralized I/O from the viewpoint of the user program. Profinet IO is no different in this respect to Profibus DP. The user program is generated as with Profinet DP.

Further information on program generation and new features and expansions when using Profinet IO can be found in Chapter 6.

Downloading of the configuration and user program

The configuration is downloaded before the user program. The configuration data are downloaded from HW-Config into the IO Controller. The configuration must be consistent, and the IO Controller must be accessible on the Ethernet subnet.

During the startup, the IO Controller distributes the IP address and the parameterization data to the IO Devices assigned to it, establishes all required connections to the IO Devices, and then commences with the cyclic data exchange.

Following successful testing of the plant, the configuration phase is concluded by documenting and archiving of the project.

4.2.3 Operation of Plant

Replacement of parts with Simatic Net Profinet devices

Many Simatic Net Profinet devices possess a replaceable configuration plug (referred to briefly as C-Plug). The C-Plug is present at the front (F) or rear (R) of a device. Examples of devices with C-Plug are:

- Simatic Net Profinet CP 343-1 (only IO Controller) (R)
- Simatic Net Profinet CP 443-1 Advanced (R)
- Simatic Net router IE/PB Link PN IO (R)
- Simatic Net router IWLAN/PB Link PN IO (F)
- Simatic Net Scalance S security module (R)
- Simatic Net Scalance X Switches of the X-200 and X-400 ranges (R)

The C-Plug provides non-volatile saving of the configuration and programming data of the respective device. On an unwritten C-Plug (factory states), all required configuration data are automatically saved during the device startup. If the configuration is changed during runtime, the data saved on the C-Plug are automatically updated without interfering with operation and without an operator intervention. Simply by replacing the C-Plug when a spare part is required, all data can be transferred to the replacement unit without using the engineering system (Fig. 4.48).

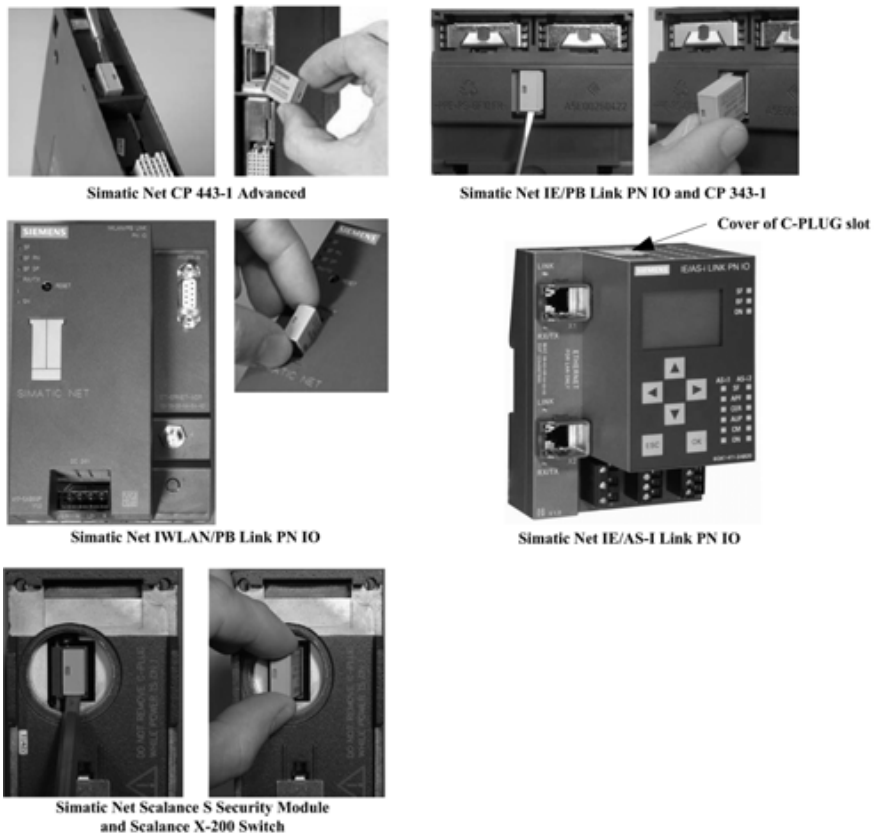


Fig. 4.48 Replacement of the C-PLUG on Simatic Net Profinet devices

Replacement of parts on Simatic S7 IO Controller and IO Devices

The MMC (multi media card) of Simatic IO Devices contains their device name and, in the case of Simatic S7 IO Controllers, also the IP address and user program. Following insertion of the MMC into a replacement device, this is automatically provided with the correct configuration data which are also required for the startup. The MMC is usually positioned on the front or rear panel behind a flap (Fig. 4.49).

Fig. 4.49
Distributed I/O module
Simatic ET 200S IM 151-3 PN HF

4.3 Diagnostics Functions for Profinet IO

The diagnostics concept supported by Profinet IO is comparable with that of Profibus DP. All diagnostics facilities already available with Step 7 for Profibus DP components can also be used for Profinet IO. The procedure is identical (see Table 4.46).

Table 4.46 Profinet IO diagnostics facilities

Diagnostics facility ...	Diagnostics facility through ...	Application
In Step 7 or NCM PC	Online diagnostics with a PG, PC or HMI device	Evaluation of the current device status, reading of identification and maintenance data (I&M data).
In the user program of the IO Controller	Reading of system status lists	Locating of faults.
	Reading of diagnostics records	Determination of detailed information on type and source of a fault. Reading of I&M data.
With network components	Network management functions with SNMP	Diagnostics of network infrastructure.
On the Profinet device	LED displays	Checking for communication faults and data transmission.

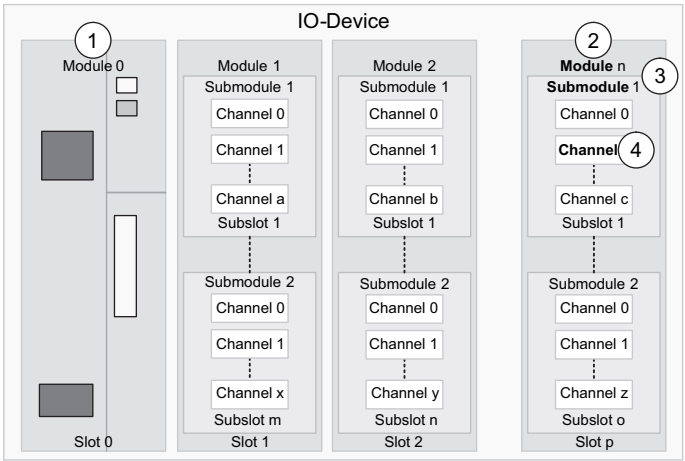


Fig. 4.50
Diagnostics levels

Table 4.47 Diagnostics levels

Level	Meaning
1	Fault in device, e.g. valve terminal 2
2	Fault in module, e.g. analog input module n
3	Fault in submodule
4	Fault in channel, e.g. open-circuit in channel 1

Profinet IO Devices are diagnosed together with Simatic S7 stations and Profibus DP slaves in HW-Config. Diagnostics information can be evaluated at four levels, as shown in Fig. 4.50 and Table 4.47.

4.3.1 Identification and Maintenance Data (I&M Data)

I&M data is information saved in a module which can be used for the following tasks:

- Checking of the plant configuration
- Locating of hardware changes in a plant
- Elimination of faults in the configuration of a plant.

Identification data (I data) contain information on the module, e.g. Order No. and serial number. I data is vendor-specific and read-only.

Maintenance data (M data) contain information on use of the module, e.g. location and installation date. M data is plant-specific, and is created during the configuration and written to the module. The I&M data can be used to unambiguously identify modules online.

Table 4.48 List of I&M data

I&M data	Length	I&M record	Meaning
MANUFACTURER_ID	2 bytes	I&M0	Vendor identification (Siemens: 2Ah)
ORDER_ID	20 bytes	I&M0	Order No. of module
SERIAL_NUMBER	16 bytes	I&M0	Serial number of module
HARDWARE_REVISION	2 bytes	I&M0	Hardware version of module
SOFTWARE_REVISION	4 bytes	I&M0	Firmware version of module
REVISION_COUNTER	2 bytes	I&M0	Reserved
PROFILE_ID	2 bytes	I&M0	Profile ID
PROFILE_SPECIFIC_TYPE	2 bytes	I&M0	Profile-specific coding
IM_VERSION	2 bytes	I&M0	Version of I&M data
IM_SUPPORTED	2 bytes	I&M0	I&M records supported by the module
TAG_FUNCTION	32 bytes	I&M1	Plant-wide unique identification of module
TAG_LOCATION	22 bytes	I&M1	Module location
INSTALLATION_DATE	16 bytes	I&M2	Installation date and time
DESCRIPTOR	54 bytes	I&M3	Comment on module
SIGNATURE	54 bytes	I&M4	Security code

Functions for accessing I&M data (I&M functions) are an integral part of S7 components. In Step 7, the I&M data are displayed in the tabs “Module status” and “Properties” of the respective module. HW-Config permits input of M data for modules (e.g. in dialog boxes during configuration).

The structure of I&M data has been defined in the “Profibus Guideline Profile Guidelines Part 1: Identification & Maintenance Functions”. A new addition with Profinet IO is standardization of access in accordance with IEC 61158-6.

I&M data are combined in I&M records. The record I&M0 must be supported by a module. The other I&M records are optional.

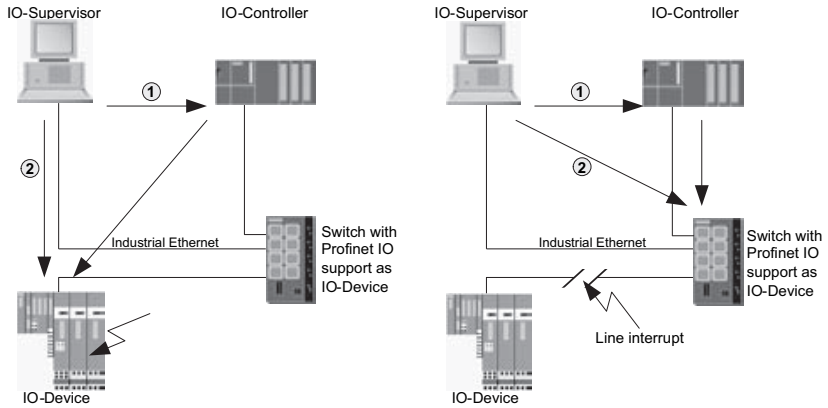
4.3.2 Diagnostics with Step 7 and NCM

Individual or simultaneously occurring faults are transmitted from the IO Device to the IO-Controller. Alternatively, the complete status of an IO Device including the faults still present can be directly read out of the IO Device.

Switches which support Profinet IO (e.g. Simatic Net Scalance X200/400) are configured in HW-Config like an IO Device and diagnosed accordingly (Fig. 4.51).

Table 4.49 provides an overview of the diagnostics facilities available in Step 7.

Different symbols are used to display device statuses and diagnostics. Diagnostics symbols are displayed in the online window of the project as well as in the window of the hardware configuration with the online view of configuration tables. Diagnostics symbols facilitate troubleshooting, and provide a rapid overview of whether diagnostics is available or not (see Table 4.50).



1: The IO Supervisor (PG, HMI) requests the station status of the IO Device.
Following triggering by the IO Supervisor, the IO Controller automatically reads the complete station status from the IO Device/Switch in asynchronous mode, and stores the read diagnostics information in system status lists (SSL) in the IO Controller. The IO Supervisor accesses these SSLs.

2: The IO Supervisor (PG/HMI) reads the station status directly from the IO Device/Switch independent of the IO Controller. In this manner, diagnostics information can be read during the commissioning phase or in the event of servicing even without the IO Controller being ready.

Fig. 4.51 Diagnostics using a Step 7 or HMI device

Table 4.49 Diagnostics facilities in Step 7

Function	Information
Simatic Manager, online view	Overview of the current status of the system (including configuration information): Call in the Simatic Manager: Menu command: View > Online
HW-Config, online view	Hardware diagnostics: Overview of the current status of the system (including configuration information): Call in HW-Config: Menu command: Station > Open online
Available stations	List of Profinet devices available on the Ethernet subnet.
Diagnostics view and quick view	Display of an overview of faulty modules: Quick view: Display of IO Controller and faulty modules. Diagnostics view: Display of all modules. Selection of fast view or diagnostics view as standard setting: Menu command: Target system > Diagnostics/settings > Hardware diagnostics.
Module information	I&M and diagnostics information: The scope of displayed information depends on the selected module and whether the function has been called from the window "Available stations" or from a project window.
Operating state	Display of operating state of a CPU module, and possibility for changing this. Operating states: Warm restart / Cold restart / Hot restart / Stop.
Step 7-NCM	NCM software integrated in Step 7 for diagnostics of Simatic Net modules. The NCM diagnostics is called using the properties dialog of a Simatic Net module or from Windows using: Start > Programs > Simatic > Step 7 > NCM S7 > Diagnostics.

Table 4.50 Symbols for representation of device statuses and diagnostics

Symbol	Meaning
	Diagnostics: deviation between expected value and actual value of configuration. The configured CPU does not exist, or the inserted CPU does not correspond to the configured one.
	Diagnostics: CPU or a module parameterized by the CPU is faulty. Possible causes: detection of a diagnostics interrupt.
	Diagnostics: diagnostics is not possible because an online connection does not exist or because no diagnostics information could be determined.
	CPU is in startup mode.
	CPU is in STOP mode.
	CPU is in STOP mode, triggered by STOP mode of another CPU in multi-computing mode.
	CPU is in RUN mode.
	CPU is in hold mode.
	CPU signals maintenance request.
	CPU signals maintenance requirement.
	Diagnostics: deviation between expected value and actual value of configuration. The configured CP is missing, or the inserted CP does not correspond to the configured one.
	CP is faulty.
	CP is in STOP mode.
	CP is in RUN mode.
	Diagnostics: diagnostics is not possible because an online connection does not exist or because no diagnostics information could be determined.
	An interface or port signals a maintenance request.
	An interface or port signals a maintenance requirement.

Simatic Manager – online view

A complete overview of the current status of the system including the configuration information is possible in the online view of the Simatic Manager. This is called in the Simatic Manager using the menu command View > Online (Fig. 4.52).

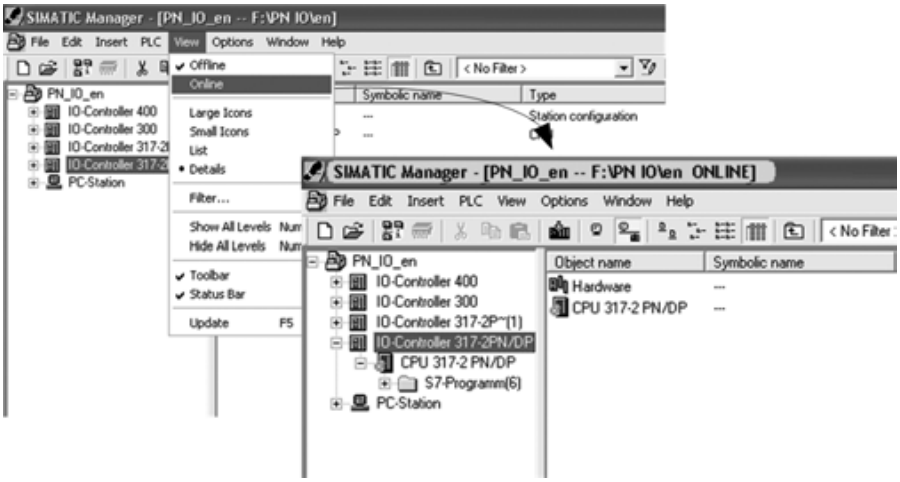


Fig. 4.52 Simatic Manager in the online view

HW-Config – offline view: signal system fault

"Signal system fault" is a convenient way of displaying the diagnostics information provided by the IO Controller in the form of messages. The diagnostics function is used as with Profibus DP.

The blocks and message texts required to use this function are automatically generated by Step 7. They only have to be downloaded by the user into the CPU, and the texts transmitted to the connected HMI devices.

"Signal system fault" supports the components of S7-300 and S7-400 stations, IO Devices, DP slaves and Simatic WinAC as long as these provide functions such as diagnostics interrupt, insert/remove module interrupt, and channel-specific diagnostics.

The following types of fault are displayed in plain text for IO Devices:

- Fault of the IO Device (failure, return)
- Module fault (module removed, incorrect module, compatible module)
- Channel fault
- Fault in integrated Profinet interface of an IO Device.

HW-Config – online view

The second possibility for determining the current status of the complete system is offered by the online view of HW-Config. This is opened in HW-Config using the menu command Station > Online (Fig. 4.53).

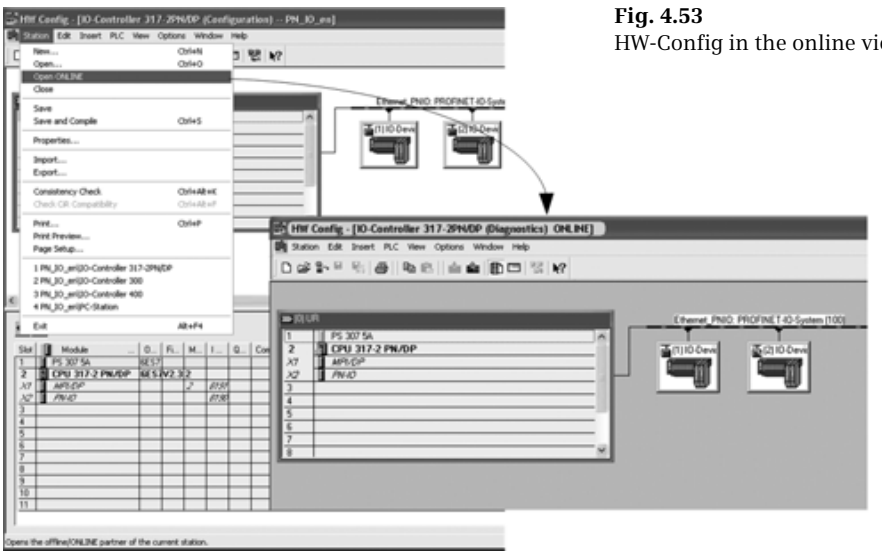


Fig. 4.53
HW-Config in the online view

Table 4.51 Types of module displayed with the function “Available stations”

Available stations, types of module	Object name	Meaning
Profinet IO device with assigned name	Device name	The IP and MAC addresses can be determined using the properties dialog. The view “Details” also displays the type of device.
Profinet IO device without assigned name	IP address, if assigned, otherwise MAC address	
Simatic Net-IE/PB-Link	As for Profinet IO device	As for Profinet IO device Special feature: if the Simatic Net-IE/PB-Link is selected in the list of available stations, the detailed view displays the connected DP slaves with their Profibus address as well as further information.
Simatic Net communications processor	Station name, if assigned, otherwise MAC address	Operating status and module type are also displayed in the view “Details”.
Simatic S7 CPUs, Simatic PC stations	Station name	Operating status, module type and, if present, information from the associated Step 7 project (station name, CPU name, plant identifier), are also displayed in the view “Details”.
Stations without DCP protocol support	–	–

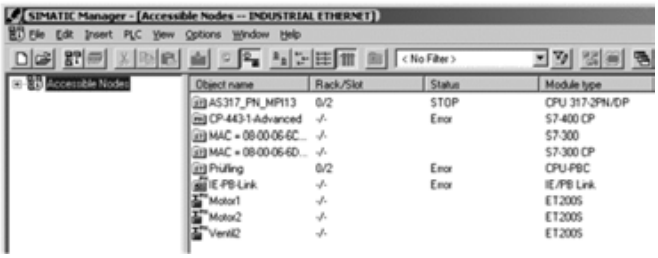


Fig. 4.54
Example: available stations

The following are displayed:

- Simatic Net communications processors,
- Simatic S7 CPUs,
- Simatic PC stations,
- Simatic Net network components,
- Simatic Net-IE/PB Link router with its subordinate DP slaves, and
- all devices which can handle the DCP protocol.

Information functions "Diagnostics view" and "Quick view"

The information function "Quick view" provides an overview of the faulty modules. The view comprises the following information (Fig. 4.55):

- Data on the online connection to the CPU
- Diagnostics symbol for the CPU
- Diagnostics symbols for modules where a fault has been detected by the CPU (e.g. diagnostics interrupt, I/O access error)
- Module type
- Address of faulty module (rack, slot, DP master system with station number, Profinet IO System).

When calling the information function "Diagnostics view" – in contrast to the quick view – the complete station configuration which can be accessed online is output with the following information:

- Configuration of racks
- Diagnostics symbols for all configured modules
- Status of the respective module
- Operating status of CPU modules
- Module type
- Order No.
- Address data
- Comments on configuration.

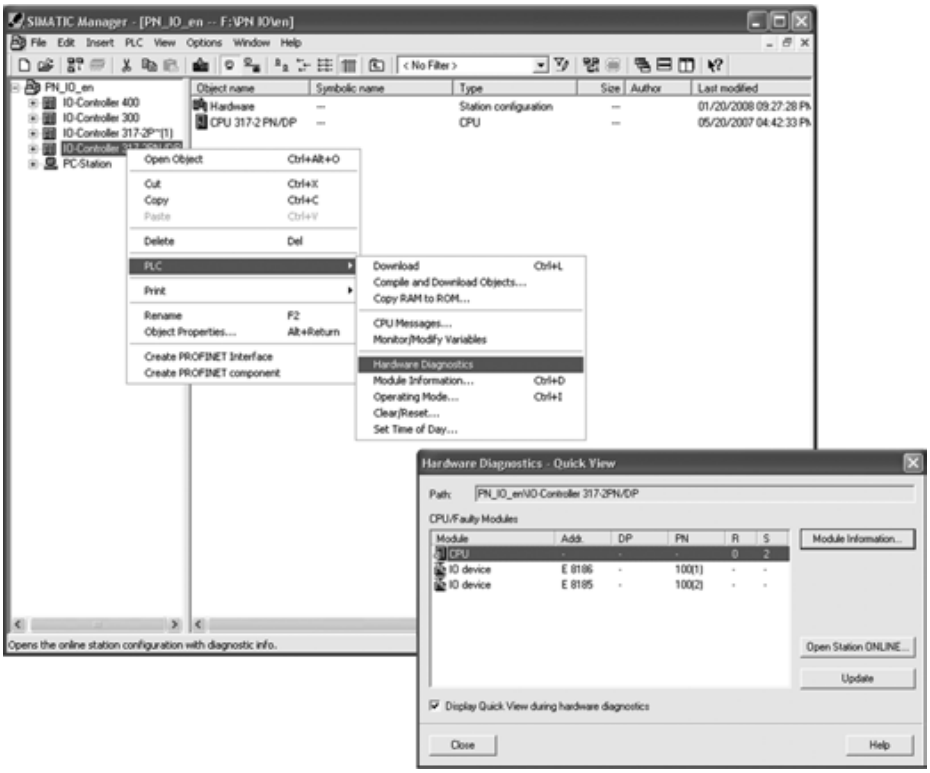


Fig. 4.55
Information function “Module Information” in the online view of the Simatic Manager

Information function “Module Information”

This information function permits the output of module-specific status data on several tags. Only the tags relevant to the respectively selected module are displayed (Figs. 4.56 and 4.57, Table 4.52).

Table 4.52 Tags of the information function “Module Information”

Register	Information	Application
General	General data for the selected module: Module description System identification Name/device name Version Rack IO system Diagnostics address Profibus address (with DP slaves) SlotDevice number System status Plant designation Location designation	The online information of the inserted module can be compared with the data of the configured module.

Table 4.52 Tags of the information function "Module Information" *(continued)*

Register	Information	Application
Diagnostics buffer	Overview of events in the diagnostics buffer as well as detailed information on the selected event.	For evaluation of the cause of a CPU STOP, and also for evaluation of previous events on the selected module. The diagnostics buffer means that system errors can still be evaluated after a longer period in order to determine the cause of a STOP or to be able to trace and assign the occurrence of individual diagnostics events.
DP slave diagnostics	Diagnostics data of selected DP slave (according to EN 50170).	For determination of the cause of a DP slave fault.
IO Device diagnostics	Diagnostics data of selected IO Device.	For determination of the cause of an IO Device fault.
Memory	Memory configuration, current loading of RAM, load memory and retentive memory, data of selected module.	Checking of whether sufficient load memory is available. Compression of memory contents.
Cycle time	Duration of the longest, shortest and last cycles of the selected CPU or M7-FM.	For checking the parameterized minimum cycle time as well as the maximum and current cycle times.
Time system	Current time, operating hours, and information on clock synchronization (synchronization intervals).	For displaying the time and date of a module, and for checking the time synchronization.
Performance data	Operand ranges and the available blocks of the selected (CPU/FM) module.	Prior to and during the generation of a user program, and to check whether the CPU provides the requirements for execution of a user program, e.g. with respect to size of the process image.
	Display of all types of block available in the functional scope of the selected module. List of OBs, SFBs and SFC which can be used in this module.	Checking of which standard blocks may contain or call your user program in order to execute on the selected CPU.
Communication	Transmission rates of communications interfaces, maximum available connection resources, configured cycle loading through communication.	Determination of how many connections, and which, are possible or occupied on the module.
Stacks	Register stacks: can only be opened in the STOP or HOLD status. The B stack of the selected module is displayed. In addition, the I stack, L stack and nesting stack can be read, and it is possible to jump to the error position of the interruption block.	Determination of cause of a transition to STOP, and for correction of a block.
Identification	I&M data of the module.	Reading of the configured I&M data.

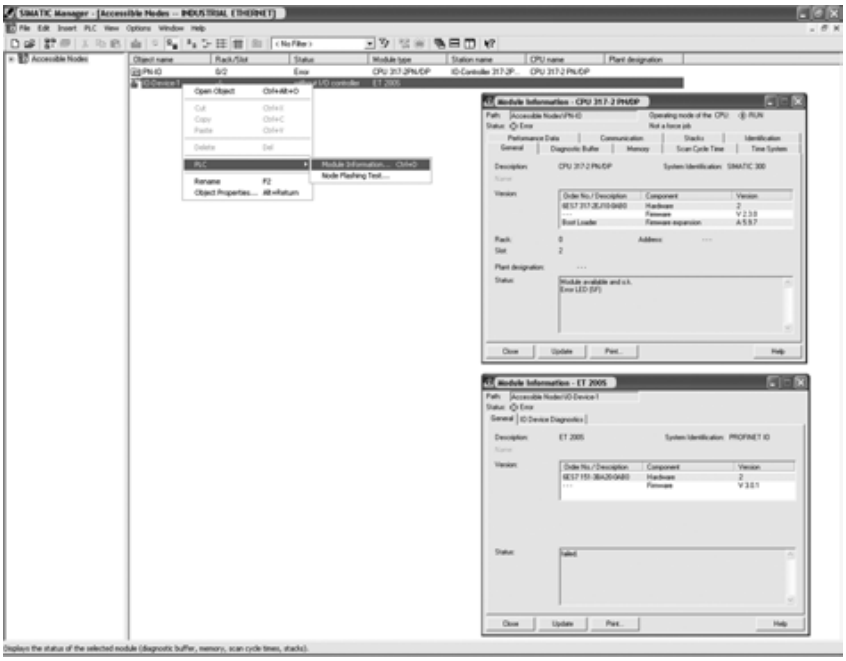


Fig. 4.56
Information function “Module Information” in the online view of the Simatic Manager

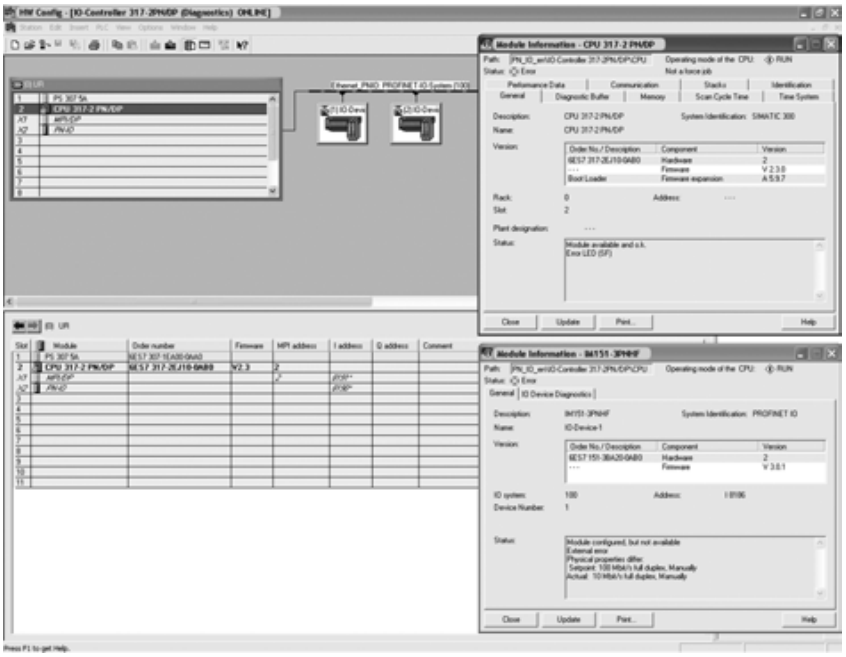


Fig. 4.57 Information function “Module Information” in the online view of HW-Config

4.3.3 Diagnostics in the User Program of the IO Controller

Evaluation of diagnostics information using system function blocks (SFB) and system functions (SFC) in the user program is similar to that with Profibus DP. Profinet IO defines a cross-vendor structure for records with diagnostics information. This information is only generated for faulty channels. Two different paths basically exist for receiving diagnostics information.

Status-based diagnostics

All individual errors are collected in a record on the header module. A complete overview of the status of the Profinet IO System is provided e.g. by the system status list SSL 0x0A91. This SSL provides a complete overview of the existing IO subsystems. The SSL with the SSL-ID W#16#0694 permits localization of faulty stations within an IO subsystem. A fault can be localized further to a module or submodule using the SSL-IDs W#16#xD91 and W#16#0696. SSLs are read using the system function SFC 51 “RDSYSST”.

The system function block SFB 52 “RDREC” reads diagnostics records directly from a faulty module. The result is the detailed description of the current module status (Fig. 4.58).

There are two different types of diagnostics records:

- Channel diagnostics records
- Vendor-specific diagnostics records.

Channel diagnostics records are displayed if a channel exhibits a fault and/or has triggered an interrupt. If a fault is not present, the returned diagnostics record has a length of 0. A maximum of 400 channel faults can be displayed at one time.

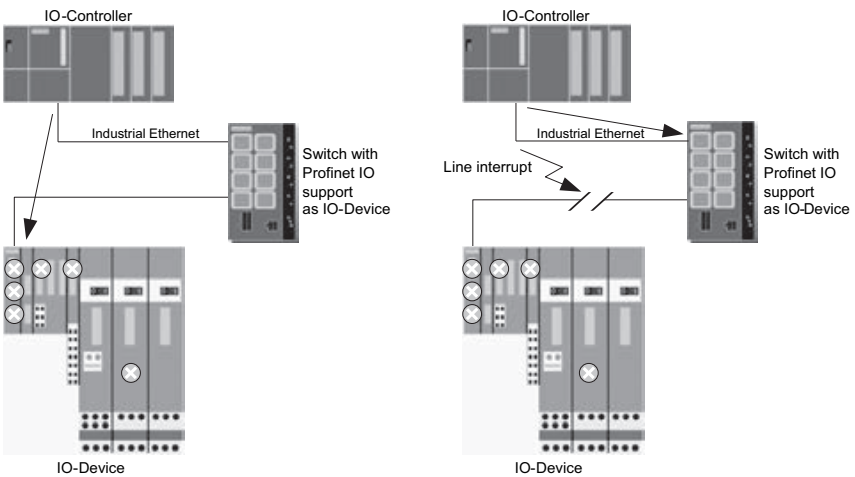


Fig. 4.58 Evaluation of the diagnostics status

The structure and size of the vendor-specific diagnostics records depend on the vendor. The corresponding information can be found in the GSD file of the device.

Event-based diagnostics

Each fault is sent individually to the IO Controller as channel diagnostics in the form of an interrupt.

The module status data are updated automatically in the IO Controller. A fault organization block (fault OB) is started in the user program of the IO Controller. Using the OB number and the OB start information, initial statements are already possible on the cause and location of the fault.

The system function block SFB 54 “RALRM” called in the OB reads the interrupt synchronously from the IO Controller without addressing the IO Device. Detailed evaluation of the interrupt is possible in this manner (Fig. 4.59).

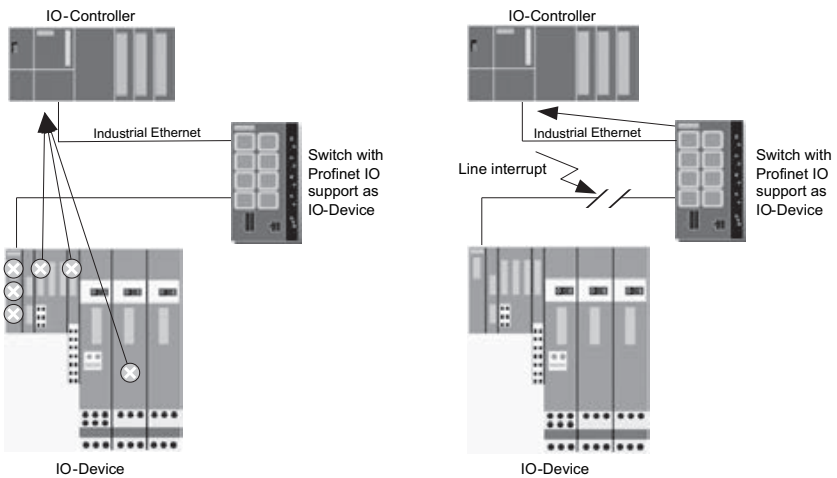


Fig. 4.59 Evaluation of interrupts

4.3.4 Network Diagnostics with SNMP

The Simple Network Management Protocol (SNMP) is a standardized protocol based on UDP for management and monitoring of network components mainly from the LAN sector. The primary targets of SNMP are reduction in the complexity of management functions and transparent exchange of information and data between various network components. SNMP is supported in office applications and in automation engineering by Ethernet network components from many different vendors.

SNMP works according to the client/server model. A so-called SNMP agent is executed on the administered device. This handles the device’s management informa-

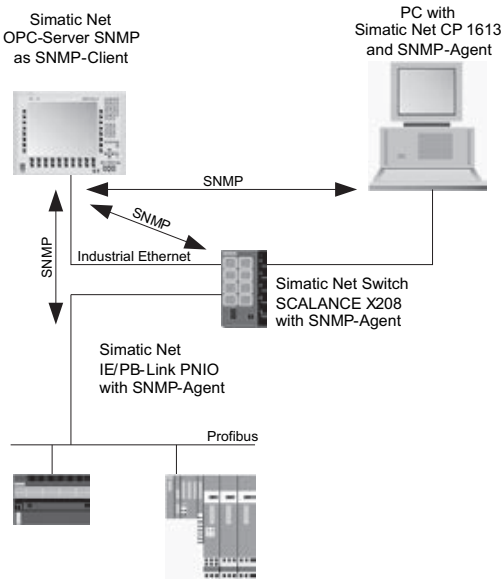


Fig. 4.60
Plant configuration with network management using SNMP

tion. Its pendant is an SNMP client, for example a Simatic Net-SNMP-OPC server which collects the data and makes them available in a conditioned form.

SNMP clients and agents send requests and responses to a special network address. Each SNMP request from an SNMP client results in a response from each SNMP agent which has received the request. An SNMP client polls the management data from the SNMP agent using SNMP requests, or receives event-based data (traps) from an SNMP agent (Fig. 4.60).

The components of a device which can be accessed by the SNMP agent or which can modify an SNMP agent are referred to as SNMP objects. The totality of all SNMP objects of a device are saved in a database, the management information base (MIB). The objects are therefore often referred to as MIB objects. The size and scope of the MIB depend on the devices. For example, a switch has more SNMP objects than a Simatic Net-CP 1616.

Information on the properties of SNMP-capable Simatic Net devices is saved in so-called MIB files. More detailed information on handling MIB files can be obtained from the documentation of the respectively used SNMP client.

4.3.5 Diagnostics on the Display Elements of Profinet IO Devices

The status of the device and that of its communications interfaces can be determined using the LED display elements on the front of a Simatic S7 or Simatic Net Profinet IO device. The LEDs enable initial diagnostics in the event of a fault (Table 4.53).

The LED display elements of Simatic S7 Profinet IO devices are divided into two groups (Tables 4.54 to 4.57):

- General status and fault displays
- Status displays for the communications interfaces.

It is generally applicable that the RX/TX LED displays whether data are being transmitted over Ethernet. If an Ethernet connection exists, it flickers at different rates depending on the load. The two LEDs can also be combined into one. If the LEDs are permanently, this means that the Ethernet connection is interrupted.

Table 4.53
General tips for fault locating using the BUSF/BF2 LED with Simatic S7 Profinet IO devices

BUSF/BF2	Meaning	
1	General: Communication over Ethernet is faulty. OB 86 is called in the case of Simatic S7-CPU Profinet IO Controllers if the CPU is in the RUN status. If the OB is not loaded, the CPU enters the STOP status.	
	Bus fault (no physical connection to a subnet/switch).	Check bus cable for short-circuit or open-circuit.
	Incorrect transmission rate.	Check whether the module is actually connected to a switch and not to a hub.
	Full-duplex transmission is not activated.	Check whether data transmission is carried out at 100 Mb/s and with full duplex.
0/1	IO Controller: Communication over Ethernet is faulty. OB 86 is called in the case of Simatic S7-CPU Profinet IO Controllers if the CPU is in the RUN status. If the OB is not loaded, the CPU enters the STOP status.	
	Failure of a connected IO Device.	Check whether the Ethernet cable is connected on the failed IO Device or whether the communications link to the IO Device is interrupted.
	At least one of the higher-level IO Devices cannot be addressed.	Wait for CPU startup. If the LED does not stop flashing, check the IO Devices or evaluate the IO Device diagnostics.
	Incorrect configuration.	Check whether the configured device name agrees with the actual name assigned to the IO Device.
0/1	IO Device:	
	The response monitoring time has expired.	Check the module.
	Bus communication over Profinet is interrupted.	Check whether the communications link to the IO Controller is interrupted.
	IP address is incorrect, or incorrect configuration, or incorrect parameterization.	Check the configuration and parameterization.
	IO Controller not present or switched off, but Ethernet connection exists.	Switch on IO Controller, or check the communications link to the IO Controller.
	Incorrect or faulty device name.	Check whether the expected configuration corresponds to the actual configuration, and whether the configured device name agrees with the device name actually assigned to the IO Device.

0: off, 1: on, 0/1: flashes, x: indefinite

Display elements of the Simatic S7 CPU 31x-y PN/DP

Table 4.54 General LED status and fault displays of the CPU 31x-y PN/DP

SF red	DC5V green	FRCE yellow	RUN green	STOP yellow	Meaning
0	0	0	0	0	CPU without power supply.
0	1	x	0	1	CPU is in STOP status.
1	1	x	0	1	CPU is in STOP status. The STOP status has been triggered by a fault.
x	1	x	0/1	1	2 Hz: CPU is in startup status. 0.5 Hz: CPU is in hold status.
x	1	x	1	0	CPU is in RUN status.
1	1	x	x	x	Hardware or software fault. The CPU's diagnostics buffer must be read to permit exact fault locating.
x	x	1	x	x	Force order active.
x	x	0/1	x	x	2 Hz: The function "Node flashing test" is active (with CPU with FW of V2.2.0 or later)
x	1	x	0	0/1	2 Hz: complete reset active. 0.5 Hz: request complete reset.
0/1	0/1	0/1	0/1	0/1	Internal system fault.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.55
LED status display of communications interfaces of the CPU 31x-2 PN/DP

BF1 red	BF2 red	LINK green	RX/TX yellow	Meaning
0	x	x	x	All DP slaves configured on the Profibus DP interface X1 are exchanging data.
1	x	x	x	Bus fault on the Profibus DP interface X1. Possible causes: – Bus fault (interruption/short-circuit) – Fault in the DP interface – Different baud rates in multi-DP master mode – Bus short-circuit (with active DP slave interface or DP master mode) – Searching for baud rate (with passive DP slave interface).
0/1	x	x	x	Bus fault on the Profibus DP interface X1. Possible causes: With DP master mode: – Failure of a connected station – At least one of the assigned DP slaves cannot be addressed – Incorrect configuration With operation as active DP slave: – Response timeout – Bus communication is interrupted – Incorrect Profibus address – Incorrect configuration.
x	0	x	x	All IO Devices configured on the Profinet interface X2 are exchanging data.

Table 4.55
LED status display of communications interfaces of the CPU 31x-2 PN/DP *(continued)*

BF1 red	BF2 red	LINK green	RX/TX yellow	Meaning
x	1	x	x	Fault on the Profinet interface. Communication is no longer possible (e.g. with a CPU as IO Controller if the connection to the switch is interrupted). Possible causes: – No physical connection to a subnet or switch – The IP address is present more than once in the subnet – No IP address has been configured – Incorrect transmission rate (≠ 100 Mb/s) – Full duplex transmission is not active.
x	0/1	x	x	Fault on the Profinet interface (e.g. with station failure of one or more IO Devices). Possible causes: – Failure of a connected IO Device – At least one of the assigned IO Devices cannot be addressed – Incorrect configuration.
x	x	0	x	There is no connection to the Ethernet. Possible causes: – There is no connection to the switch – Negotiation of the baud rate (autonegotiation) was not successful.
x	x	1	x	A connection to the Ethernet exists. Negotiation of the baud rate (autonegotiation) was successful, and the baud rate required for Profinet IO communication was accepted.
x	x	x	0	No data are currently being transmitted over the Profinet interface.
x	x	x	0/1	Data are currently being transmitted over the Profinet interface.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.56 LED status display of communications interfaces of the CPU 319-3 PN/DP

BF1 red	BF2 red	BF3 red	LINK green	RX/TX yellow	Meaning
0	x	x	x	x	See Table 4.55, response of LED BF1
1	x	x	x	x	See Table 4.55, response of LED BF1
0/1	x	x	x	x	See Table 4.55, response of LED BF1
x	0	x	x	x	As for BF1
x	1	x	x	x	As for BF1
x	0/1	x	x	x	As for BF1
x	x	0	x	x	See Table 4.55, response of LED BF2
x	x	1	x	x	See Table 4.55, response of LED BF2
x	x	0/1	x	x	See Table 4.55, response of LED BF2
x	x	x	0	x	See Table 4.55, response of LED LINK
x	x	x	1	x	See Table 4.55, response of LED LINK
x	x	x	x	0	See Table 4.55, response of LED RX/TX
x	x	x	x	0/1	See Table 4.55, response of LED RX/TX

Display elements of the Simatic DP ET 200S IM151-3 PN, IM151-3 PN HF and IM 151-3 PN FO, PN/PN coupler

Table 4.57 General LED status and fault displays of the IM151-3 PN, IM151-3 PN HF, IM 151-3 PN FO and PN/PN coupler

SF red	BF red	ON green	Meaning
0	0	0	No voltage is present on the interface module/PN/PN coupler, or a hardware fault is present on the interface module/PN/PN coupler.
x	x	1	Voltage is present on the interface module/PN/PN coupler.
x	0/1	1	0.5 Hz: Incorrect connect frame, or none at all, received by the IO Controller. No data exchange is taking place between the IO Controller and the IO Device. The IO Device is physically connected to the switch. Possible causes: – An incorrect device name was assigned. – A configuration error is present. – The IP address has been assigned more than once. – A programming or parameterization error is present. – Response timeout. – The IO Controller is switched off, faulty, or the bus cable to the IO Controller is interrupted.
x	1	1	No connection to the switch. Possible causes: – The IO Device is not connected to a switch. – The assembly of the FO cable is poor. – Attenuation of FO cables too high.
1	x	1	The configured structure of the interface module/PN/PN coupler does not agree with the actual structure. Possible causes: – At least one configured module/submodule is not present. – At least one incorrect module/submodule is inserted. – At least one module/submodule has been removed. – At least one module/submodule is faulty or broken. – Parameterization of at least one submodule was unsuccessful. – Starting of diagnostics. In addition with the PN/PN coupler: – Voltage monitoring PS1+PS2 has been configured, but only one power supply is connected, or a power supply has failed.
1	0	1	Interface module/PN/PN coupler not accessible. Possible causes: – An S7 program is not present on the Simatic MMC. – A Simatic MMC is not inserted. – The inserted Simatic MMC is full, or has too little space for the device name. – A suitable MMC is not inserted (i.e. not a Simatic MMC).
1	1	1	The Simatic MMC is being formatted.
0	0	1	Data exchange is taking place between the IO Controller and the interface module/PN/PN coupler. The expected and actual configurations of the interface module/PN/PN coupler agree.
1	1	0	Firmware update being carried out.
0	0/1	0	0.5 Hz: Firmware update executed successfully.

Table 4.57 General LED status and fault displays of the IM151-3 PN, IM151-3 PN HF, IM 151-3 PN FO and PN/PN coupler *(continued)*

SF red	BF red	ON green	Meaning
1	0/1	0	0.5 Hz: An external fault has occurred when loading the firmware. Possible causes: An attempt was made to load incorrect firmware. 2 Hz: An internal fault has occurred when loading the firmware. Possible causes: A read/write error occurred when loading the firmware.
0/1	0/1	0/1	Module or system error. In this case, the interface module/PN/PN coupler must be switched off and on again.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.58 LED status display of communications interfaces of the IM151-3 PN, IM151-3 PN HF, IM 151-3 PN FO and PN/PN coupler

FO yellow	LINK green	RX/TX yellow	Meaning
0/1	0	0	No connection to the switch/IO Controller.
0/1	1	x	The IO Controller is accessible in the network. A connection exists to the Ethernet. Negotiation of the baud rate (autonegotiation) was successful, and the baud rate required for Profinet IO has been accepted.
x	1	0	The port is not sending or receiving any data over the Ethernet.
x	1	0/1	The port is sending or receiving data over the Ethernet.
1	1	x	Maintenance requirement/maintenance request: Possible cause: The attenuation by the FO cable is already so strong that operation will soon no longer be possible.

0: off, 1: on, 0/1: flashes, x: indefinite

Display elements of the Simatic Net-CP 443-1 Advanced

Simatic Net-CP 443-1 Advanced supports both Profinet IO and Profinet CBA functionalities (see Tables 4.59 and 4.60).

Table 4.59 LED status and fault displays of the CP 443-1 Advanced

INTF red	EXTF red	BUSF red	RUN green	STOP yellow	Meaning
0	0	0	0/1	1	CP is in STARTUP status.
0	0	0	1	0	CP is in RUN status.
0	0	0	1	0/1	CP is in HOLD status.
0	0	0	0	1	CP is in STOP status.
0	0	0	0	0/1	The CP is ready to load firmware. This mode is active for 10 seconds following power up in switch position STOP.
0	0	0	0/1	0/1	CP is waiting for a firmware update. CP contains incomplete or faulty FW release. The LEDs flash alternately.
0	1	0/1	1	0	CP is in RUN status. An external fault has occurred. One or more IO Devices cannot be accessed.
0	1	0	1	0	CP is in RUN status. An external fault has occurred. Diagnostics is present from one or more IO Devices.
1	0	0	0	1	CP is in STOP status. An internal fault has occurred. Possible cause: dual IP addressing in the network.
0/1	0/1	0/1	0/1	0/1	Module or system fault. In this case, the CP must be switched off and on again.

Table 4.60 LED status display of the communications interfaces of the CP 443-1 Advanced

TXD green	RXD green	LINK green	RX/TX yellow	Meaning
0	x	x	x	CP is not sending any data over Ethernet.
1	x	x	x	CP is sending data over Ethernet.
x	0	x	x	CP is not receiving any data from the Ethernet.
x	1	x	x	CP is receiving data from the Ethernet.
x	x	1	x	The port is working with 100 Mb/s.
x	x	0/1	x	0.5 Hz: the port is working with 10 Mb/s. 2 Hz: the function "Flashing station test" is active.
x	x	x	0	The port is not sending or receiving data over Ethernet.
x	x	x	0/1	The port is sending or receiving data over Ethernet.

0: off, 1: on, 0/1: flashes, x: indefinite

Display elements of the Simatic Net CP 343-1, CP 343-1 Lean, CP 343-1 Advanced

Table 4.61 LED status and fault displays of the CP 343-1, CP 343-1 Lean

SF red	BF red	RUN green	STOP yellow	Meaning
1	x	0	1	CP is in startup status following power ON or CP is in STOP status with fault.
0	0	0/1	1	CP is in startup status.
0	0	1	0	CP is in run status.
0	0	1	0/1	CP is in hold status.
0	0	0	1	CP is in stop status.
x	1	x	x	No LAN cable is inserted, or a double IP address has been detected.
x	0/1	1	x	The CP is configured as an IO Device; no data exchange is taking place with the IO Controller.
1	0/1	1	x	The CP is configured as an IO Controller. At least one IO Device was detected as faulty.
1	1	0/1	1	Firmware is being loaded.
0/1	0/1	0/1	0	Firmware was successfully loaded.
0/1	0/1	0	0/1	Firmware could not be loaded.
0/1	0/1	0/1	0/1	Module or system fault. In this case, the CP must be switched off and on again.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.62
LED status display of the communications interface of the CP 343-1, CP 343-1 Lean

P1/P2 gray/yellow	RX/TX green	Meaning
0	x	The port has no connection to the Ethernet.
1 (gray)	x	The port has a connection to the Ethernet.
1 (yellow)	x	Continuous data transfer is taking place at the port over Ethernet.
1 (gray) 0/1 (yellow)	x	The port is sending or receiving data over Ethernet or Profinet IO.
x	0/1	The port is sending or receiving data over Ethernet.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.63 LED status and fault displays of the CP 343-1 Advanced

SF red	BF PN red	RUN green	STOP yellow	Meaning
0	0	0/1	1	CP is in startup status.
0	0	1	0	CP is in run status.
0	0	1	0/1	CP is in hold status.
0	0	0	1	CP is in stop status.

Table 4.63 LED status and fault displays of the CP 343-1 Advanced *(continued)*

SF red	BF PN red	RUN green	STOP yellow	Meaning
0	0	0	0/1	CP is ready for starting of firmware download. This mode is active for 10 seconds following a power ON in switch position STOP.
1	0	0	0/1	CP is waiting for a firmware update. CP contains incomplete or faulty FW release. The LEDs flash alternately.
1	0	1	0	CP is in RUN status. An external fault has occurred. Diagnostics is present from one or more IO Devices.
1	0/1	1	0	CP is in run status. An external fault has occurred. One or more IO Devices cannot be accessed.
1	0	0	1	CP is in stop status. A fault has occurred. In this state, the CPU or intelligent modules in the rack can still be accessed using PG functions.
0/1	0/1	0/1	0/1	Module or system fault. In this case, the CP must be switched off and on again.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.64 LED status display of the communications interface of the CP 343-1

FD green	FAST green	LINK green	RX/TX green	Meaning
0	x	x	x	A half duplex connection exists.
1	x	x	x	A full duplex connection exists.
x	0	x	x	The port is working with 10 Mb/s.
x	1	x	x	The port is working with 100 Mb/s.
x	x	0	x	CP is not receiving any data from the Ethernet.
x	x	1	x	CP is receiving data from the Ethernet.
x	x	x	0/1	The port is sending or receiving data over the Ethernet.

0: off, 1: on, 0/1: flashes, x: indefinite

Display elements of the Simatic Net gateway IE/PB-Link PN IO

The LED display elements for the operating status are present on the front panel of the IE/PB-Link PN IO (Table 4.65).

Table 4.65 LED status and fault displays of the IE/PB-Link PN IO

SF red	BF PN red	BF DP red	RX/TX green	RUN green	STOP yellow	Meaning
1	1	1	x	1	1	Lamp test following switching-on.
1	0	0	0/1	0	1	Distribution of configuration.
0	0	0	x	0/1	1	IE/PB-Link PN IO is in STARTUP status.
0	0	0	x	1	0	IE/PB-Link PN IO is in RUN status.
x	x	x	x	1	0/1	IE/PB-Link PN IO is in HOLD status.
0	0	0	x	0	1	IE/PB-Link PN IO is in STOP status.
1	0	0	x	1	0	IE/PB-Link PN IO is in RUN status. A fault has occurred with one or more DP slaves.
1	0	0/1	x	1	0	IE/PB-Link PN IO is in RUN status. Fault on Profibus which does not concern the Profinet IO.
1	0/1	0/1	x	1	0	IE/PB-Link PN IO is in RUN status. Fault on Profibus which also concerns the Profinet IO (e.g. IO Devices) or fault with Profinet IO which also concerns the Profibus (e.g. a proxy which has not been started).
1	0/1	0	x	1	0	IE/PB-Link PN IO is in RUN status. Logical or physical connection to the IO Controller is missing.
1	1	x	x	1	0	IE/PB-Link PN IO is in RUN status. No Profinet IO device name has been assigned to the IE/PB Link PN IO. Possible cause: The Ethernet connection is interrupted.
1	x	1	x	1	0	IE/PB-Link PN IO is in RUN status. Faults on the Profibus, or incorrect Profibus configuration.
0	0	0	x	0	0/1	The IE/PB-Link PN IO is ready for starting of firmware download. This mode is active for 10 seconds following a power ON in switch position STOP.
0	0	0	x	0/1	0/1	IE/PB-Link PN IO firmware is being deleted.
1	0	0	x	0	0/1	IE/PB-Link PN IO is waiting for a firmware update. IE/PB-Link PN IO contains incomplete or faulty FW release.
x	x	x	x	0	0/1	IE/PB-Link PN IO firmware is being downloaded. The LEDs flash alternately.
1	0	0	x	0	1	IE/PB-Link PN IO is in STOP status. An internal fault has occurred.

Table 4.65 LED status and fault displays of the IE/PB-Link PN IO *(continued)*

SF red	BF PN red	BF DP red	RX/TX green	RUN green	STOP yellow	Meaning
0/1	0/1	0/1	x	0/1	0/1	Module or system fault. In this case, the IE/PB-Link PN IO must be switched off and on again.

0: off, 1: on, 0/1: flashes, x: indefinite

The display elements for the communications status are present on the front panel and on the RJ-45 socket of the Industrial Ethernet port of the IE/PB-Link PN IO (Table 4.66).

Table 4.66 LED status display of the communications interfaces of the IE/PB-Link PN IO

FDX green	FAST green	LINK green	RX/TX green	Meaning
0	x	x	x	A half duplex connection exists.
1	x	x	x	A full duplex connection exists.
x	0	x	x	The port is working with 10 Mb/s.
x	1	x	x	The port is working with 100 Mb/s.
x	x	0	x	There is a connection to the Ethernet.
x	x	1	x	There is no connection to the Ethernet.
x	x	0/1	x	The function “Node station test” is active.
x	x	x	0/1	The port is sending or receiving data over the Ethernet.

0: off, 1: on, 0/1: flashes, x: indefinite

Display elements of the Simatic Net gateway IWLAN/PB Link PN IO

Table 4.67 LED status and felt displays of the IWLAN/PB Link PN IO

SF red	BF PN red	BF DP red	RX/TX green/ yellow	ON green	Meaning
1	1	1	x	1	Lamp test following switching on.
1	0	0	0/1	x	Distribution of configuration.
0	0	0	x	1	IWLAN/PB-Link PN IO is in RUN status.
1	0	0	x	1	IWLAN/PB-Link PN IO is in RUN status. A fault has occurred with one or more DP slaves, or a C-PLUG fault is present.
1	0	0/1	x	1	IWLAN/PB-Link PN IO is in RUN status. Fault on Profibus which does not concern the Profinet IO.
1	0/1	0/1	x	1	IWLAN/PB-Link PN IO is in RUN status. Fault on Profibus which also concerns the Profinet IO (e.g. IO Devices) or fault with Profinet IO which also concerns the Profibus (e.g. a proxy which has not been started)).
1	0/1	0	x	1	IWLAN/PB-Link PN IO is in RUN status. Logical or physical connection to the IO Controller is missing.
x	x	x	0/1 (green)	x	The WLAN connection to the access point is interrupted. Possible cause: Incorrect WLAN parameterization.
0/1	0	0	0	0	Ready for starting of firmware download via the bootloader. The device was either stopped in the bootloader or contains a faulty FW release.
x	x	x	1 (green)	x	Connection exists to the access point. No data are being transmitted.
x	x	x	0/1 (yellow)	x	Connection exists to the access point. Data are being transmitted.
0/1	0/1	0/1	0/1	0/1	PRESET plug detected. Ready for the Preset function.
1	1	1	1	1	Preset function completed successfully. Device can be switched off and PRESET plug removed.
x	x	x	x	0/1	1 Hz: IWLAN/PB-Link PN IO is in STOP status. 5 Hz: The function "Flashing station test" is active.

0: off, 1: on, 0/1: flashes, x: indefinite

Display elements of the Simatic Net gateway IE/AS-i Link PN IO

Table 4.68 LED status and fault displays of the IE/AS-i Link PN IO

SF red	BF red	ON green	Meaning
1	x	x	Possible causes: – In protected mode, a diagnostics interrupt (up) was triggered in the IO Controller. – The IE/AS-i Link has detected an internal fault (e.g. EEPROM faulty).
x	0/1	x	Possible causes: – The connection between the IO Controller and IE/AS-i Link is interrupted. – The IO Controller is inactive. – The IE/AS-i Link has not been (correctly) parameterized/configured by the IO Controller.
x	x	1	Voltage is present on the IE/AS-i Link.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.69 LED status display of the communications interfaces of the IE/AS-i Link PN IO

LINK green	RX/TX green	Meaning
1	x	The port is working with 100þMb/s.
0/1	x	2 Hz: The function "Node station test" is active.
x	0	The port is not sending or receiving data over the Ethernet.
x	0/1	The port is sending or receiving data over the Ethernet.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 4.70 LED status display of the AS-i line of the IE/AS-i Link PN IO

SF red	APF red	CER yellow	AUP green	CM yellow	ON green	Meaning
1	x	x	x	x	x	In protected mode, a diagnostics interrupt (up) was triggered in the IO Controller.
x	1	x	x	x	x	AS-i power failure: Voltage supplied by the AS-i power supply unit is too low or faulty.
x	x	1	x	x	x	Configuration error:Configured structure does not agree with the actual structure. Possible causes: – A configured AS-i slave is not present on the AS-i line. – An AS-i slave which was not previously configured is present on the AS-i line. – A connected AS-i slave has different configuration data than the AS-i slave configured in the IE/AS-i Link. – -The IE/AS-i Link is in offline mode.
x	x	x	1	x	x	Autoprog available: Indication that automatic address programming of an AS-i slave is possible in the protected mode of the IE/AS-i Link.

Table 4.70 LED status display of the AS-i line of the IE/AS-i Link PN IO *(continued)*

SF red	APF red	CER yellow	AUP green	CM yellow	ON green	Meaning
x	x	x	x	1	x	Configuration mode: 0: Protected mode 1: Configuration mode
x	x	x	x	x	1	Voltage is present on the IE/AS-i Link.

0: off, 1: on, 0/1: flashes, x: indefinite

5 Profinet CBA – Distributed Automation

Modularization means that a task is divided into several subtasks. In the ideal case, the modules produced to solve a subtask are designed such that they can be used again to solve other tasks. The principle of modularization is used successfully in machine and plant construction, for it results in two significant advantages:

- The configuration and commissioning times are shorter than with centralized solutions.
- The resulting plant modules can be used repeatedly.

Data exchange between the controllers of the plant modules is of decisive significance in the automation of a modular plant concept. Current controllers comprise a centralized PLC with local or distributed I/O. Communication is usually part of the control program and configuration. The 1:1 mapping of the modularization principle with this classical method of automation would mean that the effort for commissioning and testing such a controller would have to be permanently repeated each time a plant module is reused. This also applies to plant expansions, and particularly if controllers from different vendors have to communicate with each other in a heterogeneous plant environment.

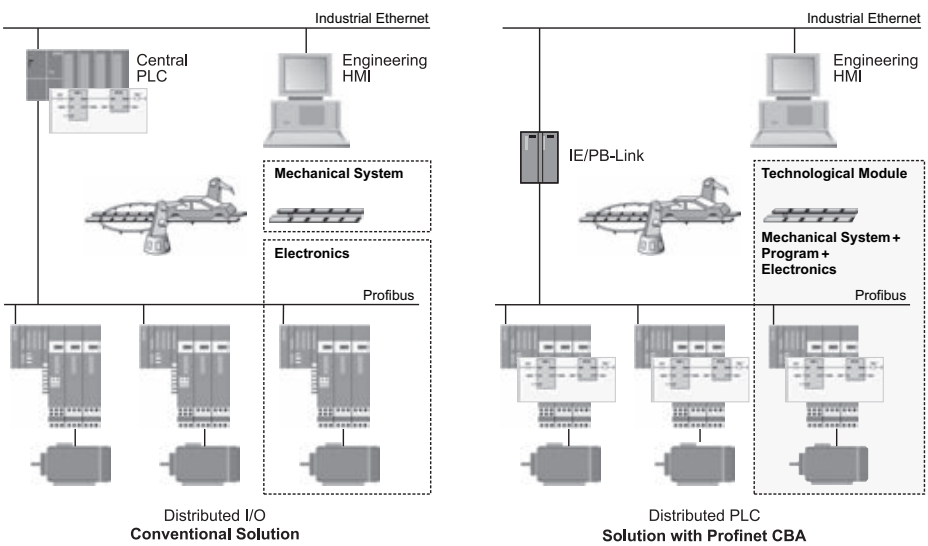


Fig. 5.1 Modular automation concept: conventional and with Profinet CBA

The Profinet CBA technology solves this problem by providing a facility for predefining technological modules which are then used as standardized automation components in large plants (Fig. 5.1).

Profinet components are technological modules in the form of software. They are produced using a vendor-specific engineering tool, for example Step 7, and managed and configured using a Profinet CBA engineering tool such as Simatic iMap.

The distributed controller and the technological module work autonomously. No information concerning the communications partners is required within the control program. Communication with other modules is carried out over defined communications interfaces in the control software. These interfaces use a Profinet CBA engineering tool to provide the plant modules with data. As a result, the OEM can carry out complete testing of a plant module prior to delivery.

During the final assembly of the complete plant, communication between the plant modules is configured graphically. No interventions whatsoever are required in the control programs of the plant modules.

The advantages of this concept:

- Significant reduction in planning overhead
- Significant reduction in adaptation process as a result of unambiguous communications interfaces
- High degree of autonomous testing without requiring the complete plant
- Simplified troubleshooting
- Simple and early commissioning.

The concept of distributed intelligence guarantees a high degree of reusability for the automation of plant modules, and significantly reduces the commissioning time for a plant. It is therefore in line with the trend towards increased modularization in machine and plant construction and the associated decentralization.

5.1 The Road to Distributed Automation

Profinet is an open automation standard based on Industrial Ethernet. Within this standard, Profinet CBA – based on IEC 61499-1 – describes a technology for implementing modular and distributed automation solutions on the basis of predefined components.

At the beginning of the 1990s, the International Electrotechnical Committee (IEC) adopted the IEC 61131 standard “Programmable controllers”, with a fundamental description of the architecture of a programmable logic controller (PLC). This standard combined existing standards, and was the first standard to receive international and industrial acceptance in the controller environment. Part 3 “Programming languages” was adopted in 1993, and particularly considers the definition of a modular and function-oriented programming model for the individual, central PLC.

Also in the 1990s, a working group of the IEC (IEC 65 WG 6) was commissioned to describe a general model for distributed automation systems (Industrial Process Measurement and Control Systems – IPMCS). This resulted in the IEC 61499 standard "Function blocks for industrial process measurement and control systems", where Part 1 "Architecture" expanded the concept of function blocks defined in IEC 61131-3 to distributed systems. IEC 61499-1 was adopted by the German Institute for Standardization (DIN) in June 2006 as DIN EN 61499-1 "Function blocks for industrial control systems – Part 1: Architecture".

The programming model of IEC 61499 is based on function blocks, and permits visual programming with reusable components. The system and program descriptions are standardized similar to IEC 61131, but not the binary format or the specific system interfaces.

The "Profibus Architecture Description and Specification" issued by Profibus International defines a cross-vendor communications, automation and engineering model based on IEC 61499-1. The objective is to implement distributed automation solutions with the assistance of uniform communication over Ethernet and fieldbus with application of open standards.

5.1.1 Distributed Automation Systems with IEC 61499-1

Distributed automation systems in accordance with IEC 61499-1 have a hierarchical structure and are component-based. Elementary terms in this context are "System", "Device", "Resource", "Application" and "Function block" (see Table 5.1). The specification of Profinet CBA is largely in accordance with the model described in IEC 61499-1.

Table 5.1 Elementary terms of IEC 61499-1 and Profinet CBA

IEC 61499-1	Profinet CBA
System	System
Device	Physical device
Resource	Logical device
Function block	Automation object/function
Application	Application
Connection	Interconnection

System

The system model describes a distributed automation system as an entity. The system is the highest level in the architecture hierarchy (Fig. 5.2). It consists of physical devices which are connected together by means of a communications network. The common process is controlled by several applications which are either present within one device (Application C) or divided between several devices (Applications A and B). The part of an application executed within a device can also be divided further between several resources of the device using local applications.

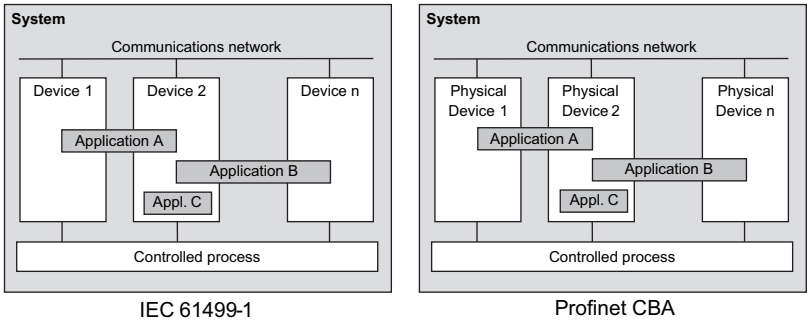


Fig. 5.2 System model with IEC 61499-1 and Profinet CBA

Devices

A device contributes a stand-alone function toward solution of the complete automation task. It is a generic term for various types of devices, covering PLCs, PCs up to fixed-programmed controllers (embedded controllers), or intelligent field devices with specific firmware (Fig. 5.3). All possess a process interface and a communications interface. Devices contain one or more resources.

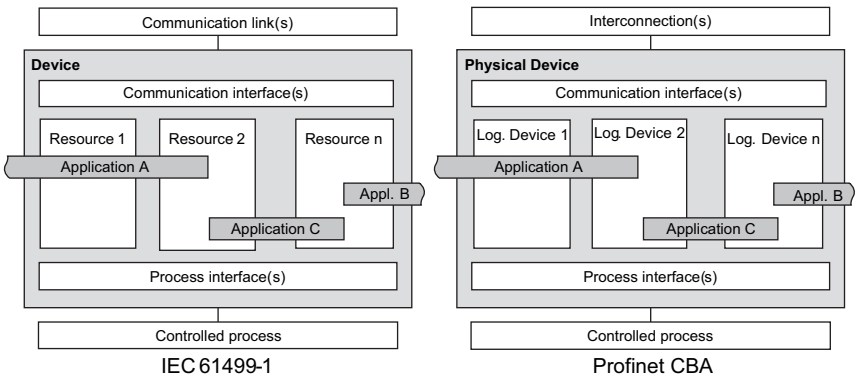


Fig. 5.3 Device model with IEC 61499-1 and Profinet CBA

Resources

The resource is the execution environment for local applications, also referred to as function blocks. They constitute a logical parenthesis around the software required to operate a device. This includes its firmware as well as a control program which may be freely-programmable. Function blocks are able to exchange data with other function blocks via connections. The communications partners can be within the same device, or located on other devices accessible over the communications network (Fig. 5.4).

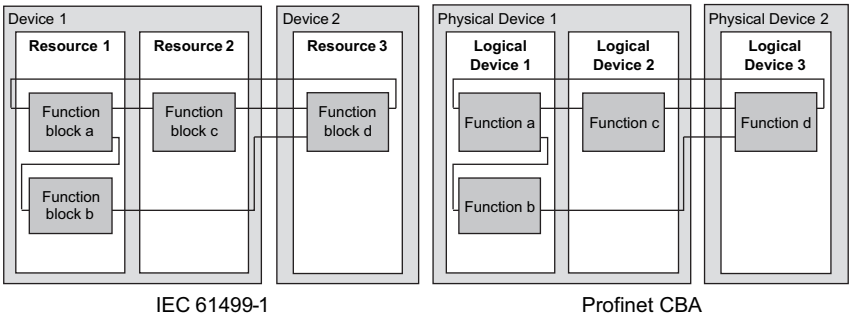


Fig. 5.4 Resource model with IEC 61499-1 and Profinet CBA

Function blocks

Function blocks are the fundamental elements of the IEC 61499-1 architecture model. They possess interfaces for sending and receiving data, and contain internal data and executable algorithms which are invisible from the outside. The technological functions of Profinet CBA are based on the application-oriented service interface function blocks (SFIB) described in IEC 61499-1.

Function blocks have a static structure or are freely-programmable. Consequently, the devices have either

- a fixed functionality, e.g. with field devices, actuators or sensors, or
- a programmable or loadable functionality like PLCs or PCs.

Whereas the functionality is part of the firmware in the first case, the latter must first be programmed and configured specific to the application prior to use. Although both types of function have extremely different internal structures with respect to architecture and programming, their external communications properties are the same. This is made possible by a uniform communications view based on ORPC (Object-oriented Remote Procedure Call).

ORPC

By means of OLE 1 (Object Linking and Embedding), the possibility was provided for the first time with Microsoft Windows 3.1 for combining different, basically stand-alone applications. This was a significant step in the direction towards modularization of user software. With OLE 2, Microsoft not only provided an extension of OLE 1, but made available a new and significantly more comprehensive architecture with a completely new approach for the development of software under Microsoft Windows.

OLE defines a standard which permits the description of objects as entities in Windows and permits these to be accessed beyond process limits. OLE is the basis of COM, the Component Object Model from Microsoft. COM basically describes the interaction between binary objects during runtime. It therefore does not refer to the source code but to executable programs. Based on COM, objects can work to-

gether which have been developed independently by different vendors and possibly also using different programming languages. Complex applications can be expanded individually through division between several objects, and individual components can be easily replaced by upgrades with improved versions. Individual objects can be used by different applications.

With Windows NT Version 4, the COM interface was extended for the first time by the capability for accessing objects beyond device limits. The objects used by an application can therefore also be distributed within a network. This expansion of COM is referred to as DCOM (Distributed COM) or ORPC. The ORPC wire protocol permits the transmission of object accessing over a network.

ORPC wire protocol

The ORPC wire protocol is present in the top layer of the seven-layer ISO/OSI communications model (see Fig. 5.5). It is based on the RPC protocol (Remote Procedure Call) and uses the latter's fields for its own purposes. The ORPC functionality largely corresponds to that of the DCE RPC protocol defined by the Open Software Foundation (OSF).

There are two versions of RPC itself:

- CLRPC (ConnectionLess RPC) with UDP as transport protocol
- CORPC (ConnectionOriented RPC) with TCP as transport protocol.

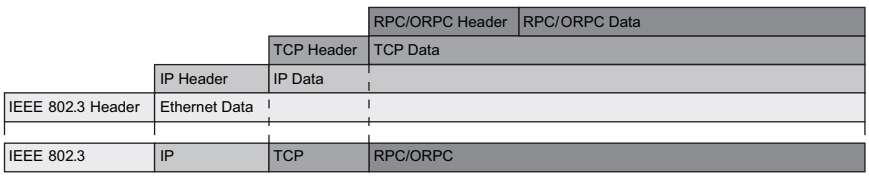


Fig. 5.5 Basic structure of an ORPC wire data packet

5.2 Profinet CBA

Profinet CBA defines the engineering for creating Profinet components, a uniform architecture for communication between devices in a distributed automation application, migration mechanisms for existing fieldbus systems such as Profibus, and the integration of HMI systems via OPC. The standard defined in IEC 61188-10 determines the communications mechanisms on the Ethernet, and describes an engineering model for communication between the autonomous technological units of an automation plant. Each of these units constitutes a stand-alone technological module which can be repeatedly used. On the engineering side, the technological module is represented by a software component, the Profinet component. Profinet components are created using a vendor-specific engineering tool and combined in a Profinet CBA engineering tool to produce the complete plant.

Component Based Automation is the first uniform implementation of this technology, and consists of the following components:

- Step 7 as engineering tool for creation of Profinet components from Simatic S7 automation devices
- Simatic iMap as Profinet CBA engineering tool for configuration of distributed plants
- Simatic S7 and Simatic Net Profinet controllers
- A comprehensive range of Profibus I/Os with migration capability and Profinet I/Os with integration capability.

5.2.1 Profinet CBA Concept

The basic idea of Profinet CBA is the separation of component creation and component application.

The "inner workings" that means the functionality of a component are defined during its creation. The component is configured, and also programmed in the case of programmable controllers. The component vendor applies the same system-specific configuration and programming tools as previously. These tools are also used to define the technologically oriented interfaces of the components. Using these technological interfaces, other components can make use of the functionality of the component in the distributed plant during runtime.

Creating the component generates an engineering component – the Profinet component – from the completely configured and programmed device. This component can be used by Profinet CBA engineering tools to create a distributed automation solution. The configuration for a specific plant as well as the final uploading of the communication configuration into the individual devices is carried out there.

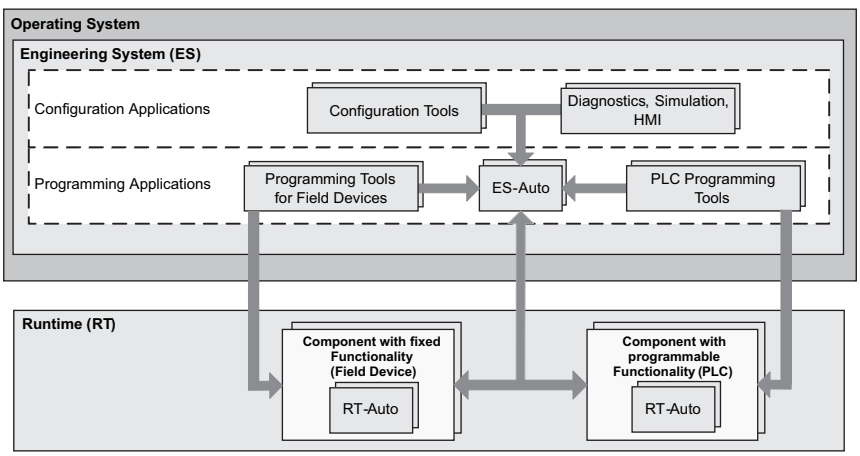


Fig. 5.6 Profinet CBA concept

Profinet CBA specifies an open and object-oriented runtime concept (Fig. 5.6). This concept is based on an object-oriented approach. Stand-alone modules are generated whose functionalities can be accessed externally over unambiguous object interfaces.

5.2.2 Profinet CBA Object Model

Profinet CBA defines a runtime object model and an engineering object model. The runtime object model represents the objects existing within a Profinet controller during runtime, and describes their relations to each other. The model describes a programmable controller consisting of a physical device (the hardware) and a logical device (the software). The component object model is based on this object-oriented approach. The runtime object model is implemented in every Profinet controller (Fig. 5.7).

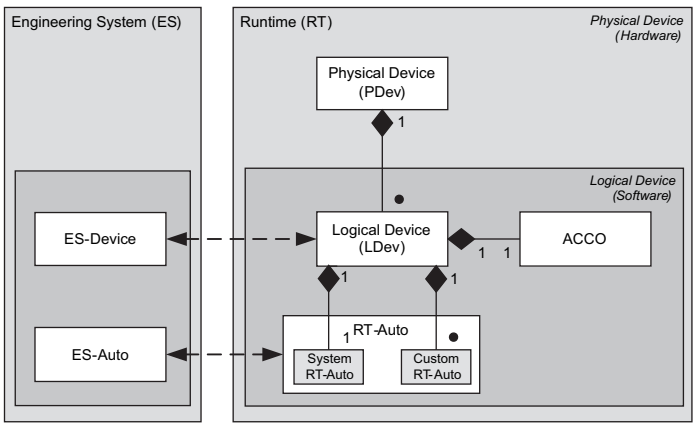


Fig. 5.7 Profinet CBA object model

Corresponding engineering objects (ES objects) exist in a Profinet CBA engineering system. They have the same basic structure as Profinet runtime objects, i.e. Profinet runtime objects are present in the engineering model in a similar form.

Profinet runtime objects possess compulsory and optional interfaces. Whereas the former implement the actual Profinet CBA functionality, the optional interfaces offer device and software vendors the possibility for implementing own proprietary functionalities as a supplement. This particularly applies to access to process variables by the RT-Autos. Special interfaces are also imaginable for diagnostics or parameterization.

The physical device object

The physical device object (PDev) represents the hardware of a device. For a Profinet controller, exactly one PDev exists during runtime. The PDev can be accessed

using the IP address(es) or the DNS name of the device, and functions as the initial starting point for other applications for navigation through the device.

The logical device object

The logical device object (LDev) is the software representative of a device. Several LDev's can exist within a device during runtime. Using Profinet controllers with proxy functionality as an example, a LDev exists for each Profinet device integrated by means of the proxy functionality as well as for the Profinet controller itself.

The runtime automation object

The runtime automation object (RT-Auto) consists of a system RT-Auto and one or more custom RT-Auto(s).

The system RT-Auto allows access to system variables. These variables contain standardized information, for example concerning the status of the RT-Auto.

A custom RT-Auto is an executable program with a corresponding data area, and provides the actual technological functionality of a Profinet controller. Custom RT-Autos are connected to a distributed application using the ACCO (Active Control Connection Object). They are modeled specially for their automation task, and have an application-specific structure.

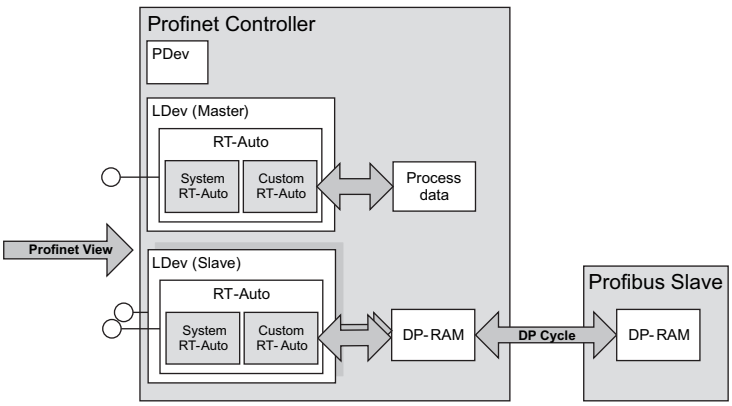


Fig. 5.8 Mapping of process data and proxy functionality

The vendor-specific interfaces of the custom RT-Autos implement the actual process coupling of a Profinet controller. They permit access to the linkable connections of technological functions, and represent their technological interface. To achieve this, an RT-Auto carries out bidirectional mapping of the control application's process data at its technological interfaces (see Fig. 5.8).

Proxy functionality with Profinet CBA

Field devices can participate in the Profinet CBA communication using a proxy. The proxy functionality in the sense of Profinet CBA is a property of Profinet controllers with DP master functionality. In this case, the Profinet-controller provides the Profinet runtime model as a proxy for a fieldbus device such as a Profibus DP slave.

The basic idea of the proxy is to provide the I/O data of any field devices in a form which permits interconnection of these data in the context of the Profinet CBA communication. From the process data view, a proxy corresponds to an Ethernet/fieldbus gateway, and makes a field device appear like a Profinet CBA from the viewpoint of Profinet CBA.

With a Profibus DP master, the I/O data present in the DP-RAM of a DP slave are transmitted to the (custom) RT-Auto of the slave LDev, and from there to the inputs/outputs of its technological interface. A field device integrated by means of a proxy can only be accessed via the proxy from the Profinet CBA viewpoint. In particular, this means that it does not have its own IP address.

Integration of field devices via proxy does not require an additional functionality on the respective fieldbus. Any real-time capability available is retained. During operation of a field device via a proxy, access to the I/O data of the field device is decoupled from the user program of the respective host, for example of a DP master. The field device only exchanges its I/O data with the (Custom) RT-Auto of the corresponding LDev. It is then possible for the field device to exchange data with any Profinet CBA communications partner. However, operation of a field device

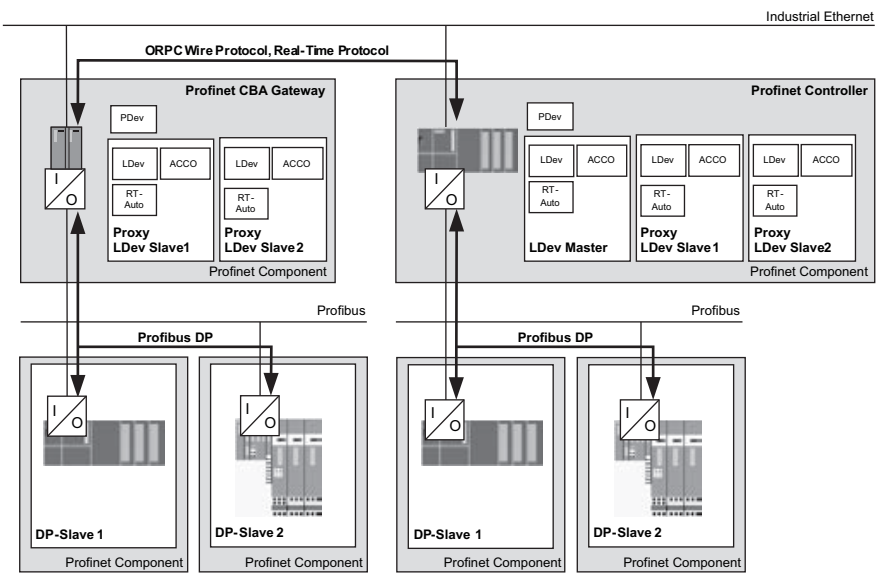


Fig. 5.9 Principle of proxy functionality with Profinet CBA using example of Profibus DP

via a proxy means that no direct access may take place from the user program of the host to the I/O data of the field device.

Profinet CBA proxies and Profinet IO proxies basically satisfy the same task with the integration of field devices, but do not possess compatible functions because of the different communications services used on the Ethernet.

The ACCO

The ACCO (Active Control Connection Object) is the central administration and management point for interconnections. It exists exactly once per LDev, and is responsible for data exchange between RT-Autos. The ACCO accesses the data of the own RT-Auto over internal interfaces, and transmits them to the ACCO of the communications partner.

Decoupling of Profinet CBA communication (ACCO) and process interfacing (RT-Auto) permits language-independent implementation of the RT-Auto and the provision of process data in any format. The interconnection configuration is loaded into the ACCO when carrying out the engineering, and interpreted there. Establishment of the interconnection is subsequently carried out.

Profinet Runtime software

The Profinet Runtime software is an implementation of the Profinet runtime model independent of the operating system. It is available as source code for downloading from PROFIBUS International, and covers the complete range of Profinet runtime communication. In addition to this, several example implementations are available for different hardware and operating system platforms.

The Profinet Runtime software consists of a stable kernel and modules for adaptation of the kernel to any target systems. With the assistance of the specification and source code, simple and efficient integration of Profinet Runtime is possible into a wide range of devices (Fig. 5.10). An implementation manual provides the corresponding development support for the Profinet Runtime Source.

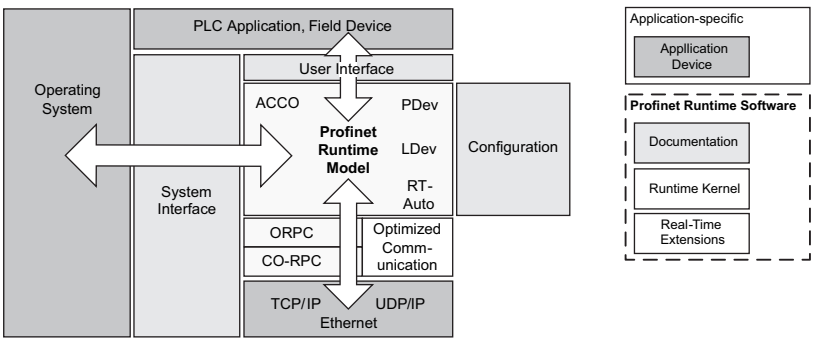


Fig. 5.10 Embedding of Profinet Runtime in an automation system

Profibus International supports vendors of automation and field devices by:

- Provision of the Profinet specification
- Provision of the Profinet Runtime Source
- Instructions for integration of the Profinet Runtime Source into various operating systems, e.g. also Linux
- Certification of Profinet products to guarantee interoperability
- Support in the implementation of Profinet devices by the Profinet Competence Center ComDeC.

5.2.3 Integration of Fieldbuses

When expanding an existing plant with Profinet CBA, existing fieldbus systems such as Profibus, AS-I, etc. must be integrated into the Profinet CBA communication. This task is solved by Profinet CBA in two manners:

- The fieldbus system is completely integrated into a Profinet component. For this purpose, the fieldbus master must possess Profinet CBA capability. This can be achieved by expanding the fieldbus master by an Ethernet interface module with Profinet CBA capability, or by replacing the fieldbus master by a Profinet controller with compatible functions.
- Profinet components are created from individual field devices, which participate in the Profinet CBA communication during runtime by means of a Profinet controller with proxy functionality.

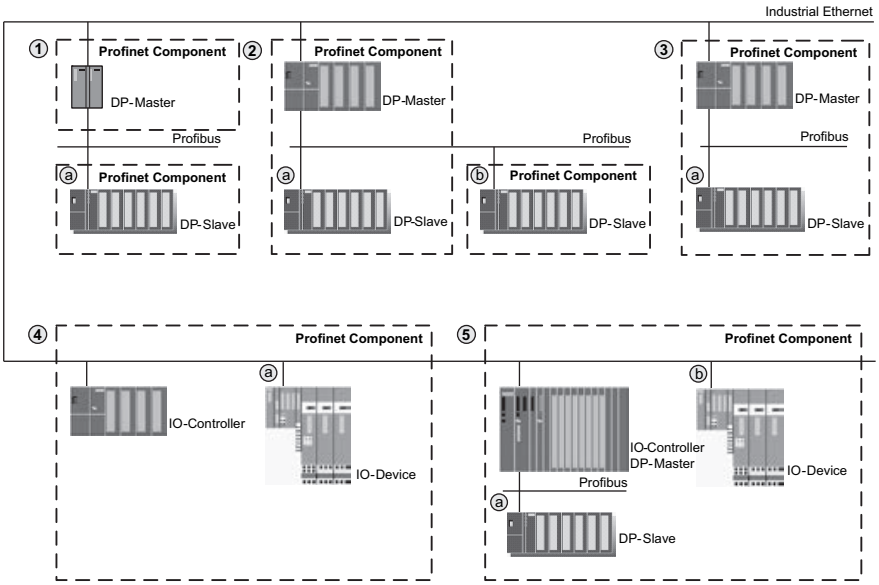
These facilities mean that it is possible to establish any mixed configurations with fieldbus-based and Ethernet-based subsystems, therefore permitting a continuous technology transition to Profinet CBA to be implemented (Fig. 5.11). The following field devices are supported:

- Profibus DP devices with own CPU,
- Profibus DP standard slaves with GSD file
- Profinet IO Devices.

5.2.4 Profinet and Profibus Devices

The device presents the hardware-specific part of the Profinet component. In association with Profinet CBA, a device is the representation of the physical device for which the Profinet component has been created. The term “Device” serves as a synonym for:

- Automation systems
- Field devices such as PLCs, PCs, hydraulic units, pneumatic units
- Active network components, e.g. distributed I/Os, valve terminals or drives.



1 Profinet CBA router as Profinet controller with proxy functionality and
a) DP slaves as Profinet component via proxy.

2 CPU as Profinet controller with proxy functionality with
a) DP slaves of a local DP master system and
b) DP slaves as Profinet component via proxy.

3 CPU as Profinet controller with
a) DP slaves of a local DP master system.

4 CPU as Profinet controller with
a) IO Devices of a Profinet IO system.

5 CPU as Profinet controller with
a) DP slaves of a local Profibus system and
b) IO Devices of a Profinet IO system.

Fig. 5.11 Fieldbus integration with Profinet CBA

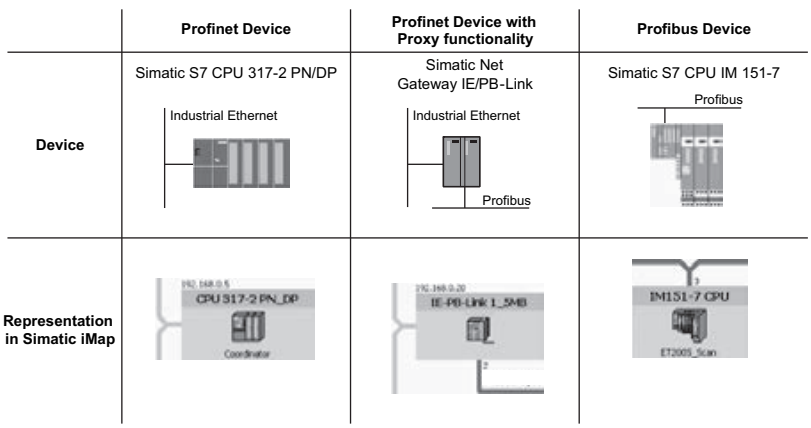


Fig. 5.12 Profinet and Profibus devices

A significant feature of a device is its integration into the Profinet communication over Ethernet or Profibus. According to the bus connections, a differentiation is made between (see also Fig. 5.12):

- Profinet devices: in the context of Profinet CBA, these devices are also called Profinet controllers. Such a device always contains at least one Industrial Ethernet connection. If it masters a proxy functionality in addition, at least one Profibus connection with DP master function is added as an option.
- Profibus devices: Profibus devices do not have an Industrial Ethernet connection, but at least one Profibus connection. Accordingly, Profibus devices cannot participate directly in the Profinet CBA communication but only via a Profinet controller with proxy functionality.

5.2.5 Simatic S7 and Simatic Net Products for Profinet CBA

Component Based Automation is the implementation of Profinet CBA for automation systems from the Simatic S7 and Simatic Net ranges. Depending on the configuration, this includes the following products (see also Fig. 5.13):

- Simatic Step 7 as engineering tool for configuration and programming of Simatic S7 and Simatic Net automation systems as well as for creating Profinet components.
- Simatic iMap as engineering tool for configuration of distributed plants and for integration of device-specific programming, configuration and diagnostics tools into a Profinet CBA engineering environment.
- Simatic Net OPC Server PN for access to process and HMI data over the OPC interface.

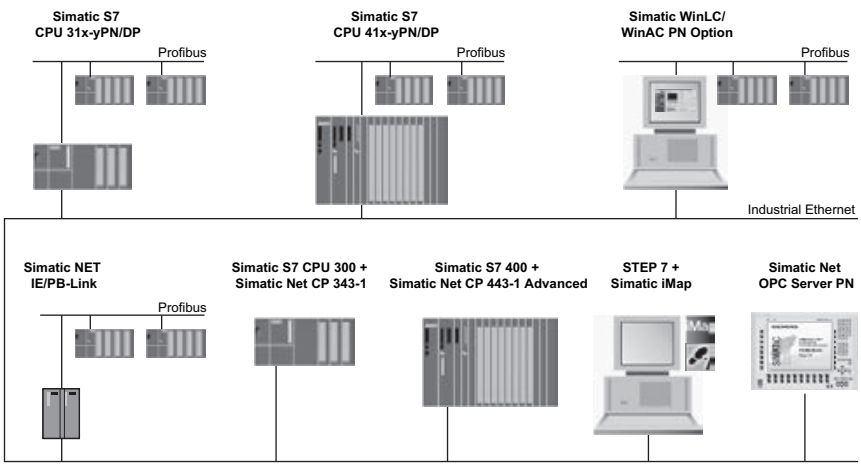


Fig. 5.13 Simatic S7/Simatic Net product range for Profinet CBA

- Simatic WinLC PN and Simatic WinAC PN-Option as Profinet controller with proxy functionality.
- Simatic S7 CPU 31x-y PN/DP as Profinet controller with proxy functionality. Simatic S7 CPU 41x-y PN/DP as Profinet controller with proxy functionality.
- Simatic Net IE/PB Link as gateway between Profinet CBA and Profibus. The IE/PB-Link has proxy functionality, and serves for migration of Profibus devices into Profinet CBA communication.
- Simatic Net-CP 343-1 PN as system connection for migration of existing Simatic S7-300 CPUs into the Profinet CBA communication. In addition to Profinet CBA, the CP also supports the standard communications services of the previous Simatic Net Ethernet system connections.
- Simatic Net-CP 443-1 Advanced as system connection for migration of existing Simatic S7-400 CPUs into the Profinet CBA communication. The CP has an integral 4-port switch and integral Web server. In addition to Profinet CBA, it also supports Profinet IO and the standard communications services of the previous Simatic Net Ethernet system connections.

5.3 Profinet CBA Engineering

Profinet CBA defines a standardized and multi-vendor engineering model for simple integration of devices and components from different vendors in a distributed automation system. Simatic iMap is a cross-vendor engineering tool based on this model for configuring Profinet CBA applications (see Fig. 5.14). A distributed automation application is combined in graphic mode, and displayed plant-wide.

All Profinet components required are available with a uniform representation in libraries. Communications connections between the technological functions of the devices are not programmed but are configured graphically as interconnection lines. This is followed by uploading of programs, the configuration and interconnection of the Profinet components into the devices in the plant. Process and diagnostics data for the devices can be scanned during commissioning and operation, and parameters and project data can be modified for test purposes.

Simatic iMap provides the OPC symbol file required for access of HMI systems via OPC, and automatically creates complete documentation of the distributed system. Supplementary to this, Simatic iMap provides software for linking to vendor-specific configuration and programming tools:

- A Step 7 add-on which enables Profinet components to be created from the Simatic Manager.
- An integration facility for vendor-specific engineering tools to support proprietary configuration and diagnostics facilities.

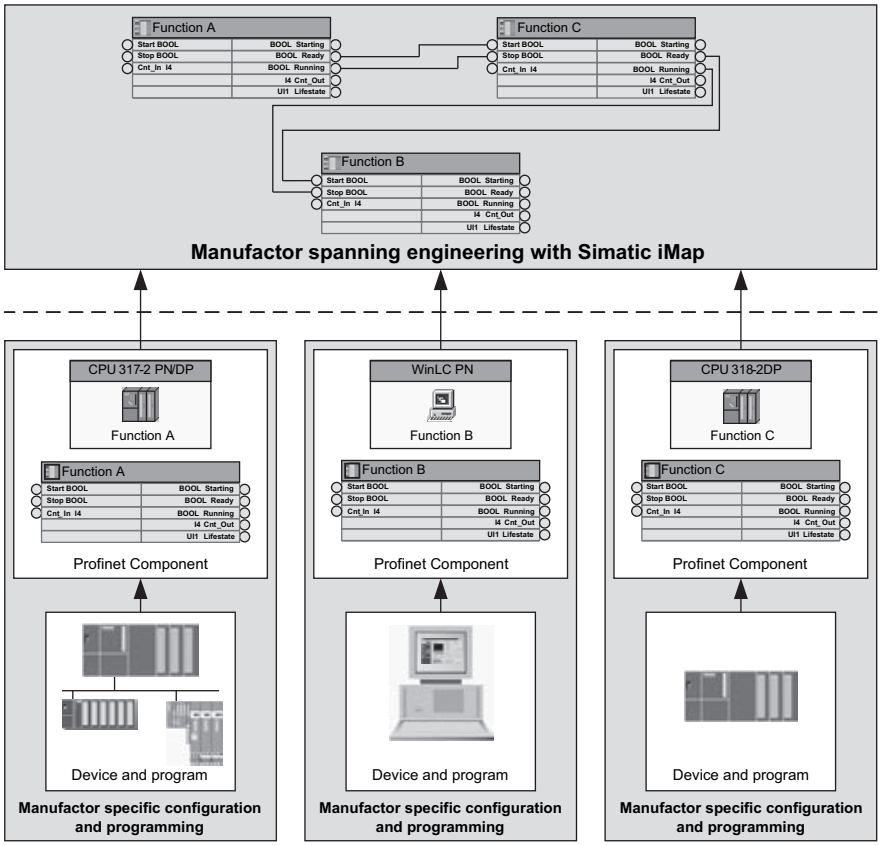


Fig. 5.14 Simatic iMap engineering concept

5.3.1 Generation of Profinet Components

Profinet components are generated by plant or machine constructors. During their creation, the respective engineering tool also generates a Universal Unique Identifier (UUID). The UUID permits unambiguous global identification of the Profinet components. Only Profinet components with the same UUID have the same functionality.

Programming and configuration of a Profinet component is carried out using the same vendor-specific tools as previously. Existing know-how for creating applications can be applied further. The component creator writes the user programs involved in communication for Profinet devices with programmable functionalities. A data area (an interface DB in the case of Simatic S7) can subsequently be created for the data exchange. The input and output data of the respective Profinet component are saved there during runtime.

The Profinet component is generated in the form of a Profinet Component Description (PCD) in the next step, and imported into a library of the interconnection editor.

5.3.2 Interconnection of Profinet Components with Profinet CBA Engineering Tool

The interconnection editor is the central component of a Profinet CBA engineering tool. Its task is the interconnection of Profinet components. The Profinet component descriptions are visible as icons in the library, and can be arranged in the plant project and connected together by drag&drop. The plausibility of an interconnection with respect to data format and transfer frequency is checked by the interconnection editor. Interconnection editors provide several views of the plant:

- The chart view has a hierarchical tree structure presenting a view of the plant with its functions and charts.
- The plant view presents the instances of the Profinet components as technological functions and their interconnections (logical data connections) within the plant.
- The network view presents the instances of the Profinet components as objects with one or more network connections, and thus permits a topological view of the plant.
- The project view shows the relationship between the Profinet components of the library and the inserted instances.

5.4 Profinet Components

5.4.1 Technological Module

Within the automation plant or production process, a particular technological function is defined by interaction of the mechanical, electrical and electronic components used. When supplemented by the associated control program, the result is an autonomous technological module (see example in Fig. 5.15).

5.4.2 Profinet Components

In the engineering of distributed plants, a technological module is represented by a Profinet component (Fig. 5.16). This comprises the complete data of a device's hardware configuration, its module parameters and an optional user program. The actual device functionality with its application-specific program is encapsulated within the Profinet component. From the Profinet view, only the technological interfaces of the device are still accessible which are required for interactions in the machine or plant, for diagnostics, visualization and vertical integration.

A Profinet component consists of two information parts:

- one device as representative for hardware
- at least one technological function.

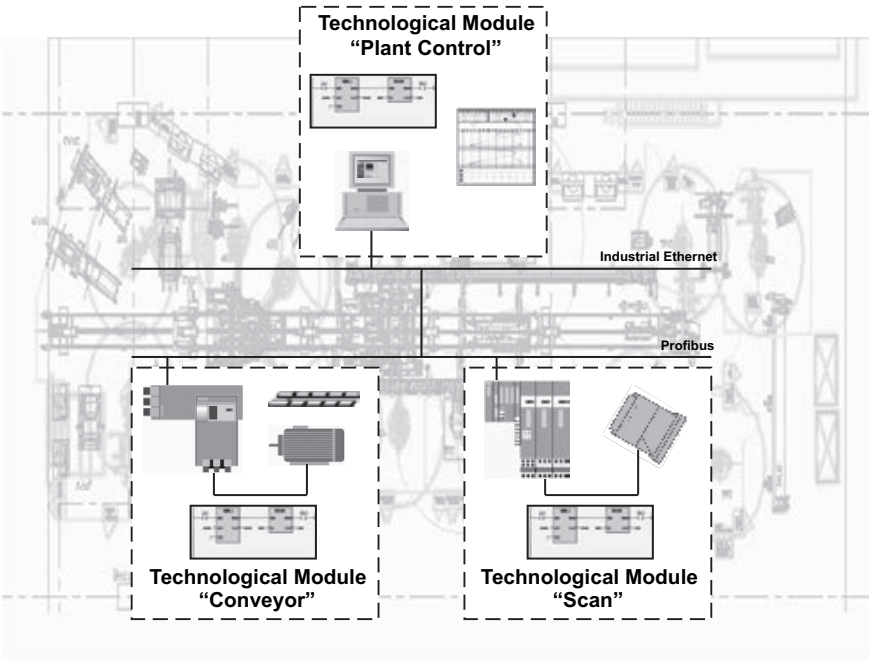


Fig. 5.15 Example of a plant section with three technological modules

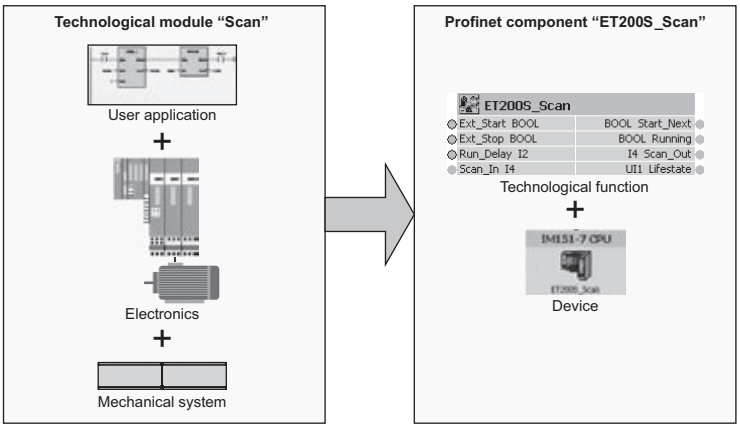


Fig. 5.16 Mapping of a technological module by a Profinet component

Device

The device is the part of a Profinet component which contains the hardware-specific data of the Profinet component. In Simatic iMap, a device is the software representation of the physical device for which the Profinet component has been cre-

ated. It is represented in the network view of Simatic iMap as an object with one or more network connections.

Technological function

The technological function represents the user application and its technological interface for communication with other Profinet components. A technological function is understood either to be the complete functionality or a part of functionality of a device. It is represented in the plant view of Simatic iMap as a block with inputs and outputs.

Technological Interface

One or more technological interfaces define the connections, i.e. the inputs and outputs of the Profinet components. Connections represent the external communications interfaces accessible over Ethernet and Profibus. Each connection is characterized by properties defined when creating a Profinet component:

- Direction: each connection is either an input (consumer) or an output (provider).
- Interconnecting in Simatic iMap: connections which are visible in Simatic iMap can be linked. Connections which cannot be interconnected are not shown graphically in Simatic iMap. These are accessible using other communications mechanisms, e.g. OPC (OLE for Process Control), and are usually used for operation and monitoring.
- Name: the name of a connection can be freely selected with consideration of the name rules, and may be up to 24 characters long.
- Data type: a data type is defined for each connection, e.g. BOOL, I1 or STRUCT.
- Value: the current value of a connection can be displayed online in Simatic iMap during runtime. In addition, online values of non-linked inputs can be modified.

Programmable and Fixed Functionality

The application-specific functionality is defined for an intelligent device by its user program. Simpler devices, e.g. actuators or field devices, do not have their own user program. The fixed functionality of these devices is integrated in their firmware. Accordingly, a Profinet component has either a programmable functionality if it contains its own user program which can be uploaded from Simatic iMap, or it contains a fixed functionality and therefore no own user program.

5.4.3 Profinet Component Types

Profinet components can be generated with or without vendor-specific device data (Fig. 5.17). Profinet components without vendor-specific data are called singleton components.

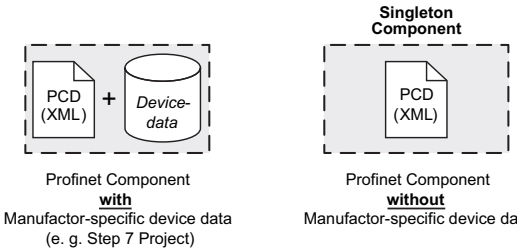


Fig. 5.17
Profinet component types

Multi function components

With a multi function component, the technological function of a Profinet component is distributed between several subfunctions. Each subfunction has its own technological interface.

The division into subfunctions allows clear representation and structuring of the complete plant in the Profinet CBA engineering system.

Fig. 5.18 shows an example of the implementation of a technological module as a conventional Profinet component and as a Profinet multi function component.

Despite the division of the technological function into several subfunctions, the user program of a multi function component including the hardware configuration data still constitutes an entity. Device-specific actions within the Profinet CBA engineering tool, e.g. generation, therefore always refer to the complete instance of the multi function component.

It must be possible to program multi function components, and they can therefore only be created using devices with a programmable functionality. Implementation is possible as standard or singleton components.

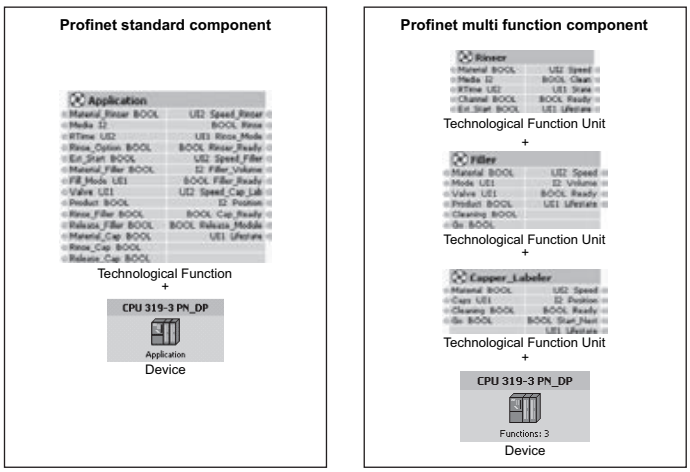


Fig. 5.18 Profinet standard and multi function components

The number of subfunctions per device is device-specific, and is stored as a device parameter <Count RT-Autos> in the Profinet Component Description (PCD). With multi function components of Profinet devices with proxy functionality, the functions or subfunctions of the coupled Profibus devices are also included in the calculation of the total quantity of subfunctions.

Singleton Components

Singleton components are Profinet components without vendor-specific device data. However, they do contain device data, although these are not part of the Profinet component but are present in a separate device-dependent form and are managed separately. In particular, this means that these data are not managed by Simatic iMap when configuring the distributed plant. Separate storage of the device-specific configuration and program data provides several advantages:

- Exclusion of particular functions such as generation or program download in Simatic iMap; therefore no influence on the processing time of the complete project.
- Facility for presetting names and addresses. It is then unnecessary to configure these properties for instances of the singleton components in Simatic iMap.

Whereas, for example, a new Step 7 project (Step 7 shadow project) which describes the total plant is created from the existing Simatic device data of all Profinet components in Simatic iMap, the device data of a singleton component are still present in their Step 7 basic projects following creation of the component. Uploading of the device data during commissioning is carried out for singleton components from the proprietary engineering tool. For Simatic devices, this is the Simatic Manager.

The singleton concept permits incorporation of previously non-supported hardware configurations with Simatic devices as part of a Profinet component into the Profinet CBA communication. These include, for example:

- Configurations with several CPUs (multi-computing)
- Integration of configurations with connections to other stations, e.g. using ISO or S7 protocol
- Applications with process diagnostics or
- Function modules (FM) as a component of intelligent Profibus DP slaves.

It is always the case that if a singleton component is generated from a Profinet device, the proxy functionality – if present – cannot be used with this Profinet device.

5.4.4 Device Configurations with Assignable Components

Profinet components can be created for:

- Profinet controllers with or without local (subordinate) Profibus DP master system, MPI bus system or Profinet IO Subsystem

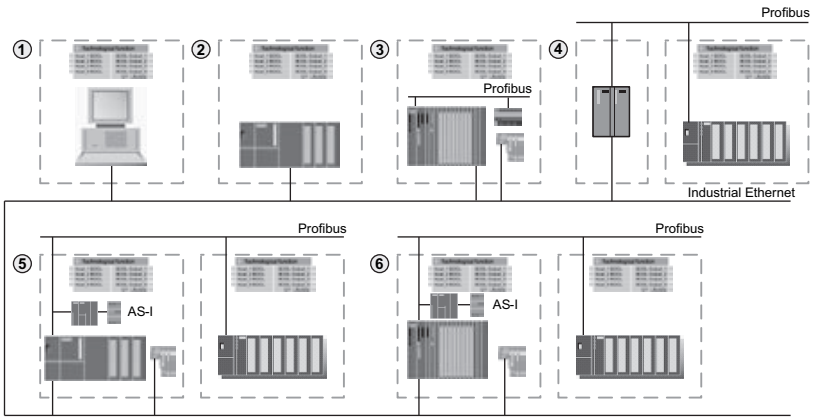
- Intelligent Profibus DP slaves with or without local Profibus DP master system or MPI bus system
- Profibus DP standard slaves with GSD file.

Profinet components with Profinet controllers

Profinet components can be created from the following Profinet controllers (Fig. 5.19):

Singleton components with any permissible device configuration can be created from configurations 1 and 2 of Fig. 5.19.

Profinet controllers with Profibus interface can simultaneously be DP masters of a local DP master system. In turn, intelligent Profibus DP slaves on this DP master



1 Windows Logic Controller WinLC PN and WinAC PN-Option V4.1:
Profinet device with proxy functionality. Local DP slaves and/or local HMI devices can be connected to the subordinate Profibus.

2 S7-300 CPUs with a communications processor with Profinet capability (e.g. Simatic Net-CP 343-1):
These device configurations do not have proxy functionality, but can nevertheless use local subnets, e.g. Profibus DP master systems or a local MPI bus.

3 S7-400 CPUs with a communications processor with Profinet capability (e.g. Simatic Net-CP 443-1 Advanced):
These device configurations do not have proxy functionality, but can nevertheless use local subnets, e.g. Profinet IO systems, Profibus DP master systems or a local MPI bus.

4 Simatic Net IE/PB Link gateway as Profinet device with proxy functionality, but without own technological function.
Local DP slaves cannot be connected to an IE/PB Link. The Profinet component for the IE/PB Link is provided for different Profibus baud rates of Step 7.

5 Simatic S7 CPU 31x-y PN/DP:
Profinet devices with proxy functionality. The CPU has an integrated Profinet interface. Local DP slaves and/or local HMI devices can be connected on the local Profibus. The Profinet interface can also be used for Profinet IO.

6 Simatic S7 CPU 41x-y PN/DP:
Profinet devices with proxy functionality. The CPU has an integrated Profinet interface. Local DP slaves and/or local HMI devices can be connected on the local Profibus. The Profinet interface can also be used for Profinet IO.

Fig. 5.19 Profinet components with Profinet controllers

system can also operate as a DP master on their own local DP master system. Parallel operation of Profinet CBA and Profinet IO over the Profinet interface is also possible with the latest CPUs.

DP slaves on a local DP master system as well as IO Devices which are part of a Profinet component together with the Profinet controller are never visible in Simatic iMap and are not involved in the Profinet CBA communication. However, Profibus addresses of these DP slaves and IP addresses of the IO Devices are recognized by Simatic iMap as being occupied.

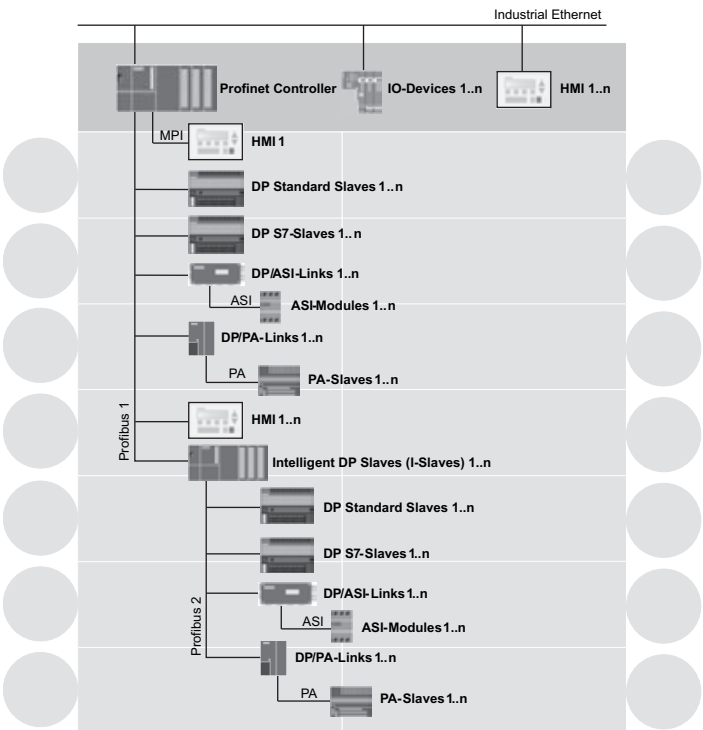


Fig. 5.20 Maximum configuration of a Profinet controller with local MPI, Profibus and Profinet IO System

During the program download, the programs of the intelligent DP slaves on the local DP master system are also loaded automatically. However, the download to an HMI device on the local MPI bus can only be carried out using the HMI engineering system, e.g. ProTool/Pro CS.

Fig. 5.20 shows the maximum configuration of a Profinet component, consisting of a Profinet controller with local Profibus and local MPI bus, local DP master system and an IO System.

Profinet components with IO Devices

If cyclic data exchange over Profinet IO and Profinet CBA is to take place on the same Ethernet subnet, the communications share reserved for Profinet IO must be defined during configuration of the Profinet controller. This is carried out using the parameter “Communication component” in the properties dialog of the Profinet IO System (Fig. 5.21).

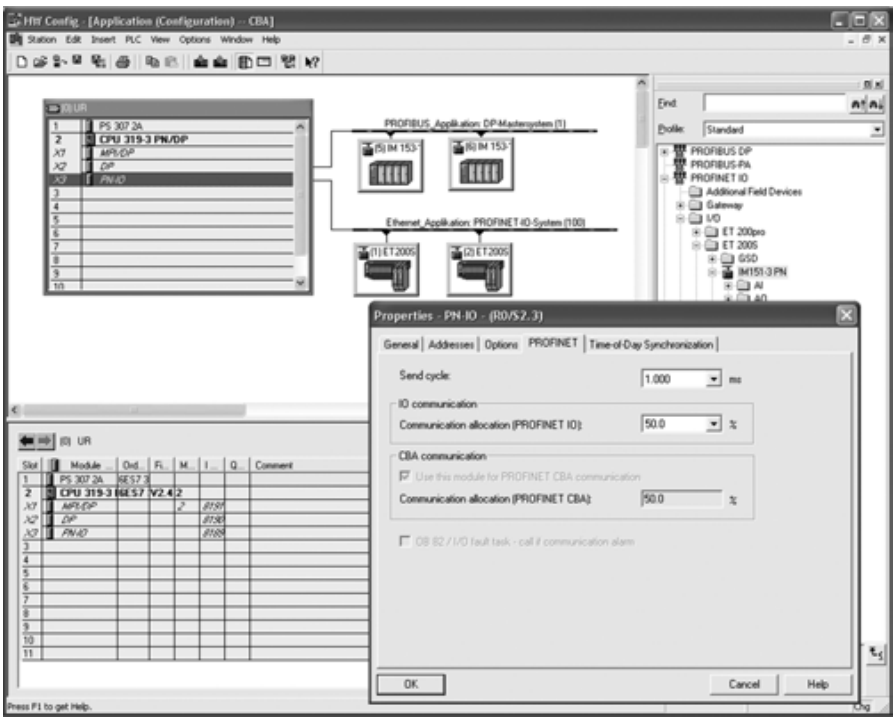


Fig. 5.21
Setting of the communications share of Profinet IO in the total Profinet communication

The shares to be set here only apply to cyclic data exchange. A sufficient share of the time is reserved in the system for acyclic data (e.g. for PG access). With a setting of 100%, the available capacity is exclusively reserved for Profinet IO data exchange. Changes in the communications share for Profinet IO may have effects on the update time of IO Devices.

Send clock

Step 7 automatically calculates the update times from the existing hardware configuration and the set send clock. The update times are the smallest possible period between two successive send/receive intervals with RT or IRT communication. The actually calculated updating times are a multiple of the send clock. This time

includes the cyclic data, the module properties, and the configured communications share for Profinet IO. The calculated send clock can be manually increased, but not decreased.

Profinet components with Profibus devices

Profinet components can also be created from Profibus devices with programmable functionality such as Simatic S7 CPU 31x-2DP or Simatic S7 CPU IM 151-7.

If these devices possess a second Profibus/MPI interface, they can simultaneously be the DP master of a local DP master system or MPI bus (Fig. 5.22). The devices connected there are not visible in Simatic iMap.

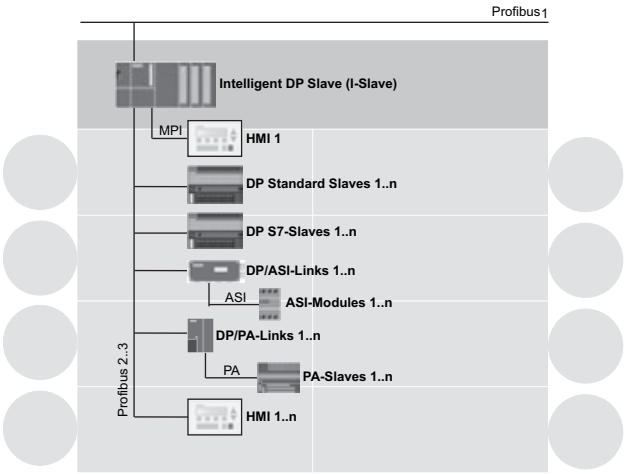


Fig. 5.22 Maximum configuration of a Profibus device with programmable functionality and local MPI and Profibus

Profibus devices with fixed functionality, e.g. a Simatic ET 200S IM 153-x, cannot be programmed. The user program is executed in the DP master in this case. Fig. 5.23 shows the configuration possibilities for Profinet components of such Profibus devices.

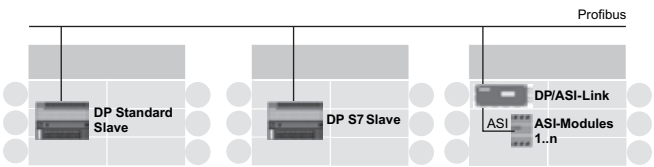


Fig. 5.23 Examples of configurations with Profibus devices with fixed functionality

Profinet components with HMI element

Profinet components can be supplemented by an HMI element. The required expansion of the PCD is carried out in a separate engineering step referred to as merging. This enables Profinet components to be integrated in a predefined design into an HMI system. With Simatic WinCC Flexible it is possible to create faceplates at the HMI engineering stage. Faceplates define the variables of the Profinet components to be visualized as well as the design for their subsequent display in the HMI system.

Illegal configurations

Illegal configurations for Profinet components are:

- Connection of intelligent DP slaves to the local DP master system of an intelligent DP slave.
- Connection of intelligent DP slaves via a Simatic Net Profibus CP to a local DP master system of the Profinet controller.
- Configurations of standard and S7 slaves with fixed functionality and containing programmable modules, e.g. FMs and CPs.
- Configurations with a Simatic Net CP as DP slave.
- Combination of several stations or DP slaves without DP master system into one Profinet component.

5.4.5 Profinet Component Description (PCD)

A Profinet component can possess vendor-specific configuration and program data as an option. Characteristic, however, is the existence of a Profinet Component Description (PCD).

The PCD is usually created by the plant or machine constructor using the respective vendor-specific engineering tool (e.g. Step 7). A prerequisite is that a component generator is integrated in the engineering tool.

The PCD contains the following information on functions and objects of the Profinet component:

- Information on creation tool as well as compatibility information.
- General information such as name, UUID, etc.
- Information on device-specific parameters.
- Description of the technological interface.
- Information on the storage location of the component project.

All Profinet CBA engineering tools are able to interpret a PCD. This is saved as an XML file. XML (Extensible Markup Language) is a metalanguage defined by the World Wide Web Consortium (W3C) with the facility for presenting information in a multi-platform and multi-vendor format. The structure of the PCD conforms to

the ISO 15745 “Open Systems Application Integration Framework”, and is oriented according to the device profile defined there. A detailed description of the PCD structure can be found in the “Profinet Architecture Description”.

5.5 Creation of Profinet Components with Step 7

There are basically two possibilities for creating a Profinet component:

- From the complete station of a project in Step 7 or
- From one of the DP slaves with fixed functionality within a station.

The creation of Profinet components using the Simatic Manager is carried out in the following steps:

- Creation of the Step 7 basic project. The Profinet component is subsequently generated from the project station.
- Configuration of hardware and programming of modules in HW-Config.
- Definition of the Profinet interface of a programmable controller using the Interface Editor.
- Copying of blocks from the system supplies into the block folder of the S7 program, and creation of the program for the station.
- Creation of the Profinet components.

5.5.1 Creation of a Step 7 Basic Project

Simatic CPUs – both Profinet controllers and intelligent DP slaves – are configured as independent stations within a Step 7 project. This project is referred to as the Step 7 basic project. Configuration of Profibus devices with a fixed functionality, such as Simatic ET 200S IM 153-1, is carried out as a Profibus slave within a Profibus DP master station. Programming is carried out as previously with one of the LAD, FBD or STL languages, and the configuration using HW-Config.

5.5.2 Loading of User Program Cycle by Communications Processes

The communications processes always influence the user program cycle (OB 1 cycle) to a certain extent. The duration of communications processes, e.g. the data transmission to another CPU, can be controlled within a certain range using the parameter “Scan Cycle Load from Communication” (Fig. 5.24).

The operating system of a Simatic S7 CPU continuously provides the communications process with the configured percentage of the total CPU processing capacity (time slice procedure). If this processing capacity is not required for communications, it is available for the remaining processing functions.

Test functions with the programming device (PG) are only influenced by this parameter by an insignificant amount: you can considerably increase the cycle time.

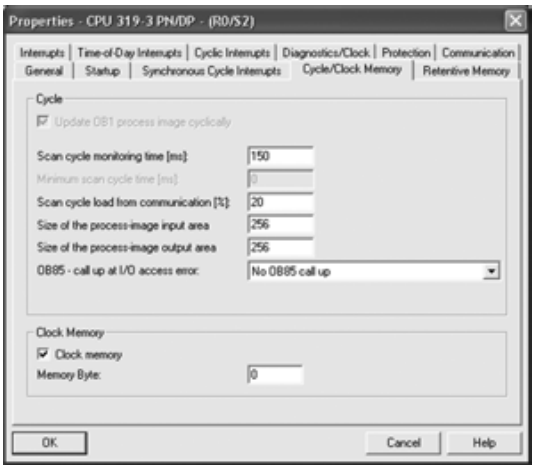


Fig. 5.24
Parameter "Scan Cycle Load from Communication" in the properties dialog of a CPU

The time made available for test functions can be limited in process operation depending on the CPU.

Effect on the actual cycle time

Without additional asynchronous events, the cycle time is extended by a factor which can be calculated using the following equation:

$$\text{Cycle time} = \frac{100}{100 - \text{“Scan cycle load from communication” (\%)}}$$

Example 1: Cycle time without consideration of additional asynchronous events

With a setting for "Scan cycle load from communication" of 50%, the OB 1 cycle time may be doubled.

Example 2: OB 1 cycle time with consideration of additional asynchronous events

The OB 1 cycle time can also be influenced by asynchronous events, e.g. process or watchdog alarms, in addition to the communications load. Through extension of the cycle time by the communications share, more asynchronous events also occur statistically within an OB 1 cycle. This in turn additionally lengthens the OB 1 cycle. This extension depends on the number of events per OB 1 cycle and the duration of event processing.

With a pure OB 1 execution time of 500 ms, a communications load of 50% can result in an actual cycle time of up to 1,000 ms. If a watchdog alarm with an execution time of 20 ms is carried out parallel to this every 100 ms, this would increase the cycle – without communications load – by a total of 5 · 20 ms = 100 ms. The actual cycle time in this case would be 600 ms. Since a watchdog alarm also interrupts communication, it has an effect of 10 · 20 ms on the cycle time with a com-

munications load of 50%, i.e. in this case the actual cycle time is not 1,000 ms but 1,200 ms.

Changes in the value of the parameter “Scan cycle load from communication” always have an effect on plant operation. The communications load must be considered when setting the minimum cycle time, otherwise time errors will result. The following is always applicable:

- The default value should be used if possible.
- The default value should only be increased if the CPU is mainly used for communications purposes and if the user program is not time-critical.
- In all other cases, the value should only be reduced.
- When configuring Profinet components, the parameter “Scan cycle load from communication” should be at least 50%.

5.5.3 Creation of the Profinet Interface

The Profinet interface of a device corresponds to its technological interface. Each function is represented by data blocks, so-called Profinet interface DBs. The external inputs and outputs of the Profinet component are declared in the Profinet interface DB (Fig. 5.25).

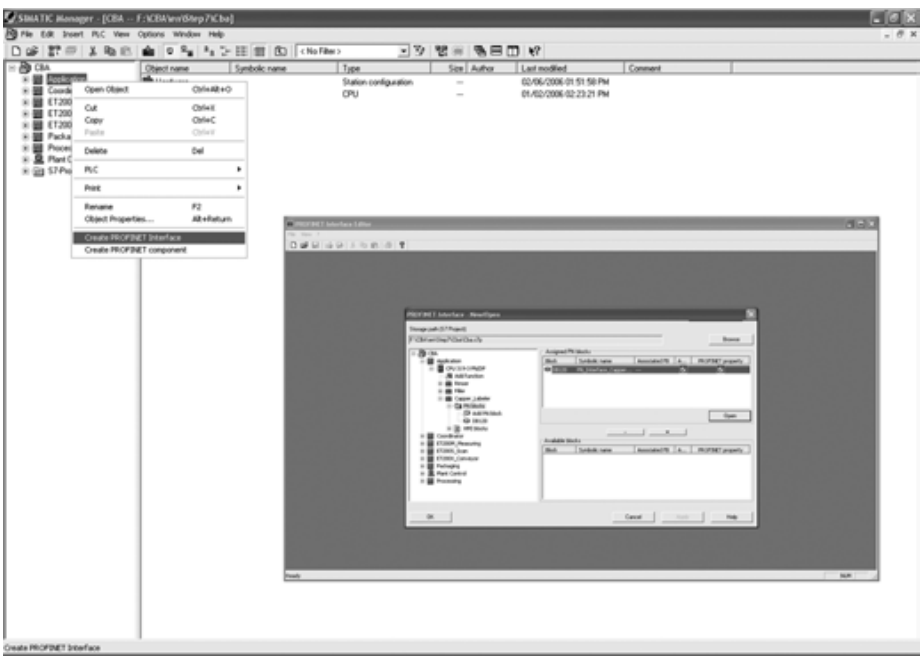


Fig. 5.25 Creation of the interface DB

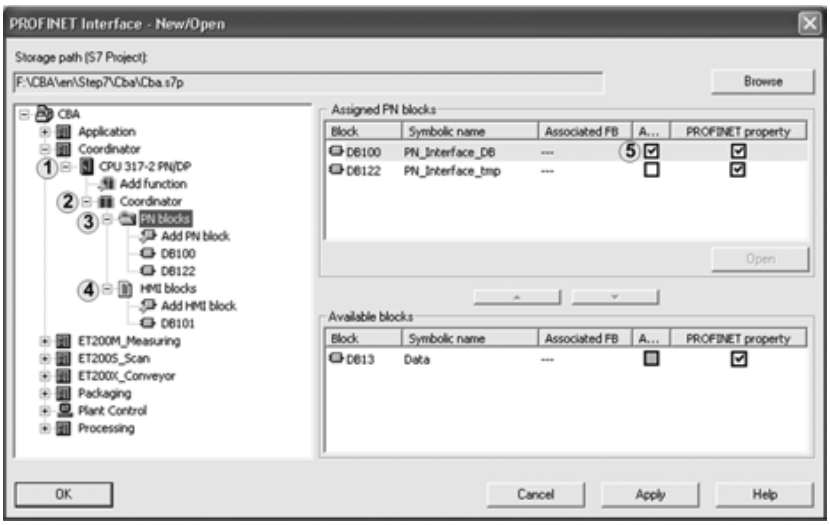
Profinet interface DB

The Profinet interface DBs contain the interface definitions of the Profinet components. They are created and edited using the Profinet Interface Editor integrated in Step 7. The Profinet Interface Editor is called using the context menu of the respective station.

The Profinet interface DB always has a fixed assignment to a device, and to a function of the device. Several Profinet interface DBs can be present in the Step 7 basic project, of which only the one which is switched to active is considered during creation of the Profinet component.

Profinet interface DBs represent the function or subfunctions of a Profinet component. A separate interface DB is assigned to each subfunction. The interface DBs contain the data of all inputs and outputs of the device's technological interface and are updated during runtime by the operating system and/or special program blocks depending on the device and its configuration. Specific to the device, an interface DB can also contain connections which cannot be linked, so-called S7 variables. These connections are only accessible using S7 protocols, and can be used by HMI/MES systems such as the S7 OPC server.

Profibus devices with a fixed functionality do not have their own user program. The Profinet interface DB of such a device is saved in the block container of a temporary DP master station to which the Profibus device is assigned. If a DP master station contains several DP slaves, correspondingly more interface DBs can be present in the block container: one interface DB per DP slave from which a Profinet



1 Device
2 Function
3 Profinet interface DB
4 HMI interface DB
5 Active Profinet interface DB

Fig. 5.26 Example of the assignment between interface DB, device and function

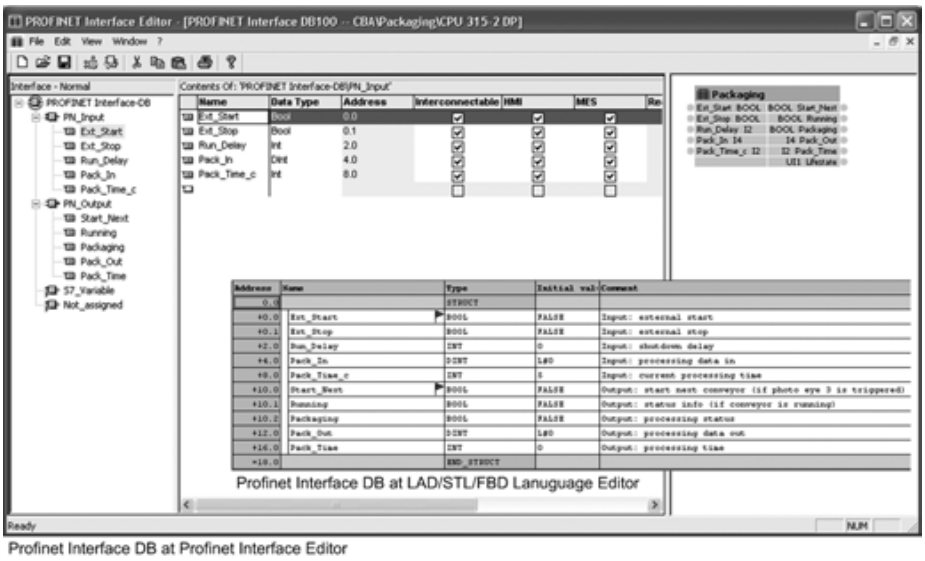


Fig. 5.27 Profinet interface DB in the Profinet Interface Editor and in the LAD/STL/FBD language editor

component is to be created. Interface DBs for Profibus devices with a fixed functionality are only required temporarily for creating the Profinet interface, and are not used further in the subsequent engineering phases (Fig. 5.27).

HMI interface DB

In order to achieve a clear separation between variables of the Profinet interface and HMI data in the case of large interface DBs, it is possible to export HMI data

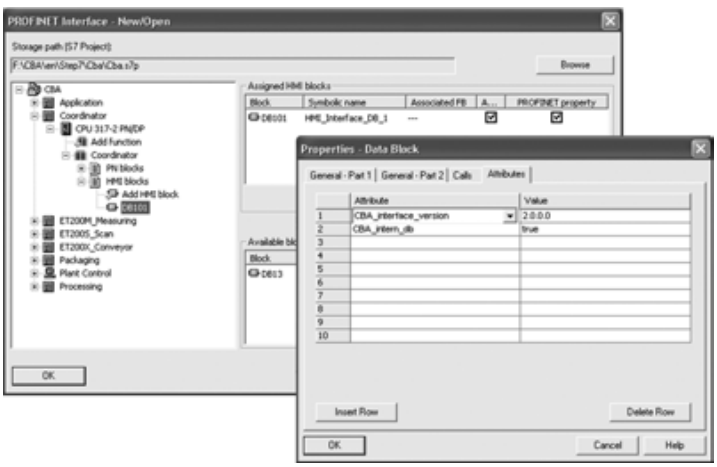


Fig. 5.28 Creation of the HMI interface DB

into separate data blocks, so-called HMI interface DBs. These data are not visible in the Profinet interface, and cannot be connected either. HMI interface DBs are also created using the Interface Editor (Fig. 5.28). When saved, they are assigned the attribute “CBA_intern_db”.

Structure of the Profinet interface DB

The correct structure of an Profinet interface DB is guaranteed by the Profinet Interface Editor. However, a number of conditions must be observed in the design:

- The maximum size of the Profinet interface with Profibus devices with programmable functionality (I slaves) depends on the device and is typically between 32 and maximum 244 byte.
- The maximum size of an individual connection in the Profinet interface of Profibus devices is limited to 32 byte. This limit results from the maximum size of data which can be transmitted consistently between DP master and slave. In addition, this particularly means that a maximum of 30 characters are possible for a variable of data type STRING.
- The maximum connection size in the Profinet interface of Profinet controllers is basically unlimited. However, it may be subject to device-dependent limitations.
- The maximum size of an individual connections of combined data types as well as the length of variables of data type STRING are also device-dependent.
- Depending on the device type, limitations are possible with respect to the scope of supported data types as well as the respective ranges of values.

Four areas exist in the interface DB for definition of the Profinet interface (Table 5.2).

When observing an interface DB in the LAD/STL/FBD language editor of the Simatic Manager, the declaration lines of a variable, the definition of a connection, or special components as delimiters or dummy elements are visible. The declaration lines of the inputs constitute the input section (PN_Input), those of the outputs the output section (PN_Output) of the interface DB. The declaration lines of the inputs are present before those of the outputs.

Each section contains variable declarations. A variable declaration corresponds to a connection of the Profinet interface. Variables possess specific properties which

Table 5.2 Areas in the Profinet interface DB

Area	Meaning
PN_Input	This area contains the inputs of the Profinet interface of a Profinet component accessible using Profinet protocols.
PN_Output	This area contains the outputs of the Profinet interface of a Profinet component accessible using Profinet protocols.
S7_Variable	This area contains the connections which cannot be interconnected for HMI/MES. The variables defined here can be accessed during runtime using S7 communications mechanisms. None of these variables is visible in Simatic iMap. This area is only present in devices with programmable functionality.
Not_assigned	These variables are not (yet) assigned to any area of the Profinet interface.

Table 5.3 Variable properties

Attribute	Meaning
Name	Name of connection.
Data Type	Data type of connection (e.g. BOOL, WORD, STRING).
Address	Address of variable in the Profinet interface DB; format: BYTE.BIT
Interconnectable	With this option selected, the connection is visible in the plant view of Simatic iMap and can be interconnected. The connections of the Profinet interface are displayed in the right-hand window of the editor. An Profinet interface DB must possess at least one interconnectable connection.
HMI	With this option selected, the variable is accessible for HMI via OPC.
MES	With this option selected, the variable is accessible for MES via OPC.
Read-only	With this option selected, the variable can only be read.
Initial value	The value of the connection which is imported as the current value when the object is saved for the first time.
Comment	Comment on the connection.

are assigned to them in the Profinet Interface Editor. The possible properties of a variable are listed in Table 5.3.

Data types

Each connection of the Profinet interface has a defined format which is mapped in the data types of the variables in the Profinet interface DB, and thus the Simatic S7 format. Table 5.4 shows a comparison between Profinet CBA data types and the corresponding Simatic S7 data types.

Table 5.4 Data types with Profinet CBA and Simatic S7

Profinet CBA data type	Simatic S7 data type	Data link/byte	Range of values with Simatic S7
BOOL	BOOL	2	TRUE / FALSE
UI1	BYTE	1	0 to 255
UI2	WORD	2	0 to 65,535
UI4	DWORD	4	0 to 4,294,967,295
I1	CHAR	1	–128 to +127
I2	INT	2	–32,768 to +32,767
I4	DINT	4	–2,147,483,648 to +2,147,483,647
R4	REAL	4	±3.4E +/- 38
DATE	DATE_AND_TIME	8	01.01.1990 00:00:00 to 31.12.2089 23:59:59
BST_n	STRING[n]	4 + 2 · n	String; n: 0 to 255
ARRAY	ARRAY[1..n] m	n · data type length	m: data type of array element. Arrays and structures may only comprise simple data types. Simple data types are all types except ARRAY and STRUCT. The range of values corresponds to the ranges of the respective array/structure elements.
STRUCT	STRUCT, UDT	Total length of all data types	

Interface DB with Profibus devices with fixed functionality

With an Profinet interface DB for Profibus devices with fixed functionality, the sections “PN_Input” and “PN_Output” are divided into slots (Fig. 5.29). These correspond to the slot of an input or output module of the DP slave.

- Outputs of the DP interface of the DP master are mapped in slots of the section “PN_Input”. The inputs of the technological function are defined in this section.
- Inputs of the DP interface of the DP master are mapped in slots of the section “PN_Output”. The outputs of the technological function are defined in this section.
- A connection must not be declared beyond slot limits.

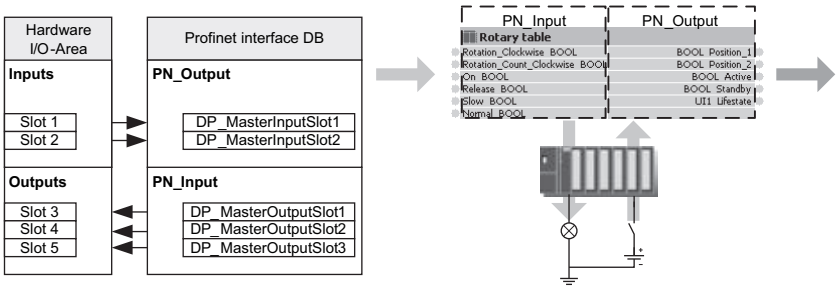


Fig. 5.29 Structure of the Profinet interface DB with Profibus devices with fixed functionality

The maximum permissible data length of a connection corresponds exactly to the consistency length of the slot. The consistency length is usually:

- 1 byte (8 bits) for digital inputs or outputs
- 1 word (16 bits) for analog inputs or outputs.

Depending on the module type, the consistency length can be configured in HW-Config.

Several connections can be declared within a slot. However, the data length of a connection must not be larger than the data length of the slot for which it is defined. Unused areas of a slot must be occupied by a dummy element according to their length (BOOL, BYTE, WORD, etc.).

Data exchange between Profinet controller and Profibus devices

To permit Profinet data to reach the user program of an intelligent DP slave connected via proxy, the data must be synchronized between its interface DB and I/O address area during runtime. This task is carried out by the functions FC 10 “PN_IN” and FC 11 “PN_OUT”. These are made available by Step 7 in the Profinet system library. No special (system) functions are required for use of Profibus devices with fixed functionality (Fig. 5.30).

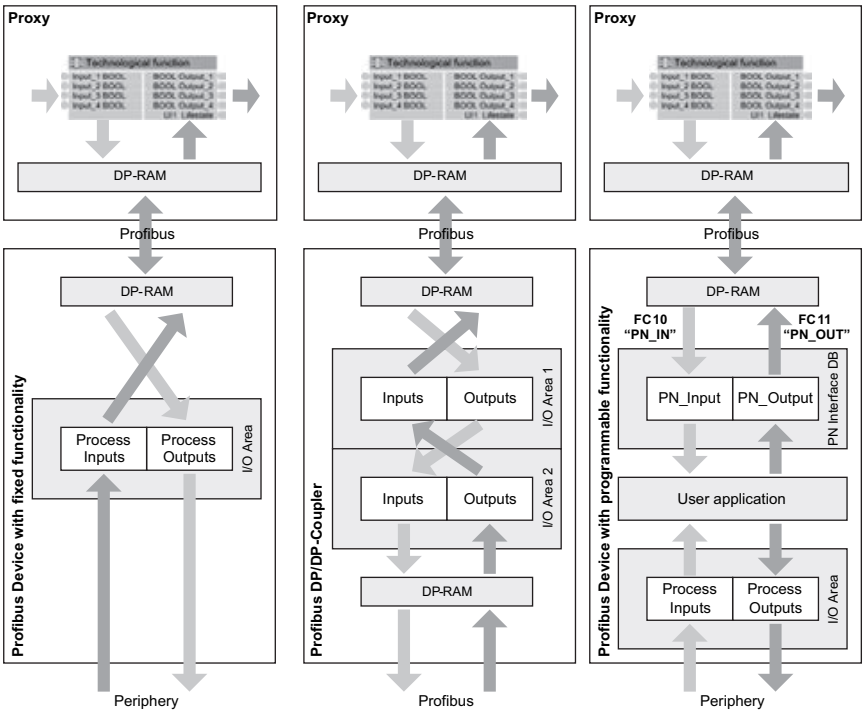


Fig. 5.30 Profinet data flow with Profibus devices

5.5.4 Creation of Profinet Components

The creation of a Profinet component for Simatic PLCs is carried out in the Simatic Manager of Step 7 (Fig. 5.31). A prerequisite is a complete Step 7 basic project, i.e. individually:

- The S7 application program including the Profinet interface DB has been created and tested.
- The HW configuration and the parameterization of the modules have been completed.
- The files with the icons for representation of the Profinet components and their elements, the technological functions and the device are available. The icons are used for the graphic representation in Simatic iMap. If no component-specific icon files are available, the icon files delivered by Simatic iMap can be used.
- The documentation of the future Profinet component has been completed (optional).

The following processes take place during component assignment:

- A Profinet component description (PCD) is generated from the Profinet interface DB and the configuration data of the PLC.

Fig. 5.31
Creation of a Profinet component

- In the case of Profinet components with device data, the station data of the PLC with created components are extracted from the Step 7 basic project and saved in a separate Step 7 component project and/or in a library.
- In the case of singleton components, the station data of the PLC with created components are supplemented in the Step 7 basic project by the information relevant to Profinet CBA communication.

5.6 Profinet CBA Communication

Communication in Profinet CBA is based on Ethernet. Simatic Profinet controllers work in line with the 100BASE-TX specification standardized by IEEE 802.3u. This results in a transmission rate of 100 Mb/s. Smaller transmission rates are basically also possible on the path between engineering system and Profinet controller, for example when using WLAN links. However, 100 Mb/s is obligatory to guarantee high-performance exchange of process data between Profinet controllers.

5.6.1 Interconnections

Communication links between the connections of technological interfaces of a device are called interconnections. These are used to exchange process data between Profinet controllers, and are configured in Simatic iMap. The following rules apply to interconnections:

- Connections can be interconnected if they are of the same data type. Connections of combined data types must have identical types, i.e. arrays and structures have the same format.
- Outputs can be interconnected to several inputs, but inputs to only one output.

Interconnections are immediately and automatically established by the Profinet controller following loading of the interconnection configuration. Interconnection

management and data exchange are based on a provider/consumer model. In addition to interconnections for exchange of process data, there are non-configurable HMI connections for operation and monitoring of technological interfaces via OPC and special status connections for calling device-specific information by Profinet CBA engineering systems.

Consumer and provider

Profinet CBA establishes a provider/consumer model for exchange of process data (Fig. 5.32). The consumer (receiver) of a technological function corresponds to an input. It is also the receiver of the interconnection configuration, and immediately and automatically commences to establish the corresponding interconnection to the communications partner following receipt of the configuration information. Its pendant is the provider (transmitter). It corresponds to an output and is therefore the data source of an interconnection.

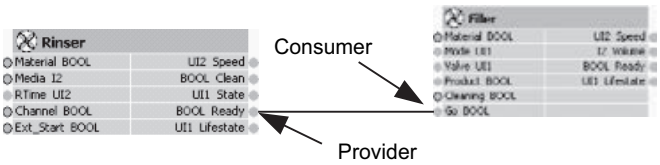


Fig. 5.32 Consumer and provider shown by example of two functions in Simatic iMap

Interconnection types

Three different types of interconnection can be configured:

- Constants: these supply an input with a constant value. They are used, for example, when testing technological functions.
- Acyclic interconnection: this type of interconnection is used to exchange process data which are not time-critical. An output value is determined by the provider at a configurable sampling frequency, and transmitted when the value changes. Data transmission is carried out using the ORPC wire protocol and TCP/IP.
- Cyclic interconnection: this type of interconnection is used for real-time exchange of time-critical process data. An output value is transmitted by the provider at a configurable frequency independent of whether it changes. Data transmission is carried out using the Profinet real-time protocol.

Local and remote interconnections

If the communications path of an interconnection is over the Ethernet, it is a remote interconnection, otherwise a local one.

Local interconnections are:

- Interconnections between Profibus devices on the Profibus of a Profinet controller with proxy functionality.

- Interconnections between a Profinet controller and its Profibus devices coupled by a proxy functionality
- Interconnections between connections of the same Profinet controller or its Profibus device.

Data exchange over a local interconnection takes place exclusively within the operating system of a Profinet controller. It is irrelevant whether the interconnection has been configured as acyclic or cyclic.

Quality of Service and frequency levels

The Quality of Service (QoS) is a quality feature of interconnections, and is specified in milliseconds. It is defined by the following two parameters depending on the type of interconnection:

- Scanning frequency: this is the maximum time interval which passes before a change in value is transmitted from the provider to the consumer. The scanning frequency is a feature of acyclic interconnections.
- Transfer frequency: this is the time interval at which a provider transmits data cyclically to the consumer. The transfer frequency is a feature of cyclic interconnections.

The QoS is set in Simatic iMap on the basis of the frequency levels Fast/Medium/Slow. Each frequency level corresponds to a QoS value (see Tables 5.5 and 5.6). The minimum possible QoS value of an interconnection is defined by the performance parameters of the respective Profinet communications partner.

Table 5.5 Recommended values for assignment of QoS to frequency levels in cyclic interconnections

Frequency level	Fast				Medium			Slow		
QoS in ms	1	2	5	10	20	50	100	200	500	1000

Table 5.6 Recommended values for assignment of QoS to frequency levels with acyclic interconnections

Frequency level	Fast							Medium	Slow	
QoS in ms	1	2	5	10	20	50	100	200	500	1000

Substitute values

If a consumer recognizes an invalid or faulty value, for example because of interferences in data transmission, it applies a substitute value instead of the received input value. The period until application of a substitute value is calculated as follows:

Cyclic interconnections: $t_{\text{substitute value}} = 4 \cdot \text{transmission frequency}$

Acyclic interconnections: $t_{\text{substitute value}} = 20 \cdot \text{sampling frequency}$

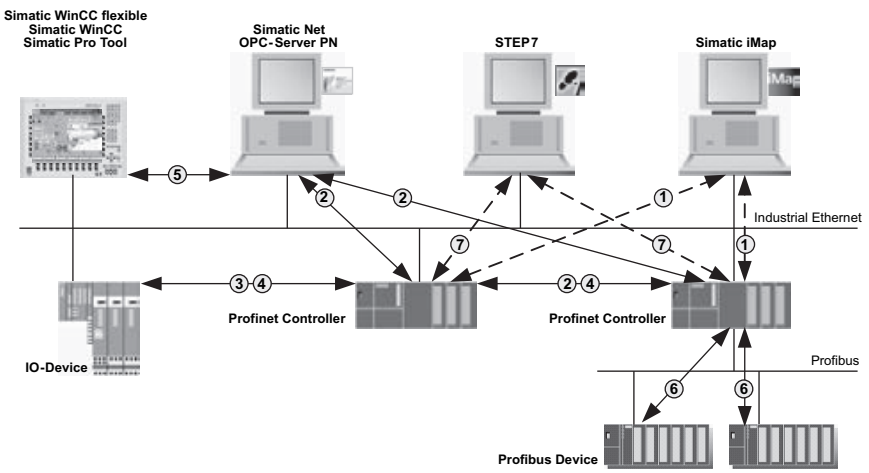
In the case of interconnections between Profinet controllers, substitute values can be configured as part of the interconnection properties.

No substitute values can be configured for interconnections to Profibus devices. In this case, an input value is always set to the safe value 0 in the event of a fault. This results in a uniform input response in the event of communication faults on the Ethernet and Profibus.

Protocols

The basis of Profinet CBA communication is the application of open standards. The basis of all communication between Profinet devices is Ethernet according to IEEE 802.3. Acyclic communication between Profinet controllers is carried out using TCP/IP, which is also the protocol for communication between HMI/engineering systems and Profinet controllers. In both cases, access to engineering or process data within a Profinet controller is through application of the ORPC wire protocol. With cyclic communication, the Profinet real-time protocol (RT Class 1) is used (see Fig. 5.33).

Fieldbus systems such as Profibus integrate Profinet into Profinet controllers through implementation of a corresponding proxy functionality.



No.	Protocol	Field of use
1	TCP/IP, ORPC wire protocol	Profinet CBA Engineering
2	TCP/IP, ORPC wire protocol	Profinet CBA Runtime
3	UDP/IP, RPC	Profinet IO Runtime
4	Real-time protocol	Profinet CBA Runtime/ Profinet IO Runtime
5	TCP/IP, ORPC wire protocol	HMI/MES
6	Profibus DP	Profibus
7	TCP/IP, S7 communication	Configuration, programming

Fig. 5.33 Communication protocols with Profinet CBA

Interconnection dynamics

A Profinet controller receives the information concerning the interconnections to be established either from a Profinet CBA engineering system, e.g. Simatic iMap, or from the saved interconnection configuration following a warm restart. Following interpretation of this interconnection information, establishment of the interconnection is commenced automatically at the consumer end. If an interconnection has been successfully initialized, the provider (output) transmits productive data to the consumer (input) according to the configured QoS value.

In the reverse direction, the consumer initiates clearance of the interconnection if interconnections are deleted by the Profinet CBA engineering system. Establishment and clearance of the interconnection are carried out by a handshake procedure between consumer and provider. The consumer always plays the active role in this procedure. Monitoring of the interconnections is carried out by the data security properties of the protocols used as well as special monitoring mechanisms at the consumer and provider ends.

5.7 From Planning to Operation of a Plant

The plant engineering process for a distributed automation solution is carried out in steps. Different groups of persons are involved from planning up to operation of a plant (Table 5.7).

Table 5.7 Distribution of tasks for the plant engineering of distributed automation solutions

Group of persons	Task
Plant planner	Planning of the plant.
Plant and machine constructor	Creation of Profinet components using a vendor-specific configuration and programming tool.
Configuration engineer	Configuration of the plant using SimaticþiMap.
Plant operator	Commissioning and testing of the plant.

5.7.1 Planning of the Plant

Prior to commencement of the actual plant engineering, the plant planner initially defines the fundamental conditions concerning the plant architecture. The result is a plan which is used as the basis for the further procedure (Table 5.8).

Table 5.8 Procedure when creating Profinet components

Step	Activity
1	Definition of the required functions
2	Definition of the automation and field devices used.
3	Definition of the functions which can be combined into reusable technological modules.
4	Definition of the technological interfaces as well as the variables for diagnostics and visualization.
5	Definition of the interaction of the Profinet components.

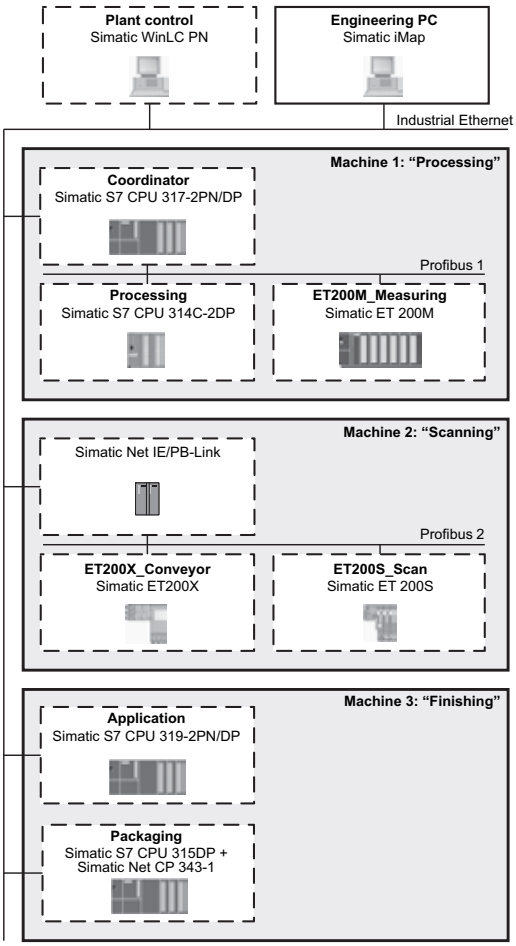


Fig. 5.34
Profinet CBA example plant

The following example plant consists of three machines and central plant control. Each machine consists of at least one Profinet device (Fig. 5.34).

5.7.2 Creation of Profinet Components with Step 7

This step comprises selection of one or more appropriate PLCs for implementation of the technological task, definition of the technological interface, and – with programmable devices – production of the control program. Following successful testing, a Profinet component is generated from the configuration and program of the PLC used (Table 5.9). Following successful testing, a Profinet component is generated from the configuration and program of the PLC used.

The creation of Profinet components is the task of the plant or machine constructor. Knowledge of the respective vendor-specific configuration and programming tools, for example Step 7, is necessary to carry out this task (Fig. 5.35).

During creation of Profinet components using Step 7, a check is carried out whether the parameter "Cycle load due to communication" has a sufficient value in the properties window of the respective station. If the value selected was too small, the window shown in Fig. 5.36 is displayed. In this case, creation of the component should be stopped, and the value of the parameter increased in the CPU properties window.

Table 5.9 Procedure when creating Profinet components

Step	Activity
1	Configuration and parameterization of device hardware used.
2	Creation of technological interface description (Profinet interface) using the Profinet Interface Editor.
3	Optional: creation of the user program for devices with programmable functionality.
4	Testing of the finished technological module.
5	Creation of the Profinet components.
6	Optional: importing of Profinet components into a SimaticþiMap library.
7	Addition of an HMI element to the Profinet component (merging).

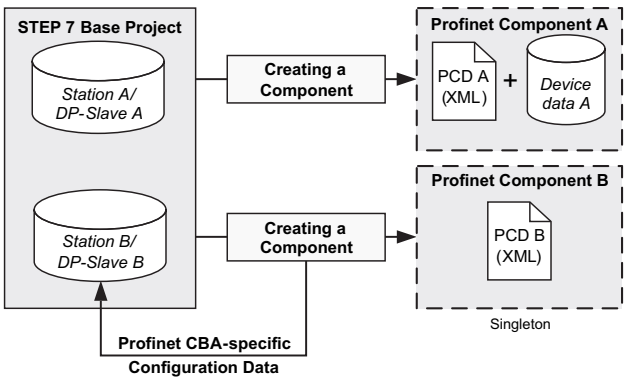


Fig. 5.35 Principle for creating components with Simatic S7 automation devices

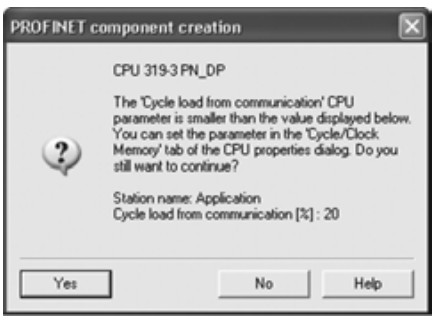


Fig. 5.36
Checking of the parameter "Cycle load due to communication" during creation of a Profinet component

Configuration facilities when creating Profinet components

Prior to commencement of component creation, it is necessary to make component-specific settings. This is carried out in the dialog *"Create Profinet component"* (Figs. 5.37 to 5.42 and Tables 5.10 to 5.15).

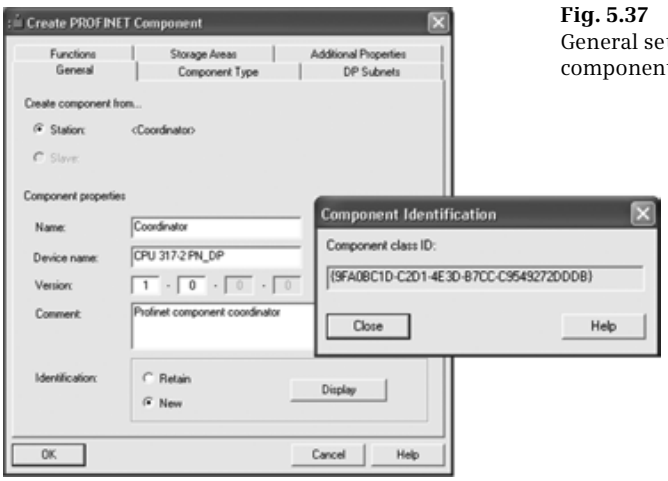


Fig. 5.37
General settings during component creation

Table 5.10 Parameters in the tab "General"

Parameter	Meaning
Create component from ...	... Station: the Profinet component is created from the station. ... Slave: the Profinet component is created from a DP slave of the station.
Name	Name of the Profinet component. The Profinet component appears with this name in the library.
Device name	Name of the device of the Profinet component. This serves as the basis for the default names of the device instances of the Profinet component.
Version	Version of the Profinet component. A Profinet component has a version number which, together with the identification (class ID), results in an unambiguous specification of the component. This guarantees that a newly created Profinet component does not overwrite an earlier version by mistake. The first two positions of the version number (User Version) can be assigned as desired (max. 3-digit), e.g. 01.04.The last two positions of the version number (Build Version) cannot be changed, they are automatically incremented. The following is applicable: – The last position (Minor Build Version) is incremented by one following each new and successful creation of the Profinet component. – The penultimate position (Major Build Version) is incremented by one following each change in a Profinet interface DB. The last position is automatically set to 0 at the same time.
Comment	Comment on the Profinet component
Identification	The identification (class ID) of the Profinet component is unambiguous, and is oriented according to the COM standard. Simatic iMap identifies Profinet components according to their class ID and version number. New: A new identification is created. Retain: The identification is retained. In this case the Profinet component is only assigned a new version number.

Fig. 5.38
Settings of the component type

Table 5.11 Parameters in the tab "Component type"

Parameter	Meaning
Component type	Standard component: A standard component is created with device data. With proxy functionality: The station contains a Profinet-compatible device with proxy functionality, and a DP master system is configured for the station. Without proxy functionality: – The station contains a Profinet-compatible device with or without proxy functionality. – The station contains a CPU which is configured as a DP slave and contains the necessary blocks in the S7 program. – The station contains a DP slave with fixed functionality from which the component is to be created. Singleton component: A Profinet component is created without device data. This component type can be created for any hardware configurations with Ethernet connection.
Updating the PN interface	The Profinet interface of a Profinet controller can be updated in two ways during runtime: 1. Via a user program (Copy blocks): The system functions SFC 112 "PN_IN", SFC 113 "PN_OUT" and SFC 114 "PN_DP" must be copied from the Profinet system library into the block container of the Step 7 basic project and called in the S7 program. 2. Automatic (at the Scan Cycle Check Point): The Profinet interface is automatically updated by the operating system of the Profinet controller at the cycle check point.

Fig. 5.39
Creating the DP subnets of a Profinet component

Table 5.12 Parameters in the tab "DP Subnets"

Box	Meaning
Profibus connectors of the component	The tab "DP-Subnets" is only available for hardware configurations with more than one DP master system. Profibus 1-4: If the Profinet component is a "standard component with proxy functionality", up to four Profibus connections can be specified here for operation of Profibus devices via proxy. Furthermore, unambiguous assignment is carried out here regarding which Profibus line corresponds to which Profibus line of the Profinet component.

Fig. 5.40
Display of the functions of a Profinet component

Table 5.13 Displays in the tab "Functions"

Box	Meaning	
Functions of component and associated blocks	Function: Block: Block type: Associated FB (only for instance DBs):	Name of technological function Type and number of block Profinet interface DB or HMI interface DB Type and number of associated function block

Fig. 5.41
Settings of the storage areas of a Profinet component

Table 5.14 Parameters in the tab "Storage Areas"

Parameter	Meaning
Save component in ...	Possible storage areas of the Profinet component.
Simatic iMap target library	Library into which the Profinet component is to be imported. Libraries are created in Simatic iMap.
Storage area in file system	Path in the file system in which the Profinet component is to be saved.

Fig. 5.42
Settings of the additional properties of a Profinet component

Table 5.15 Parameters in the tab “Additional Properties”

Parameter	Meaning
Component icon	Path to the icon file of the Profinet component in Simatic iMap.
Device icon	Path to the icon file of the device in Simatic iMap.
Documentation link	Path of the documentation file or address of a document on the Internet (URL). Path data according to the Universal Naming Convention (UNC), e.g. \\Server\Release\Document.doc, are not permissible. Possible documentation links: Path of document in file system. The document is copied and saved as part of the component data. Address of document on the Internet (URL), e.g. http://www.my_site.com/component-document.htm. In this case, only the link to the component is copied, and not the document.

5.7.3 Creation of Profinet Components with the Profinet Component Editor

The Profinet Component Editor provided by Siemens is a tool which provides an easy way of creating Profinet components from a range of non-Simatic S7 PLCs, without a corresponding vendor-specific engineering tool (see Table 5.16). These PLCs can be operated in the context of Profinet CBA with a Simatic Net-IE/PB Link as proxy. The Profinet Component Editor automatically generates the following data:

- The PCD for integration of the Profinet component into a Profinet CBA engineering tool
- A cbs configuration file for the Simatic Net-IE/PB Link

Table 5.16
Non-Simatic S7 PLCs which can be configured with the Profinet Component Editor

PLC	Profibus DP interface module
Allen Bradley CompactLogix	Hilscher RIF 1769-DPS
Allen Bradley ControlLogix	SST-PFB-CLX
Allen Bradley FlexLogix	Hilscher RIF 1788-DPS
Allen Bradley MicroLogix	Hilscher RIF 1769-DPS
Allen Bradley SLC500	SST-PFB-SLC
Allen Bradley PLC5	SST-PFB-PLC5
ELAU PacDrive Max-04	Hilscher CIF 104-DPS
Mitsubishi Q series	QJ71PB93D
Omron PLC (C200H, CS1)	C200HW-PRT21
Schneider Quantum/Unity	ProSoft PTQ-PDPS
Siemens Simatic S5-115/135/155	IM 308C
Siemens Simatic S5 90/95/100	CP 541
Siemens Simatic S5 95U-DP	Integrated

- Icons for representation of the Profinet component in the plant and network views of Simatic iMap
- A csv file (comma separated value) for documentation of the Profinet component (e.g. in Microsoft Excel).

The Profinet Component Editor knows the configurable I/O constellations for a number of fixed combinations of PLCs and their Profibus DP interface modules. If these agree with the actual configuration of the Profibus DP interface module used, a corresponding Profinet component can be created.

5.7.4 Configuration of Plants with Simatic iMap

Plant configuration includes importing of Profinet components into Simatic iMap libraries, single or repeated insertion of Profinet components into a project (instanciating), interconnection of technological functions, configuration of devices, technological functions and interconnections, as well as generation of the Simatic iMap project.

The task of the configuration engineer is to carry out complete configuration of the plant in Simatic iMap. This commences with the creation of libraries and finishes with uploading of the program data and interconnection data to the respective devices. The project is subsequently documented and saved (Table 5.17).

Table 5.17 Procedure for configuration of plant with Simatic iMap

Step	Activity
1	Optional: Importing of Profinet components into the (project) library.
2	Insertion of Profinet components into the project (instanciating).
3	Networking of devices in the network view.
4	Assignment of network addresses (IP addresses and/or Profibus address).
5	Interconnection of technological functions in the plant view.
6	Structuring of the plant.
7	Adaptation of device and/or function properties.
8	Checking of configuration.
9	Generation of Simatic iMap project.
10	Documentation and saving of the project.

Importing of Profinet components into libraries

In order to use Profinet components in Simatic iMap, they must be available in a library. They are therefore imported into libraries created using Simatic iMap (Figs. 5.44 and 5.44). The establishment of a library is based on technological criteria. Libraries can contain standard and singleton components.

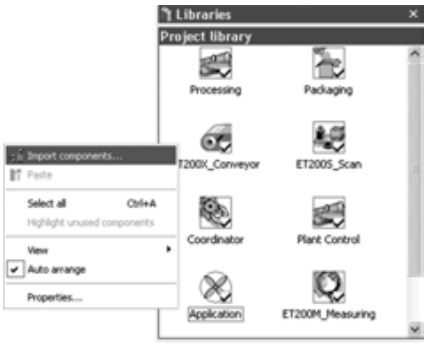


Fig. 5.43
Importing Profinet components into Simatic iMap

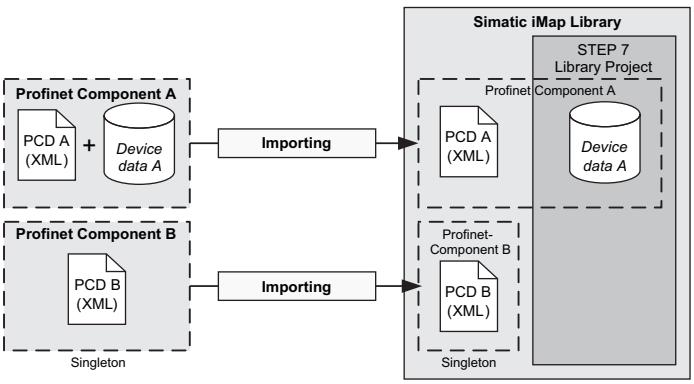


Fig. 5.44 Principle of importing Profinet components from Simatic S7 devices into Simatic iMap

Instantiating of Profinet components

Insertion of a Profinet component from a library into a Simatic iMap project results in an instance of the Profinet component, i.e. an application of this type of component. The instance of a Profinet component is generated using the information present in the PCD (Fig. 5.45). Profinet components can be repeatedly instantiated. The ID and version number of an instance serve as its reference to the associated Profinet component. Instances of a Profinet component consist of a device and an optional technological function, just like the Profinet component itself.

Profinet components can be inserted in the network, plant or project views and project tree of Simatic iMap.

- In the plant view, the instances of the inserted Profinet components are visible as technological functions. The interconnections, i.e. the logical data connections between technological functions, are displayed as lines.
- In the network view, the instances of the inserted Profinet components are displayed as devices with one or more network connections.

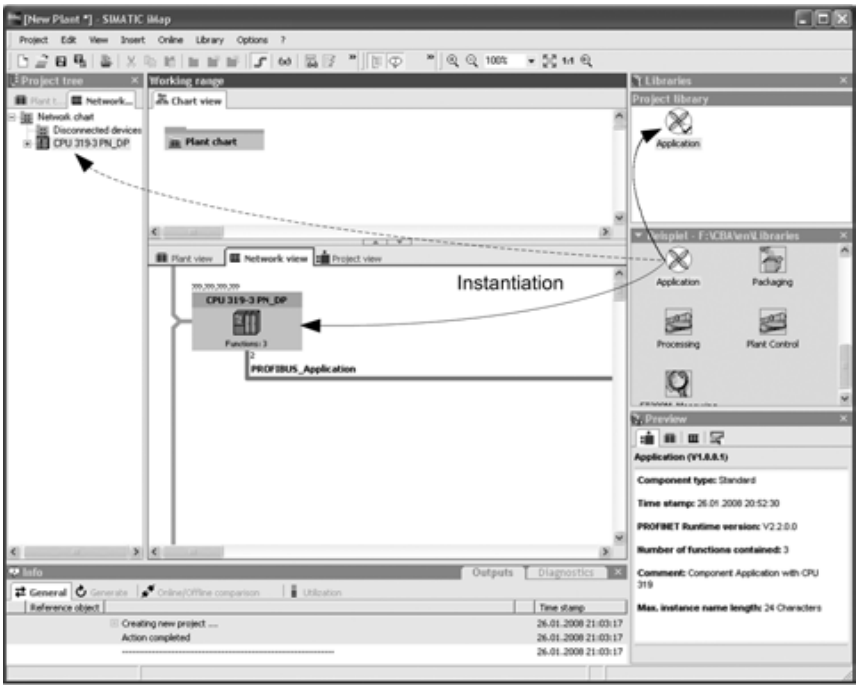


Fig. 5.45 Instantiating of Profinet components into the network view of Simatic iMap

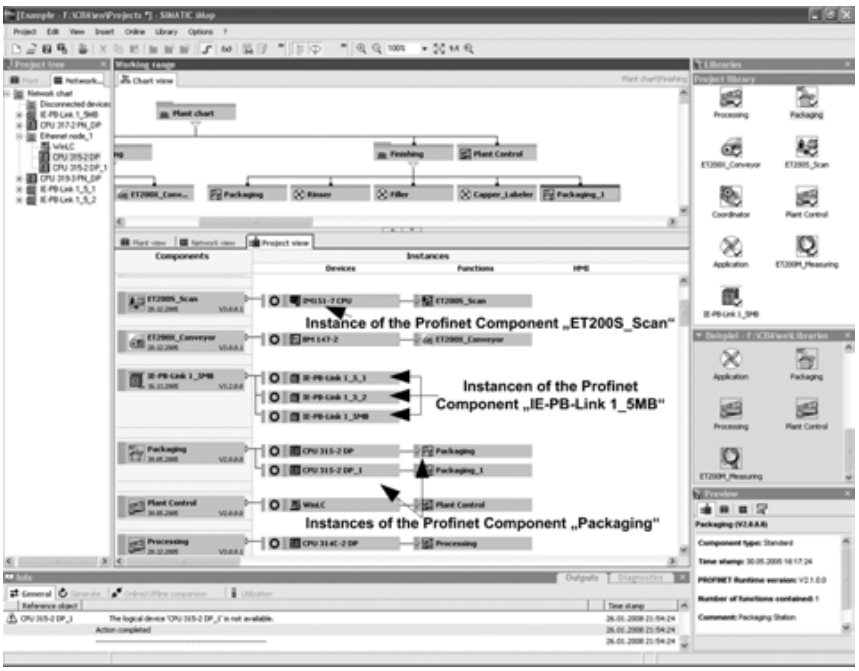


Fig. 5.46 Instances of Profinet components in the project view of Simatic iMap

- In the project view, the association is displayed between the Profinet components of the project library and the inserted instances, functions and devices (Fig. 5.46).
- All objects of the project are displayed hierarchically in the project tree. The project tree is divided into the plant tree and the network tree. Following insertion of a Profinet component (instantiating), its technological functions appear in the plant tree and the device in the network tree. Subordinate charts are also displayed hierarchically in the plant tree. Those instances which do not contain technological functions, e.g. the IE/PB Link, are only displayed in the network tree.

Properties of instances

Instances have properties which describe them unambiguously (Figs. 5.47 and 5.48). Important properties include the name and IP address of a device, or the name of a technological function. This guarantees unambiguous addressing of the corresponding device during runtime and the technological function executed on it.

Simatic iMap automatically generates the names during instantiating. These names are based on the name of the instanciated Profinet component and can be

Table 5.18 Parameters in the tab "Instance"

Box	Meaning
Elements	Device name: Current name of instance. Name in the component: Name of the device in the associated Profinet-component. Function name: Name in the instance: Current name of the technological function(s) of the instance. Name in the component: Name of the technological function(s) in the associated Profinet component. HMI display modules: Names of all integrated HMI display modules of the instance.
Generation status	Function and device: Current status of Step 7 shadow project for this instance. The Step 7 shadow project is generated from the device data of the Profinet standard components when generating a Simatic iMap project: Not generated: The Step 7 shadow project has not yet been generated, or the Profinet component is not yet present in it. Generated: The Step 7 shadow project has been generated, the Profinet component is present in it, and the properties of the Profinet component are consistent with the Step 7 shadow project. Inconsistent/changed: The properties of the Profinet component have been changed, and are no longer consistent with the Step 7 shadow project. Generation not possible: Illegal values are present in the properties of the Profinet component, making generation impossible (e.g. address assigned twice). HMI components: Generation status of the HMI components of this instance.
Comment	Comment on the instance.

modified during configuration (see Figs. 5.49 and 5.50 as well as Tables 5.18 and 5.21).

The input of address information allows the engineering system to upload the configuration to a specific device (see Fig. 5.49). To ensure that a device is accessible at the configured address, it must first be assigned this address (Table 5.20). This procedure is referred to as initialization.

Fig. 5.47
Instance properties

Fig. 5.48
Connection properties

Table 5.19 Parameters in the tab “Connections”

Parameter	Meaning
Function name	Name of the instance of the technological function whose connection properties are displayed.
Mask hideable connections in the plant view	If this option is clicked, the connections marked as hideable are not visible in the plant view of the Simatic iMap project.
Inputs	List of names and data types of all inputs of an instance.
Outputs	List of names and data types of all outputs of an instance.
Mark selected connections as hideable	If this option is clicked, the marked connection is identified as hideable. This option can only be selected for non-interconnected connections.
Comment on the connection	Comment on the selected input or output. Comments are defined during creation of the Profinet component.

Fig. 5.49 Address properties

The tab “Internal IE devices” is only displayed if the instance possesses an internal Profinet IO System.

All automatically assigned IP addresses are unique within the SIMATICþiMap project. However, uniqueness throughout the network must be guaranteed by the configuring engineer. IP addresses which are assigned more than once can result in network conflicts.

Table 5.20 Parameters in the tab "Addresses"

Box	Meaning
Ethernet addresses	Only with devices with Ethernet connection IP address: IP address of Profinet device. Subnet mask: The subnet mask consists of four decimal numbers within the range 0 to 255, separated from each other by a point, e.g. 255.255.255.0. The binary representation of the four decimal numbers of the subnet mask must have a sequence of "1" without gaps from the left, and a sequence of "0" without gaps from the right. Router: If a router is present in the communications path of the device to the engineering/HMI system or one of its communications partners, the IP address of the router must be entered here. This address is defined by the network administrator or the company operating the plant. The IP addresses of the device and router must belong to the same subnet. Use router: If "Use router" is clicked, the IP address of the router must be specified for the parameter "Router".
Profibus address(es)	Only for devices with Profibus connection and proxy functionality. DP master system name: Name of the DP master system. The name is defined during creation of the Profinet component. Address: Profibus address of the device. If the device is a Profinet controller with proxy functionality with local Profibus, the Profibus addresses used there are recognized as being assigned, and cannot be selected for the coupled Profibus devices.

Fig. 5.50 Properties of internal IE devices

Table 5.21 Parameters in the tab “Internal IE devices”

Box	Meaning
Addresses of Profinet IO Devices	Profinet IO System name: Name of the Profinet IO System. The name can be assigned automatically or manually. It is part of the device names of the internal IO Devices and the IO controller. An assigned device name must be unique throughout the network! Assign name automatically: If this option is clicked, the system name is automatically generated from the IP address of the IO controller. Profinet IO controller: The name of the IO controller and its IP address are displayed. The name comprises the device name of the IO controller in the vendor-specific configuration tool and the Profinet IO System name. The two names are separated by a point. The displayed IP address corresponds to the IP address of the IO controller in the tab “Addresses”. Profinet IO Devices: Name of the internal IO Devices and their IP addresses. A name comprises the device name of the IO Device in the vendor-specific configuration tool and the Profinet IO System name. The IP address can be assigned automatically or manually. It is important that the IP address of an IO Device is in the same subnet as the addresses of the IO controller. Suggest addresses: Automatic assignment of the IP addresses to internal IO Devices.

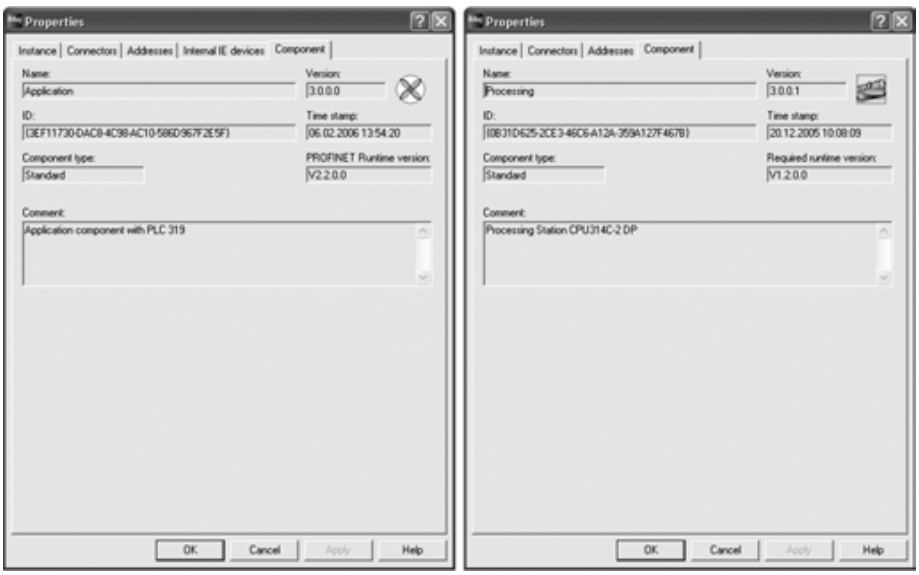


Fig. 5.51 Component properties

Table 5.22 Parameters in the tab "Component"

Parameter	Meaning
Name	Name of Profinet component from which the instance originates.
Version	Version number of Profinet component from which the instance originates.
ID	Class identification of Profinet component from which the instance originates. Unambiguous identification of the Profinet component from which the current instance originates is only possible with the version number and ID together.
Time stamp	Creation date and time of Profinet component from which the instance originates.
Component type	Type of Profinet component from which the instance originates. Standard: Profinet component with device data Singleton: Profinet component without device data (singleton component)
Profinet runtime version/ Required runtime version	The Profinet runtime version identifies the release of the Profinet functionality in the firmware of the Profinet controller. The Profinet runtime version of a Profinet device with proxy functionality is particularly important for the coupled Profibus devices. The coupled Profibus devices can only use certain functions if the proxy device supports these functions, e.g. connections of data type STRUCT.
Comment	Comment on the Profinet component from which the instance originates.

Replacing of instances

Instances of a Profinet component can be replaced in Simatic iMap by the instances of a different Profinet component. It is possible in this manner to rapidly incorporate changes in Profinet components into existing Simatic iMap projects.

The requirements which must be fulfilled by an instance in order to make it eligible as a replacement for an existing instance are defined by specific rules. If these rules are observed, the configured properties of the old instances, such as IP addresses or Profibus addresses, are largely transferred to the new instances. This applies equally to interconnections if the technological function of the new component has connections of the same type (input or output), same name and same data type. Configured substitute values and transmission properties of the interconnections are also imported.

Project library

When instantiating for the first time, Simatic iMap creates a copy of the Profinet component in the project library. This library is part of the Simatic iMap project, and serves as database during subsequent generation of the project (Fig. 5.52).

In the event of component revision, the project library permits direct navigation to the associated component project where the corrections can be carried out. Following completion of the corrections and renewed creation of a component, the instances used can then be updated quickly and easily.

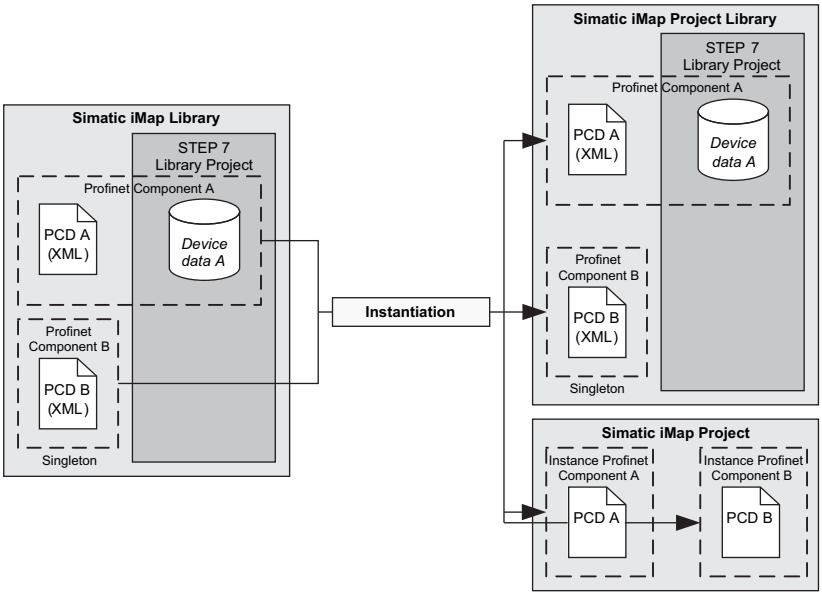


Fig. 5.52 Principle of instantiating Profinet components from Simatic S7 devices

Interconnections between technological functions in the plant view

Once all required Profinet components have been instantiated, the interconnections are configured graphically. The plant view of Simatic iMap reflects the technological view of the plant. Interconnections between technological functions are produced there by drawing lines. These lines define the communications relations between the technological modules, and thus the actual total functionality of the plant (Fig. 5.53).

If a line cannot be meaningfully shown, for example due to space reasons, the interconnection is displayed by so-called continuation connectors. These show the respective ends of the interconnection. Continuation connectors with the same number represent a single interconnection.

Interconnections are established between outputs and inputs. They must be of the same data type and – with combined data types – have the same data structure. An output can be interconnected to several inputs.

Cross-project interconnections (external interconnections)

In the case of Simatic iMap projects with a large number of instances, it may be meaningful to divide the project into several small Simatic iMap projects. Simatic iMap supports the configuration of cross-project interconnections for this purpose. Cross-project interconnections are those between the connections of technological functions present in different Simatic iMap projects. For this purpose, the

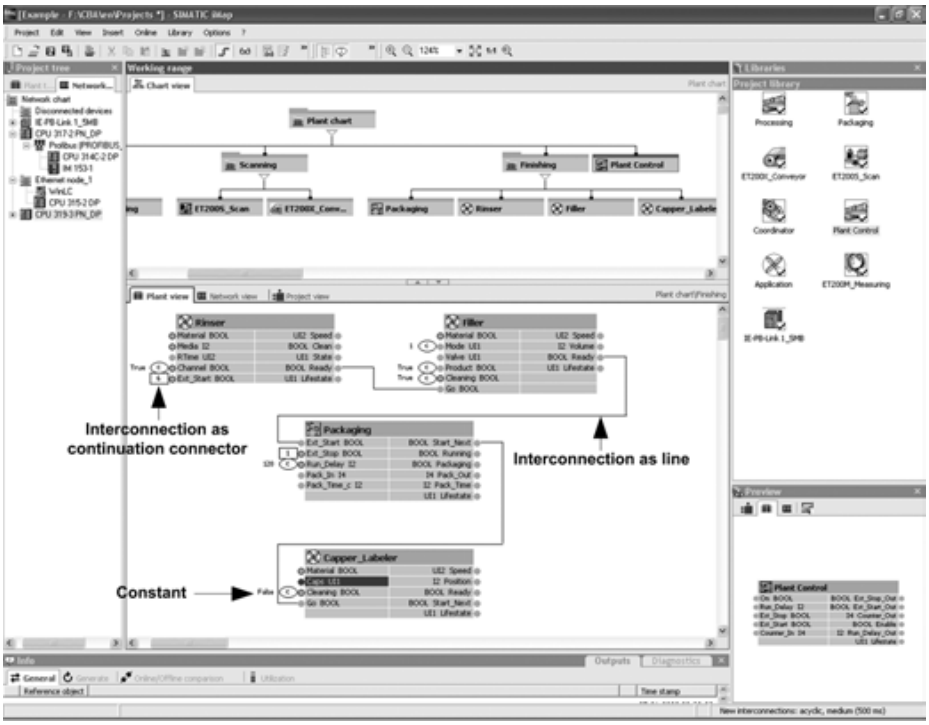


Fig. 5.53 Interconnection of instances in Simatic iMap

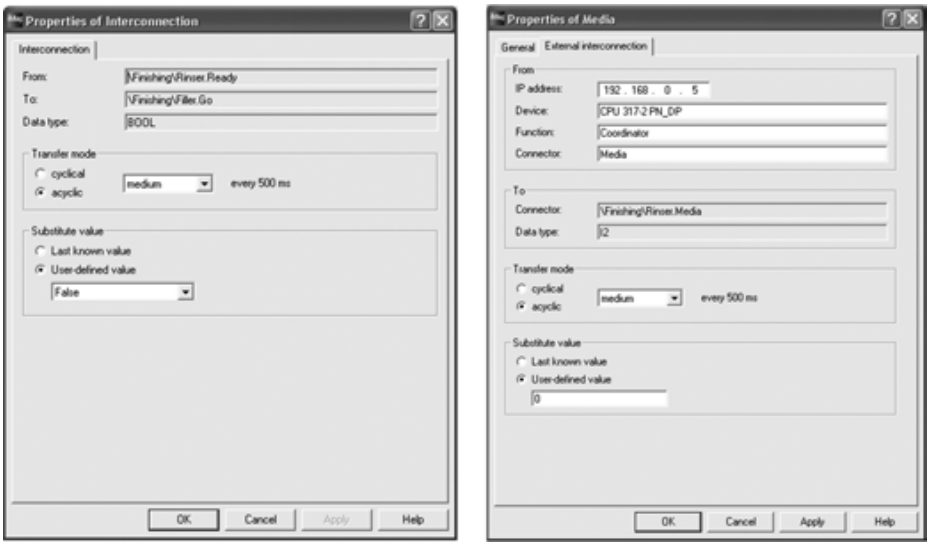


Fig. 5.54 Interconnection properties

Table 5.23 Parameters in the tab "Interconnection"

Box	Meaning
From	Project-internal interconnection: Display of name of technological function and of interconnected output. Cross-project interconnection: Address information of remote Profinet communications partner: IP address Device name Name of technological function Connection name.
To	Display of name of technological function and of interconnected input.
Data type	Type of data to be transferred.
Transfer mode	Transfer properties of interconnection: Transfer mode: Cyclic: Transfer using real-time protocol Acyclic: Transfer using ORPC wire protocol Fast/Medium/Slow: Level for transfer frequency (cyclic) or sampling frequency (acyclic). The time values in milliseconds are defined cross-project in the menu item "Project\Properties" in the tab "Interconnections".
Substitute value	Substitute value in event of interconnection fault: Last known value/user-defined value. Substitute values can only be configured for interconnections between Profinet devices.

interconnection source is addressed by specifying the IP address, device name, function name and connection name. Configuration of external interconnections is only possible in the top chart hierarchy.

Structuring of the plant

If all technological functions are interconnected, the total plant should be structured. It is possible for this purpose to combine technological functions in subordinate charts.

Subordinate charts

Charts are displayed in the chart area within the working area of Simatic iMap. The representation is similar to that of a technological function with its own interface (chart interface). The chart interface contains the inputs and outputs of the technological functions present in the chart which are to be routed beyond the chart limits. Furthermore, charts in the plant tree are visible within the project tree as a folder with the technological functions present in the chart and possibly with further subordinate charts.

Two different procedures are recommended when structuring with the assistance of charts:

- Interconnection of the technological functions in the plant view in the top chart of the chart hierarchy (plant chart) and subsequent arrangement of the technological functions in subordinate charts. The chart interfaces for interconnections are generated automatically when arranging the functions in subordinate

charts. This is recommended in the case of many interconnections between technological functions, and it is clearer for new configurations.

- Arrange the functions in subordinate charts, with subsequent cross-chart interconnection of the functions. This is recommended in the case of fewer interconnections between technological functions, and for the integration of new functions into existing configurations with subordinate charts.

Generation of a Simatic iMap project

When generating a Simatic iMap project, the device configuration required for operation is generated for all instances of Profinet components with device data (Fig. 5.55). Downloading of the program data into the plant devices is only possible following generation.

The vendor-specific configuration data and program data of Simatic automation devices are present following completion of the generation as a vendor-specific project, or as a Step 7 project (Step 7 shadow project) in the case of Simatic S7 devices. Instances of singleton components are not considered during the generation, since their configuration is already present in the Step 7 basic project. The HMI components of an instance are generated separately.

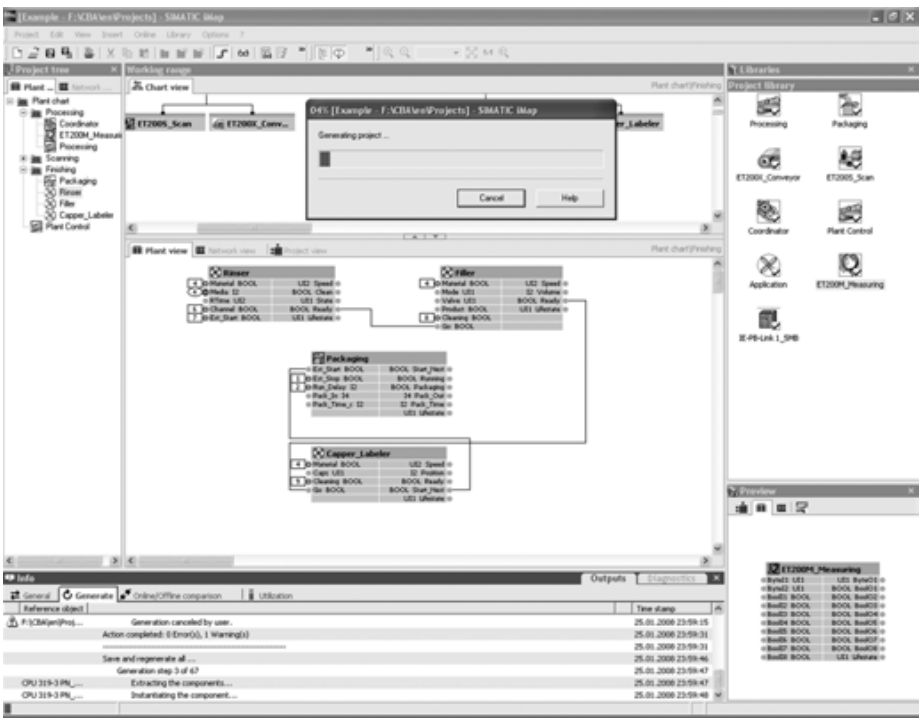


Fig. 5.55 Generation of Simatic iMap project

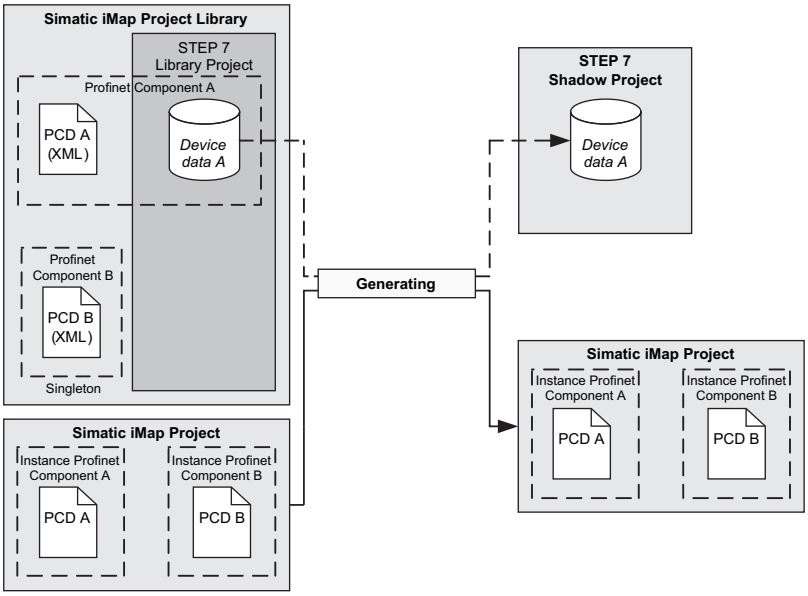


Fig. 5.56 Principle for generation of a Simatic iMap project with Simatic S7 devices

To carry out the generation, Simatic iMap requires the vendor-specific configuration and programming tools of the devices used in the projects, e.g. Step 7 for Simatic PLCs. A separate generation process is required for each vendor-specific configuration and programming tool incorporated (Fig. 5.56).

When regenerating a Simatic iMap project (as backup), a new Step 7 shadow project is generated for Simatic S7 devices, and the previously existing one – if present – is saved first. A fully regeneration is necessary, for example, during the initial generation of a Simatic iMap project or if there are inconsistencies between the current vendor-specific Simatic iMap project and the current project.

If changes have been made to an existing Simatic iMap project, it is usually sufficient to only regenerate these changes. The existing vendor-specific project is updated in this case by the changes.

5.7.5 Commissioning and Testing the Plant

The work for the plant operator commences following completion of the configuration phase. The plant devices are started up successively, and provided with their configuration data by means of downloads.

A download corresponds to the transfer of data from Simatic iMap to a PLC or field device. The data consist of program data and interconnection data.

The commissioning phase is completed following the plant test and subsequent generation of the symbol file for access to process data via OPC. The several steps are carried out (Table 5.24).

Table 5.24 Procedure for commissioning and testing the plant

Step	Activity
1	Device commissioning.
2	Downloading of programs and interconnections.
3	Optional: revision of Profinet components.
4	Plant test.
5	Creation of symbol data for access via OPC.

Assignment of the IP address to a device (initialization)

Devices connected to a subnet do not usually have an IP address prior to initial loading. In order to access a device on the network, it must first be initialized, i.e. assigned an unambiguous IP address and corresponding IP parameters (Fig. 5.57).

Fig. 5.57
Setting of PG/PC interfaces

The station must be accessible online in order to initialize it:

- The Ethernet interface of the Step 7 engineering computer must be accessible from Step 7/NCM PC. To achieve this, the access point for the IE module must be set to S7ONLINE in the window "Set PG/PC interface" (Fig. 5.58 and Table 5.25).
- The device and the Step 7 engineering computer must be connected to the Ethernet.
- The device must be located on the same Ethernet subnet as the Step 7 engineering computer.

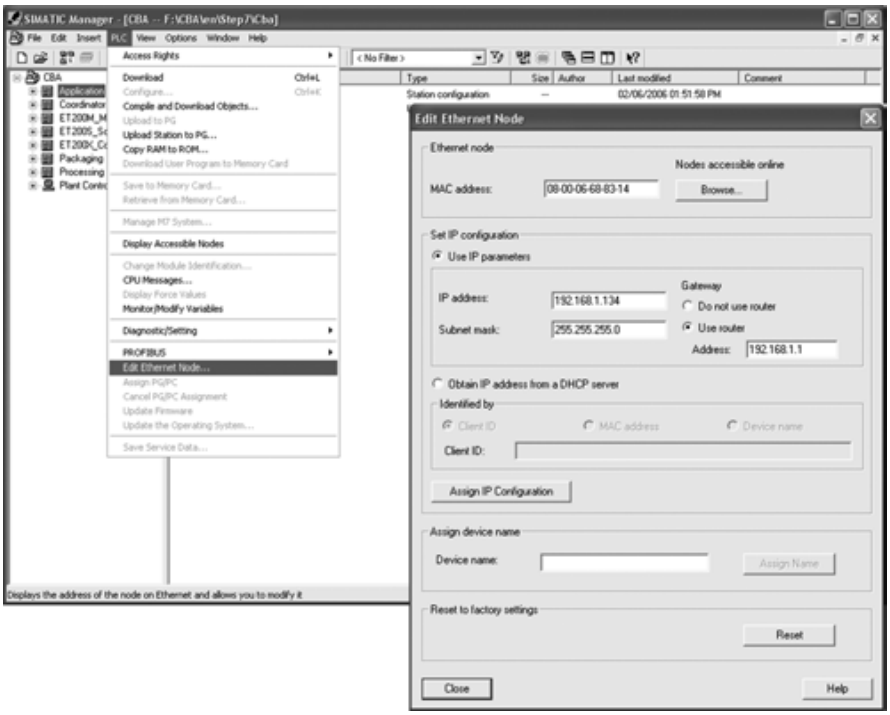


Fig. 5.58 Assignment of the IP address in the Simatic Manager

Table 5.25 Parameters in the window "Edit Ethernet Node"

Box	Meaning
Ethernet node	MAC address: The Ethernet address of the device to be initialized is entered here in the format: aa-bb-cc-dd-ee-ff. Nodes accessible online: If the Ethernet address is unknown, the Ethernet subnet connected to the engineering computer can be searched for accessible nodes by clicking the "Browse" button. When using switches with VLAN capability, make sure that frames are not rejected by VLAN tag = 0. Otherwise, nodes may not be found.
Set IP configuration	Use IP parameters: If the window was selected in the context of a selected node, the IP address is present with the values configured for the node. Otherwise the IP address and subnet mask must be entered here. Gateway: Do not use router: This option is only selected if device communication takes place exclusively within its own IP subnet. Use router: This option is selected if the device communicates with devices (also engineering) in a different IP subnet. In this case, the IP addresses of the network card of the router which is present in the same IP subnet as the device must be entered under "Address". Obtain IP address from a DHCP server: If selected, the IP address of the device is obtained from a DHCP server. For this purpose, the DHCP server is assigned the MAC address of the CP, the device name or the client ID depending on the selected option. The client ID is a string with a maximum of 63 characters. If the IP address of the DHCP server is to be determined from the device name, a name must first have been assigned to the device. Click the "Assign IP Configuration" button to transfer the configuration to the device.

Table 5.25 Parameters in the window "Edit Ethernet Node" *(continued)*

Box	Meaning
Assign device name	If the edited Ethernet device is an IO Device, the name of the IO Device can be assigned here. The device name is also required if the IP address is to be determined by a DHCP server using a device name. Name convention (in accordance with DNS): – Max. length 240 characters. – A string between two points within the device name must not be more than 63 characters long. – No special characters are permissible, except a hyphen. – The device name must not begin or end with the "-" character. – The device name must not have the format n.n.n.n (n = 0...999). – The device name must not begin with the string "port-xyz-" (x, y, z = 0...9). Example: [Name from short description].[Name of PN IO System]. Click the "Assign Name" button to transfer the device name to the Ethernet device.
Reset to factory settings	Click the "Reset" button to reset the factory settings for the device. The IP configuration and device name are then deleted.

Downloading of programs and interconnections

The program download comprises the loading of program data. This includes the data of the user program including all device-specific data such as the hardware and network configurations. Simatic iMap applies the communications mechanisms of the respective device vendor for the program download. The respective vendor-specific configuration and programming tools, e.g. Step 7, are therefore required.

The configuration data of Profinet controllers with proxy functionality also include configuration information on the coupled Profibus devices. For this reason, the program downloaded of the Profinet controller must be carried out before the coupled Profibus devices are downloaded.

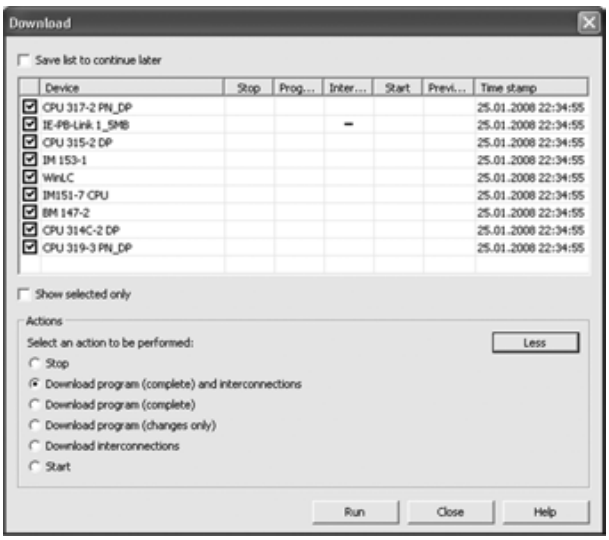


Fig. 5.59
Downloading of programs and/or interconnections

A program download is always required

- during commissioning of a device,
- following the connection or disconnection of Profibus devices, and
- following the replacement of instances.

Following the connection or disconnection of Profibus devices as well as following the replacement of the instance of a Profibus device, the program download must be carried out for the Profibus device itself, for the associated Profinet device with proxy functionality, and for the intelligent DP slaves operated on this Profibus subnet.

The downloading of interconnections comprises the downloading of interconnection information into the Profinet controllers of the plant (Table 5.26). During this procedure, all information required for establishment of interconnections is transferred to the Profinet controller. A vendor-specific configuration tool is not required to download interconnections with Simatic iMap.

Table 5.26 Options for downloading

Box	Meaning
Save list to continue later	The statuses of the devices are saved following execution of the desired actions. The list of devices contains the execution status of the download actions (successful or faulty), and can be used as the basis for continuing the download.
Show selected only	Only the selected devices are considered during the download.
Actions	Stop: Stop the identified devices (with SIMATIC devices, change to "stop" state). Download program and interconnections: Downloading of programs and all interconnections to the identified devices. The devices are stopped prior to the program download, and subsequently restarted. Download program (complete): Downloading of programs to the identified devices. Download program (changes only): Downloading of program changes to the identified devices. Download interconnections: Downloading of interconnections to the identified devices. Downloading is carried out independent of the operating state of the devices. Start: Start the identified devices (with SIMATIC devices, change to "RUN" state).

Data exchange commences immediately following completion of the download procedure. The establishment of interconnections is always initiated by a consumer, i.e. by the device whose technological function is expecting data. Connection values and interconnection status can be diagnosed in online mode by Simatic iMap immediately following the download.

Modification of Profinet components and plant test

Final corrections to devices and technological functions may be required during commissioning. The vendor-specific engineering and HMI systems used during creation of the Profinet components must be available in addition to Simatic iMap in order to carry out the modifications.

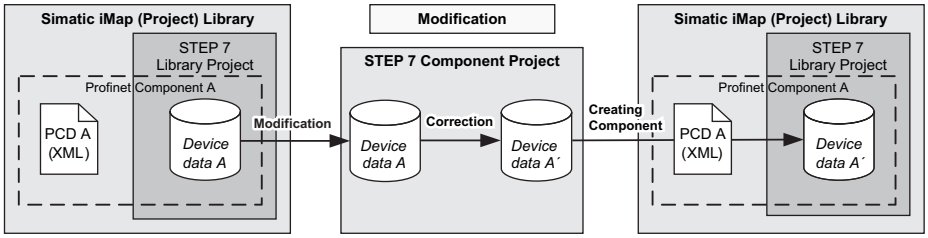


Fig. 5.60 Assignment of the IP address in the Simatic Manager

Profinet components with device data can be modified in Simatic iMap directly from any library or from project view. To carry this out, Simatic iMap produces a copy of the Profinet library components in a vendor-specific project. This project can be modified for Simatic devices using Step 7, and serves as a new basic project for the modified Profinet component (Fig. 5.60).

Creation of symbol data for access via OPC

An OPC symbol file can be created for a Simatic iMap project. For all configured devices, this file contains the address information of the information variables accessible via OPC.

The OPC symbol file is not automatically created in Simatic iMap during the generation procedure for performance reasons; it must be specifically triggered when this procedure has been completed. It is the last step prior to actual plant operation.

5.8 Profinet CBA Diagnostics

In addition to the standard Step 7 diagnostics aids, Simatic iMap provides new diagnostics facilities specially tailored to Profinet CBA plants. Profinet CBA diagnostics can be divided into offline and online diagnostics. Offline diagnostics permits checking of the configuration of a distributed automation solution created with Simatic iMap prior to downloading of the configuration and program into the devices. Online diagnostics permits location and elimination of faults in the completely configured plants during runtime.

5.8.1 Offline Diagnostics with Simatic iMap

The communications properties of Profinet controllers with a Profinet Runtime version V2.x or later are defined by performance parameters. These permit an offline capacity utilization test of the Profinet controller already during the engineering phase, thus preventing load-dependent interferences when the plant is running. Performance parameters apply to the Profinet controller itself and to all Profibus devices coupled via it by means of a proxy functionality. Performance parameters are part of the Profinet component description.

Capacity utilization test

Capacity utilization parameters are divided into parameter groups:

- Device parameters for a Profinet device without proxy function or for the complete proxy system of a Profinet device with proxy functionality
- General interconnection-dependent parameters (independent of the transmission mode)
- Parameters for acyclic remote interconnections of masters and slaves
- Parameters for cyclic remote interconnections of masters and slaves.

During the capacity utilization test, Simatic iMap compares the device-specific performance parameters with the actual device configuration. It is checked (see also Tables 5.27 and 5.31), whether:

- certain performance parameters of the devices have been exceeded in the configuration,
- the configured transmission properties of the interconnections (e.g. cyclic transmission) are supported by the device,
- a Profibus device and the associated Profinet controller with proxy functionality are compatible with respect to the Profinet runtime version.

Table 5.27 Device parameters

Parameter	Meaning
Number of coupled Profibus devices	Actual and maximum numbers of local Profibus devices and those connected via proxy functionality which can be operated on the Profinet controller.
Number of functions on this device	Actual and maximum numbers of all technological functions of a device. In the case of Profinet devices with proxy functionality, the technological functions of Profibus devices coupled via proxy are also considered.
Total number of connections	Actual and maximum numbers of all connections of the technological interfaces of a Profinet controller. In the case of Profinet devices with proxy functionality, the connections of the technological interfaces of Profibus devices coupled via proxy are also considered.
Maximum data length for arrays and structures per connection	Actual and maximum lengths of arrays and structures in bytes. In the case of Profinet devices with proxy functionality, the connections of the technological interfaces of Profibus devices coupled via proxy are included.
Total data length of all inputs	Actual and maximum lengths of all inputs of the technological interfaces of a Profinet controller in bytes. In the case of Profinet devices with proxy functionality, the inputs of the technological interfaces of Profibus devices coupled via proxy are included.
Total data length of all outputs	Actual and maximum lengths of all outputs of the technological interfaces of a Profinet controller in bytes. In the case of Profinet devices with proxy functionality, the outputs of the technological interfaces of Profibus devices coupled via proxy are included.
Memory requirements for type descriptions of all connections	Actual and maximum sizes of the memory occupied for the description of the data types of all connections of the technological interfaces in bytes. In the case of Profinet devices with proxy functionality, the connections of the technological interfaces of Profibus devices coupled via proxy are included. This memory is required in addition to the user data (total data length of all inputs and outputs).

Table 5.28 General interconnection-dependent parameters

Parameter	Meaning
Number of device-internal and Profibus interconnections	Actual and maximum numbers of the local interconnections. These include interconnections: – Between Profibus devices on the same DP master system – Between Profibus devices and the associated Profinet device with proxy functionality – Between connections of the same device.
Total data length of all device-internal and Profibus interconnections	Actual and maximum lengths of all local interconnections in bytes.
Number of interconnections with constants	Actual and maximum numbers of interconnections with constant values. In the case of Profinet devices with proxy functionality, the connections of the technological interfaces of Profibus devices coupled via proxy are also considered.
Total data length of all interconnections with constants	Actual and maximum lengths of all interconnections with constant values in bytes. In the case of Profinet devices with proxy functionality, the connections of the technological interfaces of Profibus devices coupled via proxy are also considered.
Number of remote interconnection partners	Actual and maximum numbers of communications partners on the Industrial Ethernet.
Capacity utilization by number of device elations to remote interconnection partners	Shows the capacity utilization in percent resulting from the number of so-called directed communications relations (see below) between a logical device and its communications partners as well as in the local proxy system and remote. A directed communications relation comprises one or more interconnections in one direction between two logical devices. Example of directed communications relations: All interconnections from outputs of logic device A to inputs of logic device B are considered as a directed communications relation. All interconnections from outputs of logic device B to inputs of logic device A are considered as a further directed communications relation.

Table 5.29 Parameters for acyclic interconnections of DP master and DP slaves

Parameter	Meaning
Minimum interval for sampling frequency	Actual and minimum values of the quality-of-service (sampling frequency "Fast") of all interconnections.
Quantity	Actual and maximum numbers of incoming and outgoing interconnections. In the case of Profinet devices with proxy functionality, the interconnections to connections of the technological interfaces of Profibus devices coupled via proxy are also considered.
Total data length	Actual and maximum lengths of all connections with incoming/outgoing interconnections. In the case of Profinet devices with proxy functionality, the interconnections to connections of the technological interfaces of Profibus devices coupled via proxy are also considered.
Distribution of frequencies	Information concerning the distribution of the Fast/Medium/Slow frequency levels for all incoming/outgoing remote interconnections. A frequency level corresponds to the quality-of-service value of the Fast/Medium/Slow sampling frequency. Distribution and limit value (device parameter) configured per frequency level for: – Time interval of Fast/Medium/Slow frequency levels in ms. – Number of incoming/outgoing interconnections of the Fast/Medium/Slow frequency levels. – Total data length of all inputs/outputs with interconnections of the Fast/Medium/Slow frequency levels in bytes.

Table 5.30 Parameters for cyclic interconnections of DP master and DP slaves

Parameter	Meaning
Minimum interval for transmission frequency	Actual and minimum values of the quality-of-service (transmission frequency "Fast") of all interconnections.
Maximum interval for transmission frequency	Actual and minimum values of the quality-of-service (transmission frequency "Slow") of all interconnections.
Maximum data length for arrays and structures per connection with DP master and DP slaves	Actual and maximum lengths of arrays and structures in bytes. In the case of Profinet devices with proxy functionality, the connections of the technological interfaces of Profibus devices coupled via proxy are included.
Configured transmission frequencies	Values of the configured transmission frequencies of the project.
Quantity	Actual and maximum numbers of incoming/outgoing interconnections. In the case of Profinet devices with proxy functionality, the interconnections to connections of the technological interfaces of Profibus devices coupled via proxy are also considered.
Total data length	Actual and maximum lengths all connections with incoming/outgoing interconnections in bytes. In the case of Profinet devices with proxy functionality, the interconnections to connections of the technological interfaces of Profibus devices coupled via proxy are also considered.
Configured distribution of transmission frequencies (fast/medium/slow)	Interconnection numbers: Number of incoming/outgoing interconnections of the corresponding frequency level. Data lengths: Data lengths of the incoming/outgoing interconnections of the corresponding frequency level in bytes.
Total number of data packets	Actual and maximum numbers of incoming/outgoing data packets.
Number of data packets per x ms	Actual and maximum numbers of incoming/outgoing data packets in the fastest transmission frequency.
Number of bytes per x ms	Actual and maximum lengths of incoming/outgoing data packets in the fastest transmission frequency in bytes.
Dynamic load distribution	The result of the test with regards to the timing requirements for the distribution of outgoing data between individual data packets for the various remote communications partners. If a transmission capacity is also reserved for integral IO controllers, this is also taken into account.

Table 5.31 Error messages during the capacity utilization testing of cyclic interconnection

Error message	Remedy
The device does not support remote interconnections with cyclic transmission	Replace device by a corresponding device with a runtime version Š 2.0 or reset the interconnections to acyclic transmission.
The capacity limit for remote interconnections with cyclic transmission between <Device 1> and <Device 2> with a transmission frequency of <x> ms has been exceeded	Reduce the data volume to be transmitted with the specified frequency level between the specified interconnection partners: – Reduce the number of interconnections to remote partners – Reset the associated remote interconnections to different frequency levels – Reset the interconnections to acyclic transmission.
The connection <Name> does not support remote interconnections with cyclic transmission because of its data length	Reset the connections to acyclic transmission. *** The device does not support remote interconnections with cyclic transmission

5.8.2 Online Diagnostics with Simatic iMap

Online diagnostics of all Profinet CBA communications partners present in the distributed automation plant is carried out in the online view of Simatic iMap. This comprises checking of all configured devices with respect to accessibility, online/offline consistency and operating status, and presents the resulting diagnostics information in graphical form (Fig. 5.61 and Table 5.32).

Diagnostics messages are always produced by a Profinet controller. This also applies to diagnostics messages of Profibus devices operated on a Profinet controller

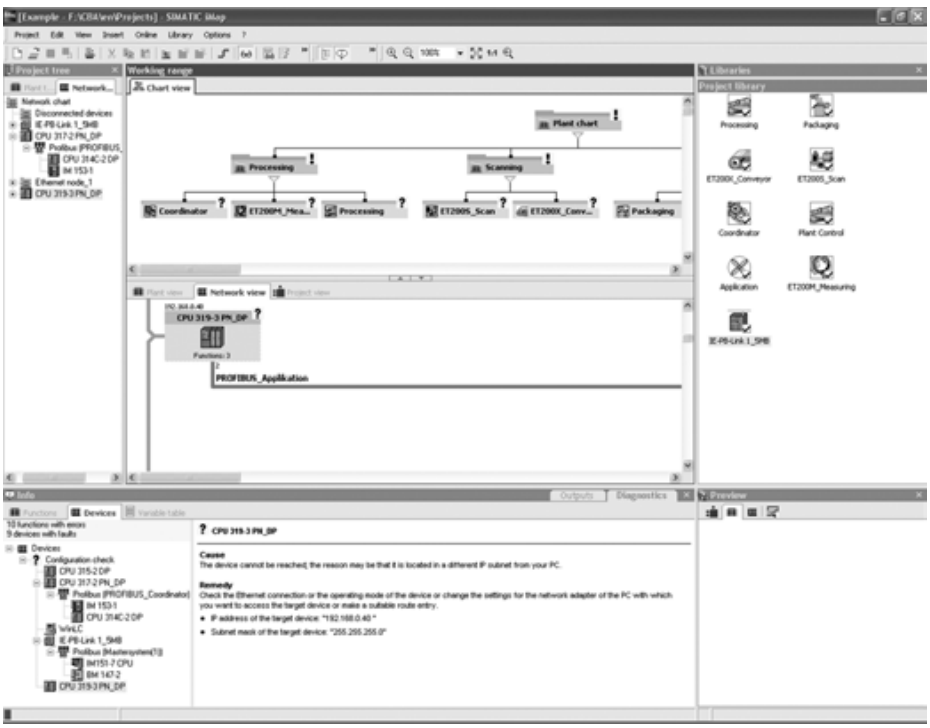


Fig. 5.61 Example of online diagnostics in Simatic iMap with non-accessible devices

Table 5.32 Diagnostics symbols in Simatic iMap and their meaning

Symbol	Meaning
	Configuration check The device cannot be accessed, i.e. no connection can be established between Simatic iMap and the device, or the technological function of the device does not exist. Possible causes: – Communications fault, e.g. through cable breakage or non-connected cable. – The device is switched off, not started, not completely initialized, or not a Profinet device. – An incorrect device or incorrect technological function has been loaded. – A faulty or incorrect hardware configuration is present. – The technological function has not yet been loaded. – A different class ID or version has been determined during the online/offline comparison.

Table 5.32 Diagnostics symbols in Simatic iMap and their meaning *(continued)*

	Device diagnostics With Simatic S7 CPUs, this diagnosis is signaled when a group fault has been detected (SF LED). Possible causes: Network view: – Device-specific diagnostics is present. – The device is in the STOP status because of a fault in the technological function. – The device is faulty. Plant view: – One or more technological functions within a chart are faulty.
	Not connected Possible causes: – The Profibus cable to the device is faulty. – The Profibus device is not connected to the Profinet controller. – The Profibus device is not switched on. – The Profibus device is in the stop status. – The Profibus device is incorrectly configured, or the configuration has not yet been downloaded.
	No information available. The device is accessible, but the device status cannot be determined. Possible causes: – The Profinet controller is faulty. – The Profinet controller is in the stop status, and the Profibus devices connected via proxy cannot therefore be accessed. – The technological function of the Profibus device has not yet been downloaded.
	Download necessary. Downloading of interconnections is required. Possible causes: – Different interconnection data in Simatic iMap and the device.
	Interconnection is faulty. At least one interconnection to an input of the technological function of the device is faulty. Possible causes: – The communications partner of the device is faulty, cannot be accessed, or is overloaded. – With cyclic interconnections: the communications partner of the device is not in the same IP subnet. – Incompatible transmission properties, or one not supported by the device, have been configured for at least one interconnection (transmission mode or transmission/sampling frequency).

via proxy functionality. If a Profinet controller is faulty or cannot be accessed, this particularly means that no diagnostics information can be determined for the Profibus devices connected to it via proxy functionality.

Basic diagnostics sequence

The basic diagnostics sequence for Profinet communications partners in Simatic iMap consists of three steps:

1. Activate online view.
2. Open the “Devices” tab in the diagnostics window. In the event of a fault, select the associated device from the displayed list, and eliminate the fault using the corresponding detailed information and support facilities.

3. Open the “Functions” tab in the diagnostics window. In the event of a fault, select the faulty technological function from the displayed list, and eliminate the fault using the corresponding detailed information and support facilities.

It is generally applicable: if several devices or technological functions are faulty, faults in the devices or technological functions should first be eliminated in the category *“Configuration check”*, since Profinet CBA diagnostics is not possible without a configuration check. Remaining faults of other categories can then be processed in any sequence.

If corrections are necessary in the hardware configuration or in the program of a Profinet component in order to eliminate a fault, these should be carried out by modifying the Profinet component (see Kapitel 5.7.5 Commissioning and Testing the Plant). Exception: with singleton components, the fault is corrected directly in its Step 7 basic project.

Status of Profinet communications stations

In the network view, Simatic iMap shows the status of Profinet communications stations. This status display corresponds

- to the operating status of the Simatic CPU user program in the case of Profinet controllers,
- to the status of the DP interface of the DP master (Clear/Operate) in the case of the Simatic Net gateway IE/PB-Link, and
- to the status of their accessibility in the case of Profibus devices.

The status of a device is also output via the “Lifestate” output of a technological function (see Table 5.33). This output exists with each technological function created using Step 7, and allows device monitoring by means of an HMI/MES system or the user program of a Profinet communications partner.

Table 5.33 Device status in Simatic iMap and corresponding “Lifestate” value

Symbol	“Lifestate”	Device status	
	0x01	Profinet controller: Simatic Net IE/PB Link:	Startup/Initialization –
	0x03	Profinet controller: Simatic Net IE/PB Link:	hold/STOP DP master in “Clear” status
	0x02	Profinet controller: Simatic Net IE/PB Link:	RUN/RUN-P DP master in “Operate” status
	0x04	Profinet controller: Simatic Net IE/PB Link:	Faulty Faulty
	0x03	Profibus device:	Accessible and in “Data exchange” status
	0x02	Profibus device:	Not accessible, or station failed

Check device accessibility

This function offers a fast possibility for checking the accessibility of devices in the automation plant when the online view is deactivated, and to absolutely exclude communication faults. With the online view activated, Simatic iMap automatically checks the accessibility of all devices and technological functions, displaying accessible devices and technological functions in blue and non-accessible ones in gray. The associated messages are explained in Table 5.34.

Table 5.34 Messages when checking the accessibility

Message	Meaning
Device <Device name> is accessible.	The device is accessible over the network.
Station at IP address <IP_address> cannot be accessed.	The physical connection to the device is: – Faulty or non-existent, or – The device is not switched on. With Profibus devices: The Profinet controller through which the Profibus device is connected via proxy cannot be accessed or is in the stop status. In this case, no Profibus devices connected to the Profinet controller via proxy can be accessed.
Profinet link on the device <IP_address> is not accessible	The device is physically connected, but not ready, for example it is in the stop status.
Logical device <Device name> (proxy at <IP_address>) is accessible, but not the physical device.	Only with Profibus devices: – The Profinet configuration data are not loaded – The Profinet configuration data of the Profibus device are present on the associated Profinet controller with proxy functionality, but the connection between DP master and DP slave is faulty.
Different identifications of component	Online and offline component identifications (class ID) of the target device do not agree.
Different versions of component	Online and offline component versions of the target device do not agree.

Comparison of online and offline data

Simatic iMap offers the facility for comparing the online data of devices and technological functions of a plant with the offline data of the generated Simatic iMap project, and to diagnose any differences in this manner. This comparison is not carried out automatically for performance reasons, but is recommendable for safety reasons in order to prevent any faults during runtime.

The following are checked in the case of connectors and interconnections:

- Correct/actual number of interconnections
- Correct/actual comparison of transmission properties of interconnections
- Correct/actual number of connectors of technological functions
- Correct/actual comparison of connectors data types
- Correct/actual comparison of configured substitute values.

The following are checked in the case of programs:

- Correct/actual comparison of blocks of all user programs
- Correct/actual comparison of all device-specific data, e.g. hardware and network configurations.

Checking of the connectors and interconnections is not possible for singleton components and non-Simatic S7 devices.

Diagnostics of interconnection status

Interconnections in Simatic iMap are displayed in specific colors depending on the interconnection status (see Table 5.35).

Table 5.35 Colored representation of interconnection status in Simatic iMap

Color	Meaning
Black	The interconnection is present and OK.
Red	The interconnection is faulty, i.e. the output of the provider's technological function is faulty or the transmission path is logically (e.g. by a router in the transmission path of cyclic interconnections) or physically interrupted.
Gray	No interconnection information is available. The device is not accessible, or the interconnection has not been loaded.
Green	The interconnection is selected in Simatic iMap.

Diagnostics of connector values

The type of representation of a connector value depends on its validity, and is derived from the quality code of the transmitted data (see Table 5.36). The quality code allows qualitative evaluation of data. It is transmitted together with data from the provider (output) to the consumer (input), or set by the consumer itself in the event of a communications fault. The quality codes used with Profinet CBA are oriented according to those defined by the PNO in "Profibus PA, Profile for Process Control Devices, General Requirements, V3.0, October 1999".

Table 5.36 Representation of validity of connector values in Simatic iMap

Representation	Meaning
Black	The value is valid.
Gray	The validity of the value cannot be determined.
Gray italics	The value is a substitute value.
Red	The value is invalid, an interconnection fault is present, or the value has not yet been confirmed by the target system following setting in Simatic iMap.
Red with exclamation mark	The value is invalid, no vacant device resources are available.
Red with question mark	The value is invalid. It has not yet been confirmed, or the target system is not (yet) accessible.

Processing of the online values of Profinet variables in the variable table

A variable table permits connectors to be monitored and control values to be set for inputs of any technological functions within a Simatic iMap project for test and diagnostics purposes. The connectors are inserted into the variable table using drag&drop (see Table 5.37 and Fig. 5.62).

Table 5.37 Structure of a variable table in Simatic iMap

Column in variable table	Meaning
No	Line number
	Symbolic display of whether the table entry is monitored online, is deactivated or not accessible.
Device	Device name
Function	Name of technological function
Connector	Connector name
Type	Data type of connector
Format	Display format of online value
Online value	Online value of connector
Control value	Control value for setting the input
Comment	Line comment

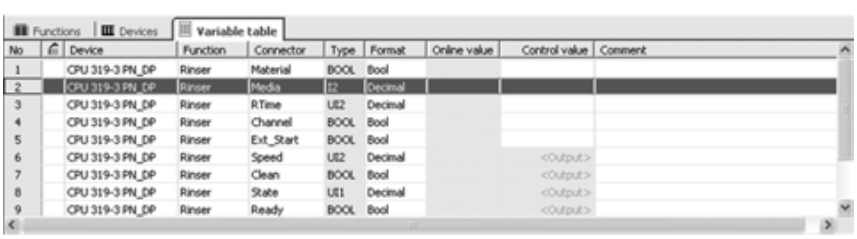


Fig. 5.62 Example of a variable table in Simatic iMap

Online device analysis

The most comprehensive online information on a Profinet controller is provided by the online device analysis. Following selection of the controller to be analyzed by means of its IP address, the following data are read out and saved as a file in HTML format:

- Performance parameters (actual value and maximum value)
- Configuration data of the device and technological function
- The configuration data of devices with proxy functionality, and of the technological function of the coupled Profibus devices
- Diagnostics information such as fault statistics and timeouts.

Access to variables with OPC

In order to access process variables using OPC mechanisms, an OPC symbol file must first be created in Simatic iMap. This serves to configure a Simatic Net OPC server. The OPC server permits OPC client applications to carry out a symbolic access to variables within the devices of a plant. In the case of Profibus devices integrated in the plant via a proxy, variable values are transmitted between OPC server and Profibus slaves using routing mechanisms in the Profibus master.

Since a corresponding number of OPC symbol files result when dividing the total plant into several Simatic iMap projects, the access path to variables can be unambiguously defined even beyond the limits of projects by using an OPC prefix (Fig. 5.63).

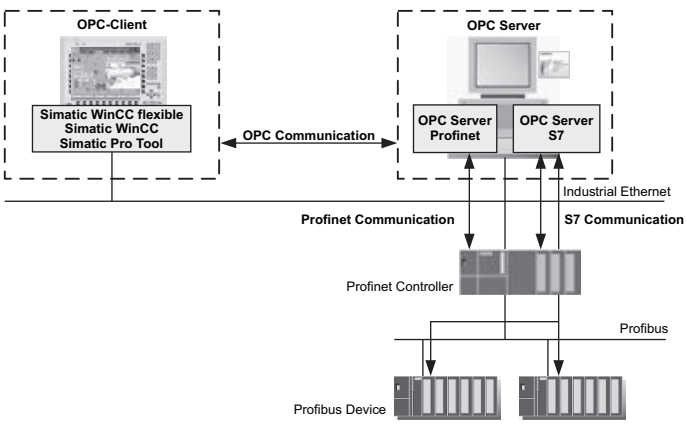


Fig. 5.63 Access to information variables via OPC

OPC client and OPC server applications can be executed in the same device or on different devices.

Information variables

The OPC symbol file contains the address information of the information variables accessible via OPC for all devices configured using Simatic iMap. Information variables therefore include all device variables which can be read and/or written via OPC.

Information variables are:

- Process variables, including all interconnectable and non-interconnectable variables
- System variables
- Device-specific information variables (S7 variables).

Table 5.38 Structure of runtime name of information variables

Element	Meaning
Protocol ID	Communications protocol for access to the variables (PN: Profinet, S7: S7 communication).
Connection name	Connection or device via which the variable can be accessed
Variable name	Symbolic name of connection

Table 5.39 Structure of symbolic name of information variables in the Simatic Net symbol file configurator

Element	Meaning
<Project_prefix>	Optional: user-defined ID which is unambiguous throughout the project and is assigned when generating the OPC symbol file.
<Chart 1>... <Chart n>	Optional: name of chart element in which the variable is present in the Simatic iMap project. May be multi-stage (chart in chart).
<Function>	Name of technological function in which the variable is present in the Simatic iMap project.
<Variable>	Symbolic name of connection.

Process variables are assigned to the interconnectable and non-interconnectable connections of technological functions. Inputs can be read and written, outputs can only be read (Fig. 5.64). Process variables are identified at the OPC interface by a runtime name (OPC item ID). The OPC item ID is the identification used by the OPC server for a process variable. An OPC item ID is passed from the OPC client to the OPC server to identify a process variable, and is unambiguous for the OPC server. It is either a symbolic name or a runtime name.

A runtime name is an OPC item ID containing protocol and addressing information for assignment purposes, and which is directly accepted by the OPC server

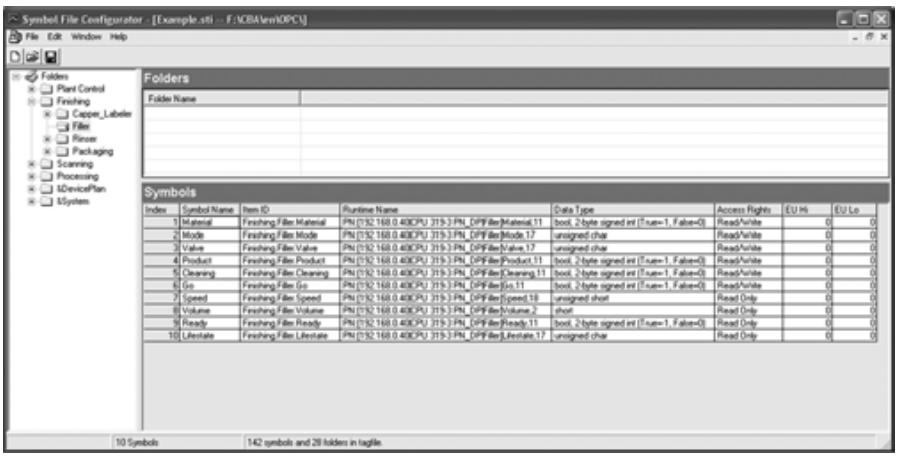


Fig. 5.64 Process variables in the Simatic Net symbol file configurator

Table 5.40 Structure of connection name within the runtime name for Profinet CBA

Element	Meaning
IP address	Profinet controller: IP address Profibus device: IP address of the Profinet controller with proxy functionality to which the Profibus device is connected.
devicename	Name of device.
funcname	Name of technological function.
variable	Symbolic name of connection.

without application of a symbol file. The syntax of the runtime name generally has the structure (see also Table 5.40):

<Protocol ID>:[<Connection name>]<Variable name>;

With Profinet CBA, the representative of the connection name comprises the IP address, device name, function name and variable name (Table 5.40).

<Connection name>: [IP address|<devicename>|<funcname>|<variable>]

Example of a runtime name with Profinet CBA:
PN:[192.168.0.40|CPU 319-3 PN_DP|Filler]Material

A special browser, for example the Simatic Net symbol file configurator, loads the OPC symbol file and presents information variables hierarchically in a tree structure. The variables are accessed in this case using a symbolic name with the following structure (see Table 5.39):

[<Project_prefix>] [<Chart 1>...<Chart n>] <Function> <Variable>

Example: Finishing.Filler.Material

System variables apply throughout the plant and can only be read (Fig. 5.65). The runtime name has the following structure (see also Table 5.41):

PN:[SYSTEM]<variable>

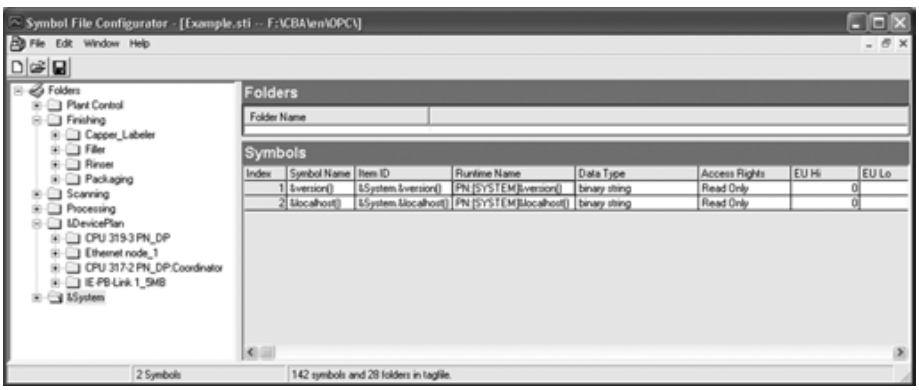


Fig. 5.65 System variables in the Simatic Net symbol file configurator

Table 5.41 Structure of runtime name for system variables

Element	Meaning
SYSTEM	Name of system variable.
variable	&localhost(): name of host computer. &version(): version of Profinet core server.

Device-specific information variables contain information which is assigned to the respective devices. The runtime name has the following structure (see also Table 5.42 and Fig. 5.66):

PN:[IP address|<devicename>]<variable>

Table 5.42 Structure of runtime name for device-specific information variables

Element	Meaning
IP address	Profinet controller: IP address Profibus device: IP address of Profinet controller with proxy functionality to which the Profibus device is connected.
devicename	Name of device
variable	&statepath(): Status of a connection to the communications partner as string "DOWN": connection is not established "UP": connection is established "RECOVERY": connection is being established "ESTABLISH": reserved &statepathval(): Status of a connection to the communications partner as value 1: connection is not established 2: connection is established 3: connection is being established 4: reserved

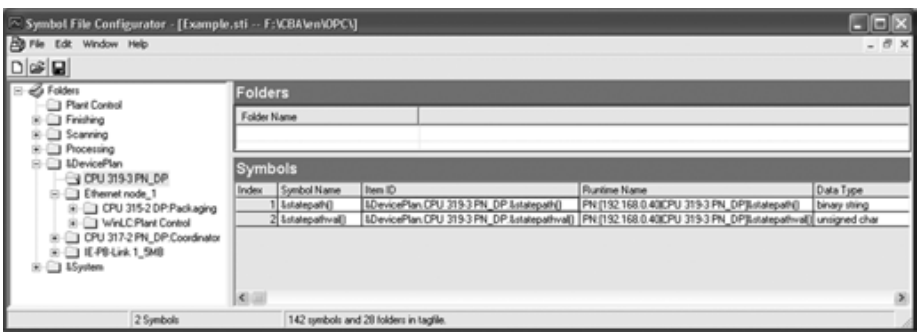


Fig. 5.66 Device-specific information variables in the Simatic Net symbol file configurator

5.8.3 Diagnostics using the Display Elements of Profinet CBA Devices

The status of Simatic S7, Simatic Net or Profinet controllers and their communications interfaces can be determined using the LED display elements on the front panel. The LEDs permit initial diagnostics in the event of a fault. The function of the display elements with Profibus devices does not change when used within a plant implemented with Profinet CBA.

This section only describes the display elements of Profinet controllers. A description of the display elements for Profinet controllers which simultaneously support the Profinet IO functionality can be found in Chapter 4.3.

Display elements with Simatic S7-CPU 31x-yPN/DP

See Chapter 4.3 “Diagnostics Functions for Profinet IO”.

Display elements of software-based Simatic PLCs

The software-based Simatic CPU WinLC PN (Windows Logic Controller) is part of the Simatic WinAC (Windows Automation Center) software package, and available in two versions:

- Simatic WinLC PN V1.1 as stand-alone product
- Simatic WinAC PN-Option V4.1 as option package for Simatic WinAC software PLC V4.1.

The display elements for statuses and faults are based on the LEDs of a Simatic S7-CPU 31x and are visible on the control panel on the programming device/PC monitor (see Tables 5.43 and 5.44).

The display element ON is always switched on, the display element BATF (battery fault) is always switched off.

Table 5.43
Status and fault displays of WinLC PN V1.1 and WinAC PN-Option V4.1

INTF red	EXTF red	FRCE yellow	RUN green	STOP yellow	Meaning
1	x	x	x	x	Internal fault. The CPU’s diagnostics buffer must be read to permit exact fault locating. Causes may be: – Firmware error – Programming error – Arithmetic error – Counter error – Time error Only WinAC PN-Option V4.1: If the control program processes the error by executing OB80, OB121 or OB122, the INTF display is switched off after 3 seconds if no further errors are present.

Table 5.43
Status and fault displays of WinLC PN V1.1 and WinAC PN-Option V4.1 *(continued)*

INTF red	EXTF red	FRCE yellow	RUN green	STOP yellow	Meaning
x	1	x	x	x	External fault. The CPU's diagnostics buffer must be read to permit exact fault locating. Causes may be: – Hardware fault – Parameterization error – Faulty memory card – I/O error – Communications error
x	x	0	x	x	Active force job running. WinLC PN V1.1: always switched off WinAC PN-Option V4.1: not present.
x	x	x	1	0	CPU is in RUN status.
x	x	x	0/1	x	0.5 Hz: CPU is in HOLD status. 2 Hz: CPU is in STARTUP status.
x	x	x	x	1	CPU is in STOP, HOLD or STARTUP status.
0/1	0/1	0/1	0/1	0/1	Module or system fault: the controller must be stopped, restarted and subsequently reset. If WinLC is used as a service, it must be stopped in the Windows control panel, and restarted.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 5.44
LED status display of communications interface of WinLC PN V1.1 and WinAC PN-Option V4.1

BUSF1 red	BUSF2 red	BUSF3 red	BUSF4 red	Meaning
0/1	x	x	x	Station fault, or at least one DP slave could not be accessed.
x	0	x	x	Not supported.
x	x	0	x	WinLC PN V1.1: not present WinAC PN-Option V4.1: not supported
x	x	x	0	WinLC PN V1.1: not present WinAC PN-Option V4.1: not supported

0: off, 1: on, 0/1: flashes, x: indefinite

Display elements with Simatic Net CP 343-1,CP 343-1 Advanced and CP 443-1 Advanced

See Chapter 4.3 “Diagnostics Functions for Profinet IO”.

Display elements with Simatic Net Gateway IE/PB-Link

The LED display elements for the operating status are present on the front panel of the IE/PB-Link (Tables 5.45 and 5.46).

Table 5.45 LED status and fault displays of the gateway IE/PB-Link

SF red	BUSF red	RUN green	STOP yellow	Meaning
0	0	0/1	1	IE/PB-Link is in STARTUP status.
0	0	1	0	IE/PB-Link is in RUN status.
0	0	1	0/1	IE/PB-Link is in HOLD status.
0	0	0	1	IE/PB-Link is in STOP status.
0	1	1	0	IE/PB-Link is in RUN status. Fault on Profibus or incorrect Profibus configuration.
0	0/1	1	0	IE/PB-Link is in RUN status. Fault in one or more DP slaves.
1	0	0	1	IE/PB-Link is in STOP status. A fault has occurred.
1	1	0	0/1	The IE/PB-Link is waiting for a firmware update. The IE/PB-Link contains an incomplete or faulty FW release.
0	0	0/1	0	IE/PB-Link firmware is being loaded.
0/1	0/1	0/1	0/1	Module or system fault. The IE/PB-Link must be switched off and on again in this case.

0: off, 1: on, 0/1: flashes, x: indefinite

Table 5.46 LED status display of communications interface of IE/PB-Link

FD green	FAST green	LINK green	RX/TX green	Meaning
0	x	x	x	A half-duplex connection is present.
1	x	x	x	A full-duplex connection is present.
x	0	x	x	The port is operating at 10 Mb/s.
x	1	x	x	The port is operating at 100 Mb/s.
x	x	0	x	There is no connection to the Ethernet.
x	x	1	x	There is a connection to the Ethernet.
x	x	x	0/1	The port is sending or receiving data over the Ethernet.

0: off, 1: on, 0/1: flashes, x: indefinite

The display elements for the Ethernet communications status are located on the front panel and on the RJ45 socket of the Industrial Ethernet port of the IE/PB-Link.

6 Profinet User Program Interfaces with Simatic S7

The Step 7 programming software offers a variety of possibilities for structuring the user program of a Simatic S7 automation system and for dividing it into autonomous program components. This offers the following advantages:

- Complex routines can be programmed more clearly.
- Individual program components can be standardized.
- Program organization is simplified.
- Programs are easier to modify.
- Program debugging is simplified since it can be carried out in sections.
- Commissioning is altogether simplified.

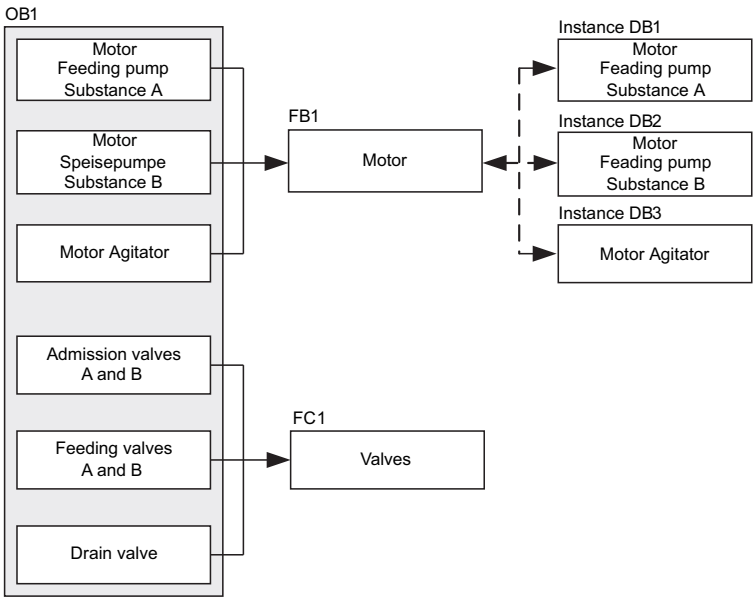
The Simatic programming languages integrated in Step 7 comply with the DIN EN 61131-3 standard. Profinet CBA and Profinet IO are supported by Step 7 Version V5.3 and later. The basic package executes with the Microsoft Windows 2000 Professional and Windows XP Professional operating systems.

6.1 Fundamentals

The program sections of a structured user program are referred to as blocks. The block types shown in Table 6.1 are available for structuring an S7 user program.

Table 6.1 Block types in Simatic S7

Block	Abbreviation	Function
Organization block	OB	Definition of user program structure.
System function block	SFB	System function block/system function call: Blocks which are integrated in a Simatic S7 CPU and which make important system functions accessible.
System function call	SFC	
Function block	FB	Blocks programmed by a user and possessing a "memory".
Function call	FC	Blocks containing program routines for frequently used functions.
Instance data block	Instance DB	Instance data block: Data block for saving dummy parameters, the "dummy values" for the actual parameters valid during runtime, and the static data of an FB or SFB. They are automatically assigned to these code blocks when called.
Data block	DB	Data areas for saving user data.



OB1:	OB1 is the interface to the CPU's operating system, and contains the main program. Blocks FB 1 and FC 1 are called in OB 1, and the specific parameters required to control the process are transferred.
FB1:	The motors of the feeding pumps for substance A, substance B and the motor agitator can be controlled by a single function block since the requirements for operating the motors (switch on, switch off, count number of operations, etc.) are identical.
Instance DB:	The actual parameters and the static data for controlling the motors for the feeding pumps for substance A, substance B and the motor agitator are different, and are therefore saved in three instance DBs assigned to FB 1.
FC1:	The admission and feeding valves for substances A and B and the drain valve use a common code block. Since only functions for opening and closing need be programmed, one single FC is sufficient.

Fig. 6.1 Examples of the hierarchy of block calls

Whereas data blocks exclusively save data, OB, FB, SFB, FC and SFC contain program components and are therefore also referred to as code blocks. Both the maximum number of blocks per type and the maximum size of a block depend on the Simatic S7 CPU on which the user program is executed.

The program structure is defined by distributing the user program between various code blocks and by the hierarchy of the block calls (Fig. 6.1).

6.1.1 Organization Blocks

A range of organization blocks (OB) are available for Simatic S7 CPUs for executing the user program. OBs are the interface between the user program and the operating system of a CPU. They permit event-controlled processing of special program components within the user program. Start events which initiate the calling of a certain OB are also referred to as alarms. For example, the receipt of a diagno-

Table 6.2 OB priority classes

OB	Start event	Priority class	Remarks
1	End of startup or end of OB 1	1	Free cycle
10-17	Time-of-day interrupts 0-7	2	No default time
20-23	Time-delay interrupts 0-3	3-6	No default time
30 31 32 33 34 35 36 37 38	Cyclic interrupt 0 Cyclic interrupt 1 Cyclic interrupt 2 Cyclic interrupt 3 Cyclic interrupt 4 Cyclic interrupt 5 Cyclic interrupt 6 Cyclic interrupt 7 Cyclic interrupt 8	7 8 9 10 11 12 13 14 15	Default: 5-s cycle Default: 2-s cycle Default: 1-s cycle Default: 500-ms cycle Default: 200-ms cycle Default: 100-ms cycle Default: 50-ms cycle Default: 20-ms cycle Default: 10-ms cycle
40-47	Hardware interrupt 0-7	16-23	
55	Status interrupt	2	DPV1 alarms
56	Update interrupt		
57	Manufacturer-specific interrupt		
60	Multicomputing interrupt	25	Call of SFC 35 “MP_ALM”
61-64	Synchronous cycle interrupts 1-4	25	
65	Technology synchronization interrupt	25	
70	I/O redundancy error	25	Only in H systems
72	CPU redundancy error	28	
73	Communication redundancy error	25	
80	Time error	26/28	Asynchronous errors
81	Power supply fault	26/28 with S7-300 25/28 with S7-400 25/28 with S7-318 The lower priority class applies in each case if the asynchronous error occurs during execution of OBþ100-102.	
82	Diagnostic interrupt		
83	Insert/remove module interrupt		
84	CPU hardware fault		
85	Program error		
86	Module failure, failure of a central expansion unit, a DP master system, or a station with Profibus DP or Profinet IO.		
87	Communication error		
88	Processing interrupt	28	
90	Warm restart or cold restart or deletion of a block being processed in the OB 90 or loading of an OB 90 into the CPU or end of OB 90	29	Background cycle
100 101 102	Warm restart Hot restart Cold restart	27	Startup
121	Programming error	Priority class of OB causing the error	Synchronous errors
122	I/O access error		

sis alarm triggered by a field device, or the failure of such a device, results in calling of an OB reserved for this event by the CPU's operating system.

Since the alarm-driven calling of an OB frequently means that another currently processed OB is interrupted, priority classes are defined for OB processing. These extend from 0 to 29, where 0 corresponds to the lowest priority and 28 to the highest. Priority class 29 corresponds to priority class 0. Priority classes 27 and 28 are only valid during the startup (execution of OB 100 - 102).

OBs with the same priority are executed in the sequence in which they are called. Priority classes can be configured depending on the type of CPU or OB (Table 6.2).

6.1.2 Function Blocks

Function blocks (FB) are code blocks with a "memory" which are programmed by the user. They have an assigned instance data block (instance DB) as memory. Parameters transferred to an FB as well as the static variables are saved in this data block. Temporary variables are saved in the local data stack (L stack), an area within the CPU memory for saving temporary data.

Data saved in the instance DB are not lost following processing of the FB. In contrast to this, data saved in the local data stack are no longer available following processing of the FB.

An FB contains a program which is always executed when the FB is called by another code block. Function blocks facilitate the programming of frequently repeated, complex functions.

6.1.3 Functions

Functions (FC) are also code blocks which can be programmed by the user. However, an FC does not have a "memory". Temporary variables as well as parameters transferred to the function when the latter is called are saved in the L stack. They are lost following processing of the FC.

Functions can save data in global data blocks. Because an FC does not have an assigned memory, actual parameters must always be specified for it. It is not possible to assign initial values to local data.

An FC contains a program which is always executed when the FC is called by another code block. Functions can be used in two cases:

- To return a function value to the calling block
  (example: mathematical functions)
- To execute a technological function.

6.1.4 Data Blocks

In contrast to code blocks, data blocks do not contain Step 7 statements. They are used to save user data, i.e. variable data which are processed by the user program.

Global data blocks serve to accommodate user data which can be used by all other blocks.

Instance data blocks are assigned to a function block with transfer parameters. The current parameters and the static data of the FB are saved in the instance DB. The variables declared in the FB determine the structure of the instance data block. “Instance” means the calling of a function block. For example, if a function block is called five times in the S7 user program, five instances of this block exist.

Data blocks can have a variable size. The maximum permissible size depends on the CPU properties.

6.1.5 System Functions and System Function Blocks

System functions (SFC) and system function blocks (SFB) are integral functions in the operating system of a Simatic S7 CPU. In addition, SFCs are frequently called implicitly by SFBs. Both SFCs and SFBs can be called by the user program like normal functions and function blocks. SFCs and SFBs are used to implement a number of important system functions for Profinet IO and Profibus DP.

General meaning of certain SFC and SFB parameters

The meaning and function of certain SFC parameters are identical for all SFC calls described below. This particularly applies to the REQ, BUSY, LADDR and RET_VAL parameters.

REQ parameter

The REQ input parameter (REQuest) is used exclusively to trigger a request for the system function. The request is started if REQ = TRUE.

Table 6.3 Different cases when calling an asynchronous function

Case	Call	REQ	BUSY	RET_VAL	Remarks
1	1	1	1	W#16#7001	With vacant system resources and correct initialization of the input parameters.
			0	Error code	With temporarily occupied system resources or errors in the input parameters.
2	2-n	0 or 1	1	W#16#7002	Request is still being processed.
3	n	0 or 1	0	=0	Request completed without errors
			0	<0	Error code
				>0	SFC 13 “DPNRM_DG”, SFC 67 “X_GET”, SFC 72 “I_GET”: Quantity of delivered data in bytes. SFC 59 “RD_REC”: Length of actually transmitted record if the destination range is greater than the length of the transmitted record.

Asynchronous SFCs may require several CPU cycles for processing. In this case, the BUSY parameter must be taken into account in the call (Table 6.3). During processing of a request, the REQ parameter is evaluated by an asynchronous function.

BUSY parameter

The BUSY parameter indicates with asynchronous functions whether the triggered request is being executed or whether the execution has already been completed.

LADDR parameter

The LADDR always contains a logical address. This can be, for example, the start address of an input/output module or the diagnostics address of a distributed field device. The input/output of logical addresses with LADDR is always in hexadecimal format, but the configuration of logical addresses in HW-Config is in decimal format.

Binary result bit (BIE bit)

The BIE bit is the eighth bit in the status word of a Simatic S7 CPU. An SFC with a value of "0" in the BIE bit indicates that an error has occurred when executing the function. If faulty execution of the SFC is indicated by the BIE bit, the SFC-specific output parameters must not be evaluated.

RET_VAL parameter

Some SFCs possess the RET_VAL output parameter. This is set by the system function, and provides information on whether the system function has been executed successfully or not (Table 6.4). In the event of an error, the return value contains:

- a general error code which can refer to any system function (Fig. 6.2) or
- an SFC-specific error code which only refers to the respective system function (Fig. 6.3).

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	1	No. of parameter causing the error (parameter 1 to parameter 111)							Event number (0-127)							

Fig. 6.2 Coding of RET_VAL parameter with a general error code

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	1	0	0	0	0	0	0	0	1	Error class (0-7)			Single error (0-15)			

Fig. 6.3 Coding of RET_VAL parameter with a specific error code

Table 6.4 General error codes of the RET_VAL parameter

Error code (W#16#...)	Description
8x7F	Internal error: This error code indicates an internal error in parameter x. The error has not been caused by the user; it cannot be eliminated by the user either.
8x01	Illegal syntax ID with an ANY parameter.
8x22 8x23	Range length error when reading a parameter. Range length error when writing a parameter. This error code indicates that the parameter x is completely or partially outside the operand range, or that the length of a bit array with an ANY parameter is not divisible by 8.
8x24 8x25	Range length error when reading a parameter. Range length error when writing a parameter. This error code indicates that the parameter x is in a range which is illegal for the system function. The description of the respective function specifies the ranges which are illegal for the function.
8x26	The parameter contains a number which is too large for a time cell. This error code indicates that the time cell specified in parameter x does not exist.
8x27	The parameter contains a number which is too large for a time cell (number error of counter). This error code indicates that the time cell specified in parameter x does not exist.
8x28 8x29	Alignment error when reading a parameter. Alignment error when writing a parameter. This error code indicates that the reference to parameter x is an operand whose bit address is not 0.
8x30 8x31	The parameter is located in the write-protected global DB. The parameter is located in the write-protected instance DB. This error code indicates that the parameter x is located in a write-protected data block. If the data block has been opened by the system function itself, the system function always outputs the value W#16#8x30.
8x32 8x34 8x35	The parameter contains a DB number which is too large (number error of DB). The parameter contains an FC number which is too large (number error of FC). The parameter contains an FB number which is too large (number error of FB). This error code indicates that the parameter x contains a block number which is larger than the maximum permissible block number.
8x3A 8x3C 8x3E	The parameter contains the number of a DB which is not loaded. The parameter contains the number of an FC which is not loaded. The parameter contains the number of an FB which is not loaded.
8x42 8x43	An access error has occurred while the system wanted to read a parameter out of the I/O area of the inputs. An access error has occurred while the system wanted to write a parameter into the I/O area of the outputs.
8x44	Error during n-th (n > 1) read access following occurrence of an error.
8x45	Error during n-th (n > 1) write access following occurrence of an error. This error code indicates that access to the desired parameter was denied.

Memory areas with SFC/SFB call parameters

Special IDs are used in the description of the SFC/SFB calls for the memory areas usable within a Simatic S7 CPU (see Table 6.5).

Table 6.5 Memory areas of SFC/SFB parameters

Type	Memory area	Unit
I	Process input image	Bit: Input IB: Input byte IW: Input word ID: Input doubleword
Q	Process output image	Bit: Output QB: Output byte QW: Output word QD: Output doubleword
F	Bit memory (flag)	Bit: Bit memory MB: Memory byte MW: Memory word MD: Memory doubleword
D	Data block	Bit: Data bit DBB: Data byte DBW: Data word DBD: Data doubleword
L	Local data	Bit: Local data bit LB: Local data byte LW: Local data word LD: Local data doubleword

6.1.6 Records

System data and parameters are saved on Simatic S7 modules as data records. Records are numbered from 0 up to a maximum of 65535, were not every module possesses all records. Depending on the type of module, there are system ranges which can be accessed from the user program only by read operations or only by write operations.

For Profinet IO, the scope of previous records has been extended by two further types of diagnostics records, the configuration and diagnostics records.

Table 6.6 Records which can be written with Simatic S7 modules

Record No.	Contents	Size	Can be written using	Remarks
0	Parameters	S7-300: 2-14 bytes	SFB 53 “WRREC” SFB 81 “RD_DPAR”	Can only be written with S7-400
1	Parameters	S7-300: 2-14 bytes	SFB 53 “WRREC” SFB 81 “RD_DPAR”	DS0 + DS1 = 16 bytes
2-127	User data	ð 240 bytes	SFB 53 “WRREC” SFB 81 “RD_DPAR”	-
128-240	Parameters	ð 240 bytes	SFB 53 “WRREC” SFB 81 “RD_DPAR”	-

The structure and size of vendor-specific diagnostics records depend on the vendor. Information concerning these records can be found in the GSDML file of the respective device.

Detailed information on the records can be found in the Profinet specifications “Application Layer services for decentralized periphery and distributed automation” and “Application Layer protocol for decentralized periphery and distributed automation”.

Table 6.7 Records which can be read with Simatic S7 modules

Record No.	Contents	Size	Can be read using	Remarks
0	Module-specific diagnostics	4 bytes	SFC 51 “RDSYSST” SZL_ID: 00B1h SFB 52 “RDREC”	
1	Channel-specific diagnostics	S7-300: 16 bytes S7-400: 4-220 bytes	SFC 51 “RDSYSST” SZL_ID: 00B2h and 00B3h SFB 52 “RDREC”	Incl. DS0
2-127	User data	ð 240 bytes	SFB 52 “RDREC”	
128-240	Diagnostics data	ð 240 bytes	SFB 52 “RDREC”	

Table 6.8 Important records for reading the I/O status with Profinet IO

Record No. (W#16#...)	Contents	Size
801E	Substitute values of a submodule.	0 – 4176 bytes
8028	Current input data of a submodule.	
8029	Current output data of a submodule.	

Table 6.9 Important records for reading the status of Profinet interfaces

Record No. (W#16#...)	Contents	Size
802A	Current settings of a port.	0 – 4176 bytes
802B	Configured settings of a port.	
802F	Configured settings of a port.	
8060	Current settings of an optical port.	
8061	Configured settings of an optical port.	
8062	Configured settings of an optical port.	
8070	Configured settings of a Profinet interface.	
F831	Common record for the configured settings of the Profinet interface and its ports (only settings of the IRT parameters).	
F841	Common record for the current settings of the Profinet interface and its ports.	
F842	Common record for the configured settings of the Profinet interface and its ports.	

Table 6.10 Important records for reading/writing of identification and maintenance (I&M) data with ProfinetþIO

Record No. (W#16#...)	Contents	Size
AFF0	I&M 0 data (read-only).	0 – 4176 bytes
AFF1-AFFF	I&M 1 – 15 data.	
F840	List of submodules which send different I&M 0 data.	

Table 6.11 Important records for reading/writing of protocol parameters with ProfinetþIO

Record No. (W#16#...)	Contents	Size
F821	All supported APIs of an IO Device.	0 – 4176 bytes
F830	List of internal error events (e.g. causes for interruption in a communications relation).	

Vendor-specific diagnostics records vary with regards to structure and size. Information concerning these records can be found in the GSDML file of the respective device.

Each record transmission triggered occupies memory in a Simatic S7 CPU for the asynchronous processing of requests. If several requests are active simultaneously, it is ensured that they do not influence one another and that all requests are handled correctly. However, the maximum number of simultaneous requests differs according to the type of CPU, and can be obtained from the performance data of the respective CPU. If the maximum number of simultaneous requests has been reached, a corresponding error code is output in the RET_VAL parameter. The request must be carried out again in this case.

Parameters in records can be static or dynamic. Static parameters, for example the input delay of a digital module, can be programmed using Step 7. In contrast to this, dynamic parameters such as the limit of an analog input module can also be modified during operation.

6.1.7 Profinet IO Records

Profinet IO supports users by means of a uniform diagnostics concept. In the event of a fault, the faulty IO Device generates a diagnostics interrupt and sends this to the IO controller. This interrupt results in calling of a corresponding OB in the user program.

If a device or module is replaced in the event of a fault, the IO controller automatically carries out parameterization and configuration of the new device or module. Following fault-free configuration, the cyclic exchange of user data restarts automatically.

Both the diagnostics and configuration information can be called in the user program using records.

Addressing levels

Analogous to the Profinet IO device model, the configuration and diagnostics concept is also divided hierarchically into four addressing levels (Fig. 6.4):

- Application Relation (AR)
- Application Process Identifier (API)
- Slot
- Subslot.

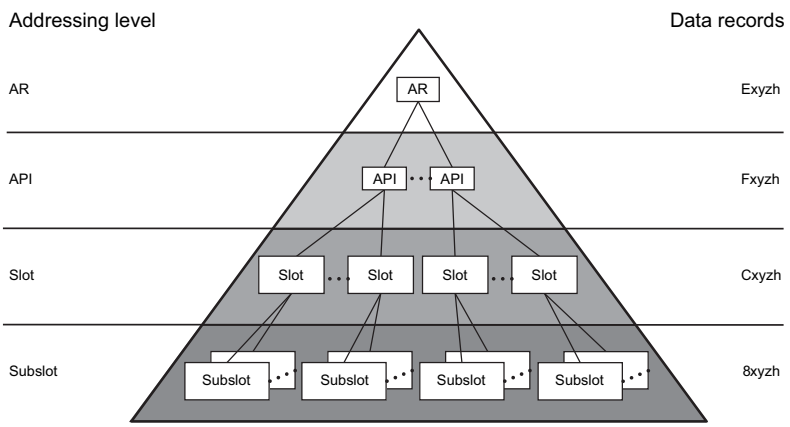


Fig. 6.4 Addressing levels for configuration and diagnostics records

A group of diagnostics and configuration records exists for each addressing level. The records differ in the first digit of the record number (Table 6.12).

Table 6.12 Record numbers and addressing levels

Record No. (W#16#...)	Meaning
Exyz	Diagnostics or configuration record for an AR.
Fxyz	Diagnostics or configuration record for an API.
Cxyz	Diagnostics or configuration record for a slot.
8xyz	Diagnostics or configuration record for a subslot.

Record version

Configuration or diagnostics records can exist in several versions. To differentiate them, records are assigned a version number (BlockVersion). The version number comprises two bytes. BlockVersionHigh identifies the version of a record; BlockVersionLow is used for further differentiation within a version. The structure of the BlockVersion is described in Appendix.

Profinet IO diagnostics records

Records are generated for channel diagnostics if a channel has a fault and/or has triggered an interrupt (see Table 6.13). If a fault is not present, a diagnostics record with a length of 0 is returned. A maximum of 400 channel faults can be represented at any one time.

Table 6.13 Important diagnostics records with Profinet IO

Record No. (W#16#...)	Contents	Size
800A	In event of fault – Channel diagnostics and/or – enhanced channel diagnostics for a submodule slot.	0 – 4176 bytes
C00A	a module slot.	
E00A	an AR.	
F00A	an API.	
800B	In event of fault – Channel diagnostics and/or – enhanced channel diagnostics and/or- vendor-specific diagnostics for a submodule slot.	0 – 4176 bytes
C00B	a module slot.	
E00B	an AR.	
F00B	an API.	
800C	In event of fault, with maintenance request and with maintenance requirement – Channel diagnostics and/or – enhanced channel diagnostics and/or – vendor-specific diagnostics for a submodule slot.	0 – 4176 bytes
C00C	a module slot.	
E00C	an AR.	
F00C	an API.	
F80C	an IO Device.	
8010	With maintenance requirement – Channel diagnostics and/or – enhanced channel diagnostics for a submodule slot.	0 – 4176 bytes
C010	a module slot.	
E010	an AR.	
F010	an API.	
8011	With maintenance request – Channel diagnostics and/or – enhanced channel diagnostics for a submodule slot.	0 – 4176 bytes
C011	a module slot.	
E011	an AR.	
F011	an API.	

Table 6.13 Important diagnostics records with Profinet IO *(continued)*

Record No. (W#16#...)	Contents	Size
8012	With maintenance requirement – Channel diagnostics and/or – enhanced channel diagnostics and/or – vendor-specific diagnostics for a submodule slot.	0 – 4176 bytes
C012	a module slot.	
E012	an AR.	
F012	an API.	
8013	With maintenance request – Channel diagnostics and/or – enhanced channel diagnostics and/or – vendor-specific diagnostics for a submodule slot.	0 – 4176 bytes
C013	a module slot.	
E013	an AR.	
F013	an API.	

User Structure Identifier (USI)

The User Structure Identifier (USI) provides information on the type of diagnostics associated with the diagnostics data of a diagnostics record. The USI is part of a diagnostics record. Its structure is described in Chapter 6.2.

Structure of the Profinet IO diagnostics records

The fundamental structure of Profinet IO diagnostics records is identical. However, the contents and size of the diagnostics records vary according to the type of diagnostics. This particularly applies to records with vendor-specific diagnostics data. Information on these records can be found in the manual of the respective device. The number of a diagnostics record corresponds to the system shown in Fig. 6.5.

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Addressing level: 8h: Submodule Ch: Module Eh: AR Fh: API				0	0	0	0	Diagnosis reason: 0Ah/0Bh: Fault 0Ch: Fault, Maintenance required and demanded 10h/12h: Maintenance required 11h/13h: Maintenance demanded							

Fig. 6.5 Number structure of a diagnostics record

The following Fig. 6.6 shows the schematic structure of the diagnostics records listed in Table 6.13.

A data block “Channel diagnostics data” is generated for each subslot with faulty channels. If no faults are present, the length of this data block is 0. The data block

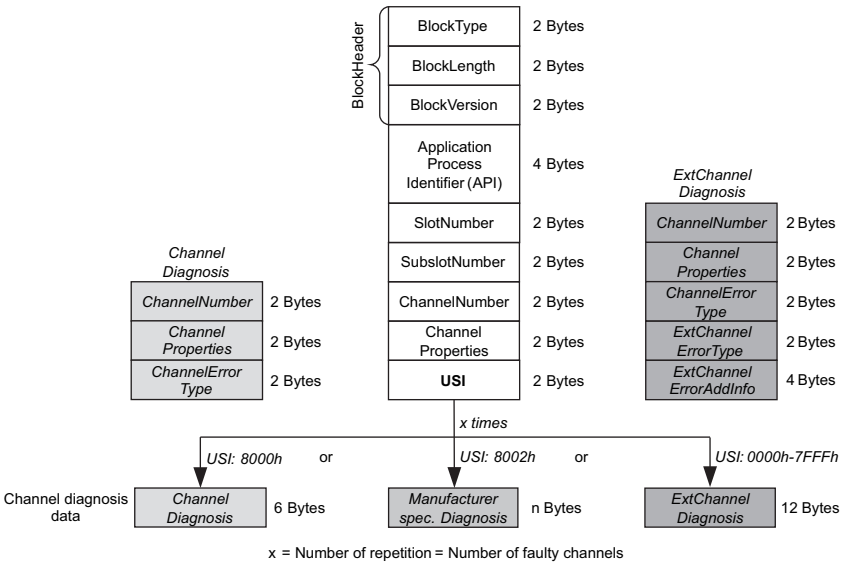


Fig. 6.6 Structure of a diagnostics record of BlockVersion 0101

is present once for each faulty channel. The number of faulty channels can be determined using the value of the parameter "BlockLength" for a diagnostics record of BlockVersion 0101 for channel diagnostics and enhanced channel diagnostics by means of Table 6.14. The meaning of the most important block elements of a diagnostics record is described in Chapter 6.2.

Table 6.14 Number of faulty channels with diagnostics records of BlockVersion 0101

USI (W#16#...)	Block length			
	22 bytes	28 bytes	34 bytes	40 bytes
8001	1 channel	2 channel	3 channel	4 channel
8002	-	1 channel	-	2 channel

Profinet IO configuration records

The configuration of a Profinet IO system is described in configuration records. If a replacement is necessary, for example in the case of a device or module fault, the IO controller automatically carries out parameterization and configuration of the

Table 6.15 Important configuration records with Profinet IO

Record No. (W#16#...)	Contents	Size
8000	Desired configuration at subslot level.	22 - 4176 bytes
C000	Desired configuration at slot level.	
E000	Desired configuration at AR level.	

Table 6.15 Important configuration records with Profinet IO *(continued)*

Record No. (W#16#...)	Contents	Size
8001	Actual configuration at subslot level.	0 - 4176 bytes
C001	Actual configuration at slot level.	
E001	Actual configuration at AR level.	
E002	Deviations between desired and actual configurations of the respective IO Device	
F000	Actual configuration at API level.	

new device or module on the basis of the existing configuration records (see Table 6.15).

Structures of Profinet IO configuration records for desired/actual configuration

The fundamental structures of Profinet IO configuration records for desired/actual configuration are identical. However, the contents and sizes of the records vary depending on the configuration. The number of a configuration record corresponds to the system shown in Fig. 6.7.

Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Addressing level: 8h: Submodule Ch: Module Eh: AR Fh: API				0	0	0	0	Configuration: 00h: Actual configuration 01h: Desired configuration							

Fig. 6.7 Number structure of a configuration record

Exception: the configuration record F000h is used, contrary to the described structure, for scanning the actual configuration.

The meanings of the most important block elements of a configuration record are described in Chapter 6.2.

6.1.8 System State Lists (SSL)

The system state list (SSL) describes the current state of the automation system. It provides an overview of:

- The configuration
- The current parameter settings
- The current states and
- Sequences in the CPU and the associated modules.

An SSL sublist is a virtual list based on the SSL which is only compiled on request. The data of an SSL sublist can only be read. This is either carried out implicitly us-

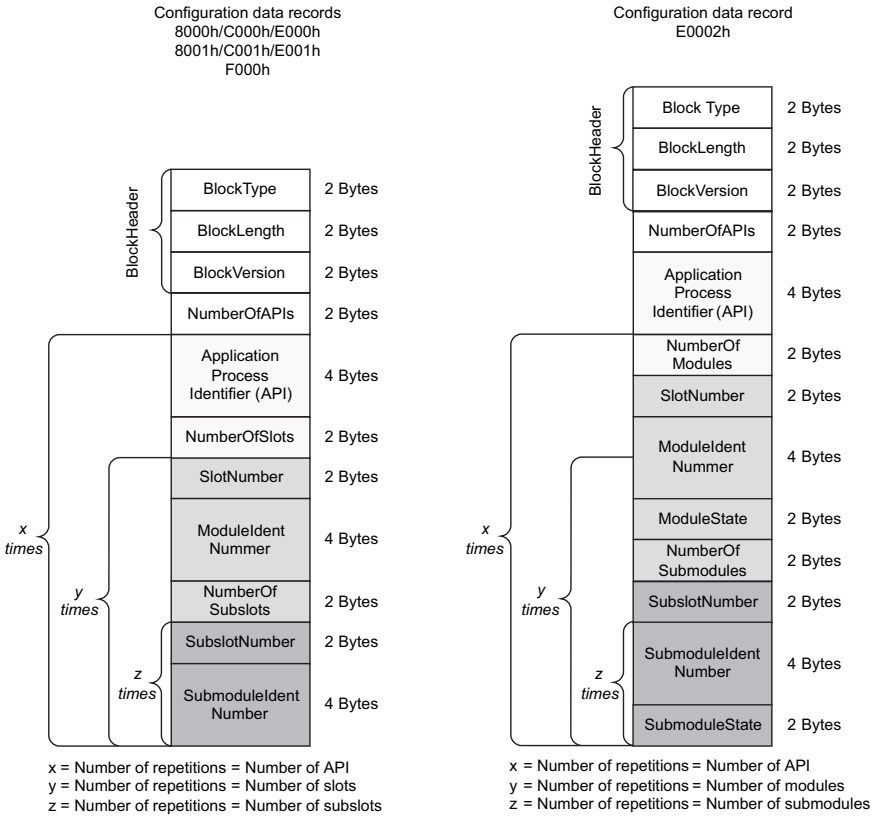


Fig. 6.8 Structure of configuration records of BlockVersion 0101

ing Step 7 menu commands or in the user program by calling the system function SFC 51 “RDSYSST” (ReaD SYStem Status). SSLs contain information on:

- System data, i.e. the fixed and parameterizable characteristic data of a CPU. These include the CPU configuration as well as the status of the priority classes and communication.
- Diagnostics status data in the CPU, i.e. the description of the current status of all components monitored by the system diagnostics.
- Diagnostics data and modules, i.e. the diagnostics data of all modules with diagnostics capability which are assigned to a CPU. These data are saved on the respective modules themselves.
- Diagnostics buffer where all diagnostics events are saved in the chronological sequence of their occurrence.

The possible sublist extracts have a fixed definition and are also identified by a number. The number of the sublist extract and its meaning depend on the requested sublist (see Tables 6.16 and 6.18).

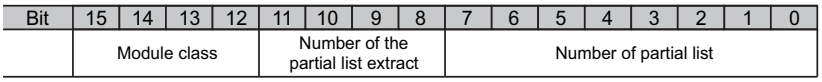


Fig. 6.9 Structure of SSL ID

The high-order four bits of the SSL ID correspond to the module class (Fig. 6.9). The type of module is specified here from which the sublist or the sublist extract is to be read (Table 6.16).

Table 6.17 provides a summary of important SSL IDs when using Profinet IO.

Table 6.16 Assignment of module class and type

Module class (SSL ID bits 15-12)	Module type
0000	CPU
0100	IM
0101	Analog module
1100	CP
1111	Digital module

Table 6.17 Important SSL IDs with Profinet IO

SSL ID (W#16#...)	Contents
0037	Details of all Ethernet interfaces.
0137	Details of one Ethernet interface.
0F37	Header information only.
0696	Module status information of all submodules of a specified module. Not possible for submodule 0 (= module).
0794	Faulty/maintenance status of Profinet IO stations or of the central racks.

Table 6.18 Important SSL IDs with Profinet IO and Profibus DP

SSL ID (W#16#...)	Contents
0591	Module status information for the interfaces of a module.
0A91	Status information of all Profibus DP subsystems and DP master systems as well as of Profinet IO systems (only S7-300 without CPU 318-2 DP).
0C91	Module status information of a module in the central rack or on an integrated Profibus/Profinet interface module via the logical base address of the module.
4C91	Module status information of a module on an external Profibus or Profinet interface module via the logical base address of the module.
0D91	Module status information of all modules in the specified rack/in the specified distributed station.
0E91	Module status information of all configured modules (central rack/integrated Profibus/Profinet interface module).
0094	Desired status of the central configuration or of distributed stations connected via an integrated Profibus/Profinet interface module.
0294	Actual status of the central configuration or of distributed stations connected via an integrated Profibus/Profinet interface module.

Table 6.18 Important SSL IDs with Profinet IO and Profibus DP *(continued)*

SSL ID (W#16#...)	Contents
0694	Status of the expansion units of the central configuration or of distributed stations connected via an integrated Profibus/Profinet interface module.
0F94	Header information only.
0195	Enhanced information via a DP master system/Profinet IO system.
0F95	Header information only.
0C96	Module status information of a central module/submodule or on a Profibus/Profinet interface module via the logical base address.

Table 6.19 SSL ID which cannot be used with Profinet IO but which can be replaced

SSL ID (W#16#...)	Contents	Can be replaced by
xy92	Rack/station status information on the desired/actual configuration of racks with central configuration and stations of a DP master system.	W#16#0x94

6.2 Coding of Profinet IO Diagnostics Records and Configuration Records

The blocks within the Profinet IO diagnostics records and configuration records are presented below. In order to guarantee unambiguity in the identification of the individual parameters, the respective name has been applied from the "Application Layer protocol for decentralized periphery and distributed automation, Specification for PROFINET, V2.1".

A record commences with a BlockHeader containing general information.

6.2.1 BlockHeader

The BlockHeader comprises the block elements BlockType, BlockLength and BlockVersion (see Table 6.20).

Table 6.20 BlockHeader

Byte	Bedeutung
1, 0	Important values: 0001h: Alarm transport channel 1 (AlarmNotification High) 0002h: Alarm transport channel 2 (AlarmNotification Low) 0010h: Diagnostics data (DiagnosisData) 0012h: Data of the reference configuration (ExpectedIdentificationDataBlock) 0013h: Data of the actual configuration (RealIdentificationData) 8104h: Data for comparison between the reference and actual configurations (ModuleDiffBlock)
3, 2	BlockLength: Total length of the record in bytes without BlockType and BlockLength
4	Version High (BlockVersionHigh)
5	Version Low (BlockVersionLow)

6.2.2 UserStructureIdentifier (USI)

The block element UserStructureIdentifier describes the type of diagnostics data of a record (Table 6.21).

Table 6.21 UserStructureIdentifier (USI)

Value (W#16#...)	Meaning
0000-7FFF	Manufacturer-specific diagnostics (ManufacturerSpecific)
8000	Channel diagnostics (ChannelDiagnosis)
8001	Multiple manufacturer-specific diagnostics (ManufacturerSpecificMultiple)
8002	Extended channel diagnostics (ExtChannelDiagnosis)
8003	Qualified channel diagnostics (QualifiedChannelDiagnosis)
8004-80FF	Reserved
8100	Maintenance request or requirement (Maintenance)
8101-81FF	Reserved
8200	Upload and save (Upload&Storage)
8201-8FFF	Reserved
9000-9FFF	Reserved for profile
A000-FFFF	Reserved

6.2.3 ApplicationProcessIdentifier (API)

The block element ApplicationProcessIdentifier describes the application process from which the data of the record originate, or for which they are intended. The default value is 0. Valuesþ>þ0 are reserved for Profinet IO profiles. The API is defined by PROFIBUS International.

6.2.4 SlotNumber

The block element SlotNumber contains the slot number (Table 6.22).

Table 6.22 SlotNumber

Value (W#16#...)	Meaning
0000-7FFF	Slot number
8000-8FFF	Reserved

6.2.5 SubslotNumber

The block element SubslotNumber contains the subslot number (Table 6.23).

Table 6.23 SubslotNumber

Value (W#16#...)	Meaning
0000	Identifies the module itself, and does not address a submodule
0001-7FFF	Subslot number
8000-FFFF	Reserved

6.2.6 ChannelNumber

The block element ChannelNumber contains the channel number (Table 6.24).

Table 6.24 ChannelNumber

Value (W#16#...)	Meaning
0000-7FFF	Vendor-specific
8000	Submodule
8000-FFFF	Reserved

6.2.7 ChannelProperties

The block element ChannelProperties describes the properties of a channel, and is coded in bits (Table 6.25).

Table 6.25 ChannelProperties

Bit	Meaning
7-0	Type: 0: With ChannelNumber = 8000h 1: 1 bit 2: 2 bit 3: 4 bit 4: 8 bit 5: 16 bit 6: 32 bit 7: 64 bit 8-255: Reserved
8	Accumulative channel fault: 0: No accumulative signal 1: Accumulative signal for several channels
10, 9	Maintenance: 0: Diagnostics 1: Maintenance request 2: Maintenance requirement 3: Graded diagnostics
12, 11	Specifier: 0: Reserved 1: UP diagnostics 2: DOWN diagnostics 3: DOWN diagnostics, further diagnostics messages are pending
15-13	Direction: 0: Manufacturer-specific 1: Input 2: Output 3: Input/Output 4-7: Reserved

6.2.8 ChannelErrorType

The block element ChannelErrorType describes the type of channel error (Table 6.26).

Table 6.26 ChannelErrorType

Value (W#16#...)	Meaning
0000	Unknown fault
0001	Short-circuit
0002	Undervoltage
0003	Overvoltage
0004	Overload
0005	Excess temperature
0006	Open-circuit
0007	Upper limit violated
0008	Lower limit violated
0009	Fault
000A-000F	Unknown fault
0010h	Incorrect parameterization
0011	Fault in power supply
0012	Fuse blown/tripped
0013	Manufacturer-specific
0014	Ground fault
0015	Reference point no longer present
0016	Scanning fault
0017	Threshold value exceeded/fallen below
0018	Output switched off
0019	Safety-relevant fault
001A	External fault
001B-001F	Vendor-specific
0020-001F	Reserved for standard profiles (PROFIsafe, etc.)
0100-7FFF	Vendor-specific
8000	No data transmission possible
8001	Incorrect neighborhood
8002	Loss of redundancy
8003	Loss of synchronization on bus
8004	Loss of clock synchronization at device end
8005	Internode connection fault
8006	Unknown fault
8007	Fiber-optic fault: Optical transmission not possible
8008	Fault in network component: Problems with network function
8009	Fault in timebase: Timer does not exist, or problems with accuracy of timebase
800A-8FFF	Unknown fault
9000-9FFF	Reserved for technological profiles (PROFIdrive etc.)
A000-FFFF	Unknown fault

6.2.9 ExtChannelErrorType

Supplementary to the block element ChannelErrorType, the block element ExtChannelErrorType contains a detailed description of the fault. The value of ChannelErrorType defines the meaning of ExtChannelErrorType. A number of important values are listed in the following Tables 6.27 to 6.35. The basic meaning is described in Table 6.27.

Table 6.27 ExtChannelErrorType

Value (W#16#...)	Meaning
0000	Reserved
0001-7FFF	Manufacturer-specific
8000-8FFF	Dependent on the value of ChannelErrorType, corresponding to Profinet Application Layer Service Definition & Application Layer Protocol Specification or IEC 61158.
9000–9FFF	Reserved for profiles
A000–FFFF	Reserved

A number of important values are listed in the following Tables 6.28 to 6.35.

Table 6.28 Meaning of ExtChannelErrorType with ChannelErrorType 8000h (no data transmission possible)

Value (W#16#...)	Meaning
8000	Fault in port status:E.g. cable not connected
8001	Fault due to incorrect interface setting:Full duplex/half duplex
8002	Fault due to runtime delay:Configured cable length not equal to actual cable length
8003–8FFF	Reserved

Table 6.29 Meaning of ExtChannelErrorType with ChannelErrorType 8001h (incorrect neighborhood)

Value (W#16#...)	Meaning
8000	Incorrect neighboring device
8001	Incorrect neighboring port
8002	Neighbor does not support real-time class 3, or is not configured
8003	Fault due to incorrect interface setting:Full duplex/half duplex
8004	Incorrect or missing media redundancy configuration
8005	No neighboring device present
8006	Neighbor does not support bumpless media redundancy
8007	Fault due to delay on the transmission path to the neighbor
8008–8FFF	Reserved

Table 6.30 Meaning of ExtChannelErrorType with ChannelErrorType 8002h (loss of redundancy)

Value (W#16#...)	Meaning
8000	Media redundancy signals error
8001	Ring open:No media redundancy available
8002	Ring open:No bumpless media redundancy available
8003	Several media redundancy managers in the ring
8004–8FFF	Reserved

Table 6.31 Meaning of ExtChannelErrorType with ChannelErrorType 8003h (loss of synchronization on bus) and 8009h (loss of timebase)

Value (W#16#...)	Meaning
8000	No synchronization maintained
8001	Real-time class 3 – incorrect synchronization configuration
8002	Real-time class 3 – incorrect configuration
8003	Jitter outside limit range
8004–8FFF	Reserved

Table 6.32 Meaning of ExtChannelErrorType with ChannelErrorType 8004h (loss of clock synchronization at device end)

Value (W#16#...)	Meaning
8000	Transfer point of outputs missed
8001	Transfer point of inputs missed
8002-8FFF	Reserved

Table 6.33 Meaning of ExtChannelErrorType with ChannelErrorType 8005h (internode connection fault)

Value (W#16#...)	Meaning
8000	Data receiver with internode communication: No transmitter or incorrect transmitter
8001	Data receiver with internode communication: Unknown transmitter
8002-8FFF	Reserved

Table 6.34 Meaning of ExtChannelErrorType with ChannelErrorType 8007h (fiber-optic fault)

Value (W#16#...)	Meaning
8000	Defined receiver level fallen below
8001-8FFF	Reserved

Table 6.35 Meaning of ExtChannelErrorType with ChannelErrorType 8008h (fault in network component)

Value (W#16#...)	Meaning
8000	Network overload:Frames are rejected
8001-8FFF	Reserved

6.2.10 ExtChannelErrorAddInfo

The block element ExtChannelErrorAddInfo contains further supplementary information for the block element ChannelErrorType (Table 6.36).

Table 6.36 ExtChannelErrorAddInfo

Value (W#16#...)	Meaning
00000000	No further information.
000000001-FFFFFFFF	Dependent on the values of ChannelErrorType and ExtChannelErrorType, corresponding to Profinet Application Layer Service Definition & Application Layer Protocol Specification or IEC 61158.

6.2.11 ModuleIdentNumber

The block element ModuleIdentNumber contains the identification number of a module (Table 6.37).

Table 6.37 ModuleIdentNumber

Value (W#16#...)	Meaning
00000000	Reserved
000000001-FFFFFFFF	Manufacturer-specific

6.2.12 SubmoduleIdentNumber

The block element SubmoduleIdentNumber contains the identification number of a submodule (Table 6.38).

Table 6.38 SubmoduleIdentNumber

Value (W#16#...)	Meaning
000000000-FFFFFFFF	Manufacturer-specific

6.2.13 ModuleState

The block element ModuleState contains the module status (Table 6.39).

Table 6.39 ModuleState

Value (W#16#...)	Meaning
0000	Module is not inserted
0001	Incorrect module inserted
0002	Module is correct, but at least one submodule is interlocked, incorrect or missing
0003	Incorrect but compatible module is inserted. The I/O device is able to adapt itself to the module
0004–FFFF	Reserved

6.2.14 SubmoduleState

The block element SubmoduleState describes the submodule status and is coded in bits (Table 6.40).

Table 6.40 SubmoduleState

Bit	Meaning
2-0	Supplementary information (AddInfo): 0: No further information 1: Submodule not suitable for importing by IO Supervisor AR 2-7: Reserved
3	Graded diagnostics (QualifiedInfo): 0: No graded diagnostics available 1: Graded diagnostics is available for at least one channel of the submodule
4	Maintenance request (MaintenanceRequired): 0: No maintenance request present 1: Maintenance request present
5	Maintenance requirement (MaintenanceDemanded): 0: No maintenance requirement present 1: Maintenance requirement present
6	Diagnostics (DiagInfo): 0: No diagnostics message available 1: Diagnostics message present
10-7	AR information (ARInfo): 0: AR is the owner of the submodule 1: AR is the owner of the submodule, but the submodule is disabled 2: AR is not the owner of the submodule. The submodule is disabled by higher-level services 3: AR is not the owner of the submodule. The submodule is disabled by IO controller 4: AR is not the owner of the submodule. The submodule is disabled by IO Supervisor 5-15: Reserved

Table 6.40 SubmoduleState *(continued)*

Bit	Meaning
14-11	Identification information (IdentInfo): 0: OK 1: Replacement 2: Incorrect 3: Not a submodule 4-15: Reserved
15	Format indicator (FormatIndicator): 0: Reserved 1: SubmoduleState consists of SubmoduleState.IdentInfo, SubmoduleState.ARInfo and SubmoduleState.AddInfo.

6.3 Profinet IO User Program Interfaces

The user program handles the distributed I/O connected to a Simatic S7 system like a central I/O. This applies equally to Profibus DP and Profinet IO. Data exchange is handled using the process input and output images of a Simatic S7 CPU or by using direct I/O access commands from the user program. Exception: communication of certain Simatic Net CPs as IO controllers necessitates the application of special functions. The user program cycle of the CPU and the cycle of the I/O data exchange between IO controller and IO Devices are always independent of one another.

Data exchange with distributed I/O devices containing more complex functions and data structures is not possible using simple I/O access operations for consistency reasons. Special standard functions are available for this purpose.

Appropriate interfaces and functions are available for handling and evaluating process and diagnostics interrupts. In addition, Simatic S7 CPUs allow reparameterization or subsequent parameterization of distributed I/O devices from the user program.

This chapter describes the functions and interfaces of the user program of a Simatic S7 CPU which are relevant to the use of Profinet.

6.3.1 Organization Blocks with Profinet IO

When using Profinet IO, it is basically the case that all organization blocks can be used as previously. New features only exist for OB 83 (insert/remove module interrupt) and OB 86 (rack failure) with respect to the call response (see Table 6.41). It

Table 6.41 OB 83 and OB 86 with Profinet IO and Profibus DP

OB	Function	Profinet IO	Profibus DP
83	Insert/remove module interrupt	Possible with S7-300; new error information	Not possible with S7-300
86	Rack failure	New error information	Unchanged

is now possible to use the OB 83 with Simatic S7 CPU 31x-2PN/DP for evaluation of insert/remove module interrupts when using Profinet IO, and enhanced error information is available for both blocks.

Insert/Remove module interrupt (OB 83)

The operating system of a CPU calls the OB 83

- if a configured module has been removed or inserted, or
- following a change in the module parameters during operation, if loaded into the CPU when in the RUN status (CiR: Configuration in RUN).

The call of the OB 83 can be disabled and reenabled by calling SFC 39 “DIS_IRT” (DISable InterRupT), SFC 40 “EN_IRT” (ENable InterRupT), SFC 41 “DIS_AIRT” (DISable Alarm InterRupT) and SFC 42 “EN_AIRT” (ENable Alarm InterRupT).

Every removal or insertion of a configured module in the RUN, STOP and STARTUP statuses results in a insert/remove module interrupt. Hot swapping of power supply modules, CPUs, adapter casings and interface modules (IM) is not permissible.

A insert/remove module interrupt results in an entry in the diagnostics buffer and in the system status list of the associated CPU. In the RUN status, the OB 83 is started in addition. If this OB has not been programmed, the CPU converts to the STOP status.

With the CPUs of the Simatic S7-400 range and with Simatic S7 CPU 318, hot swapping is monitored in second-granular mode within the system. To allow the CPU to recognize hot swapping, a minimum period of two seconds must expire between removal and insertion of an S7-400 module. With other CPUs, this minimum period may be somewhat longer.

When inserting a module into a configured slot in the RUN status, the operating system checks whether the type of inserted module agrees with the configuration. The OB 83 is subsequently started. Parameterization is carried out if the actual module type agrees with that expected.

Hot swapping of central I/Os is not permissible with S7-300 CPUs. The following modules are exceptions:

- Simatic S7 CPUs 31x PN/DP only support insert/remove module interrupts with Profinet IO components.
- Simatic S7 CPU IM151-7 only supports insert/remove module interrupts with centralized I/O.

The local data of OB 83 are listed in Table 6.42.

Table 6.42 Local data of OBþ83

Variable	Data type	Description
OB83_EV_CLASS	BYTE	Event class and IDs: B#16#32: End reparameterization of module B#16#33: Start reparameterization of module B#16#38: Module inserted B#16#39: Module removed, or cannot be addressed, or end of reparameterization
OB83_FLT_ID	BYTE	Error code, possible values: B#16#51, B#16#54, B#16#55, B#16#56, B#16#58, B#16#61, B#16#63, B#16#64, B#16#65, B#16#66, B#16#67, B#16#68, B#16#84
OB83_PRIORITY	BYTE	Priority class, can be parameterized using Step 7
OB83_OB_NUMBR	BYTE	83
OB83_RESERVED_1	BYTE	ID for module or submodule/interface module.
OB83_MDL_ID	BYTE	Range. B#16#54: I/O area of inputs (PII) B#16#55: I/O area of outputs (PIQ)
OB83_MDL_ADDR	WORD	Central and Profibus DP: Logical base address of associated module, or the smallest logical module address used in the case of a hybrid module. If the logical input and output addresses of the hybrid module are the same, the logical base address is assigned the input ID. Profinet IO: Logical base address of module/submodule.
OB83_RACK_NUM	WORD	OB83_RESERVED_1=B#16#A0: Number of submodule or number of interface module (Low byte) OB83_RESERVED_1=B#16#A0: Central: Number of rack Distributed: Profibus DP: Number of DP station (Low byte) and of DP master system ID (High byte) Profinet IO: Physical address Bit 15: ID bit: 1 (Profinet IO) Bits 11-14: IO system ID Bit 0-10: Station number
OB83_MDL_TYPE	WORD	Central and Profibus DP: Type of associated module (X: not user-relevant): W#16#X5XX: Analog module W#16#X8XX: Function module W#16#XCXX: CP W#16#XFXX: Digital module· Profinet IO: W#16#8101: Inserted type of module is same as removed type. W#16#8102: Inserted type of module is not same as removed type.
OB83_DATE_TIME	DT	Date and time of request from OB 83

In the case of an OB 83 call, the variables OB83_EV_CLASS and OB83_FTL_ID contain the values listed in Table 6.43.

Table 6.43 Alarm events triggering OB 83

OB83_EV_CLASS	OB83_FLT_ID	Event
B#16#39	B#16#54	Profinet IO submodule removed.
B#16#38	B#16#54	Profinet IO submodule inserted, and corresponds to parameterized submodule.
B#16#38	B#16#55	Profinet IO submodule inserted, but does not correspond to parameterized submodule.
B#16#38	B#16#56	Profinet IO submodule inserted, but error in module parameterization.
B#16#38	B#16#58	Profinet IO submodule access error eliminated.
B#16#39	B#16#61	Module removed or cannot be addressed.OB83_MDL_TYPE: actual type of module
B#16#38	B#16#61	Module inserted, type OK.OB83_MDL_TYPE: actual type of module
B#16#38	B#16#63	Module inserted, but wrong type.OB83_MDL_TYPE: actual type of module
B#16#38	B#16#64	Module inserted, but faulty (module ID cannot be read). OB83_MDL_TYPE: correct type of module
B#16#38	B#16#65	Module inserted, but error in module parameterization.OB83_MDL_TYPE: actual type of module
B#16#39	B#16#66	Module cannot be addressed, load voltage fault.
B#16#38	B#16#66	Module can be addressed again, load voltage fault eliminated.
B#16#33	B#16#67	Start reparameterization of a module.
B#16#32	B#16#67	End reparameterization of a module.
B#16#39	B#16#68	Reparameterization of a module terminated with error.
B#16#38	B#16#84	Interface module inserted.
B#16#39	B#16#84	Interface module removed.
B#16#39	B#16#54	Profinet IO submodule removed.

Rack failure (OB 86)

A failure or the return of a central Simatic S7-400 expansion unit, of a DP master system or of stations with distributed I/O is detected by the operating system of a Simatic S7 CPU and signaled by OB 86. If the OB 86 has not been programmed, the CPU enters the stop status when the event occurs. The local data of OB 86 are listed in Table 6.44.

Table 6.44 Local data of OBþ86

Variable	Data type	Description
OB86_EV_CLASS	BYTE	Event class and IDs B#16#38: DOWN event B#16#39: UP event
OB86_FLT_ID	BYTE	Error code, possible values: B#16#C1, B#16#C2, B#16#C3, B#16#C4, B#16#C5, B#16#C6, B#16#C7, B#16#C8, B#16#CA, B#16#CB, B#16#CC, B#16#CD, B#16#CE
OB86_PRIORITY	BYTE	Priority class, can be parameterized using Stepþ7
OB86_OB_NUMBR	BYTE	86

Table 6.44 Local data of OBþ86 *(continued)*

Variable	Data type	Description
OB86_RESERVED_1	BYTE	Reserved
OB86_RESERVED_2	BYTE	Reserved
OB86_MDL_ADDR	WORD	Depends on error code
OB86_RACK_FLTD	ARRAY [0..31] OF BOOL	Depends on error code
OB83_DATE_TIME	DT	Date and time at which the OB was requested.

In the event of an OB 86 call, the variables OB86_EV_CLASS and OB83_FTL_ID contain the values listed in Table 6.45.

Table 6.45 Alarm events triggering OB 86

OB86_EV_CLASS	OB86_FLT_ID	Event
B#16#39	B#16#C1	Expansion unit: Failure: OB86_MDL_ADDR: Logical base address of IM OB86_Z23: Those expansion units are signaled as failed which caused OB 86 to be called. EUs which had already failed earlier are no longer displayed. Of bits 1-21, those associated with the EU are set. Bit 0: 0 Bits 1-21: EU 1-21 Bits 22-29: 0 Bit 30: Failure of at least one EU in the Simatic S5 range. Bit 31: 0
B#16#38	B#16#C1	Expansion unit: Return: OB86_MDL_ADDR: Logical base address of IM OB86_Z23: The EUs which have returned are signaled. Of bits 1-21, those associated with the EU are set. Bit 0: 0 Bits 1-21: EU 1-21 Bits 22-29: 0 Bit 30: Failure of at least one EU in the Simatic S5 range. Bit 31: 0
B#16#38	B#16#C2	Expansion units: Return with deviation between expected and actual configurations: OB86_MDL_ADDR: Logical base address of IM OB86_Z23: Of bits 1-21, those associated with the EU are set. In the expansion unit: – Modules exist with an incorrect ID. – Configured modules are missing. – At least one module is faulty. Bit 0: 0 Bits 1-21: EU 1-21 Bits 22-29: 0 Bit 30: Failure of at least one EU in the Simatic S5 range. Bit 31: 0

Table 6.45 Alarm events triggering OB 86 *(continued)*

OB86_EV_CLASS	OB86_FLT_ID	Event
B#16#39	B#16#C3	Profibus DP: Failure of a DP master system (only up event): OB86_MDL_ADDR: Logical base address of DP master OB86_Z23: Bits 0-7: Reserved Bits 8-15: DP master system ID Bits 16-31: Reserved
B#16#39 B#16#38	B#16#C4	Profibus DP: Failure or return of a DP station: OB86_MDL_ADDR: Logical base address of DP master OB86_Z23: Bits 0-7: No. of DP station Bits 8-15: DP master system ID Bits 16-30: Logical base address with an S7 slave or diagnostics address with a DP standard slave. Bit 31: I/O ID
B#16#39 B#16#38	B#16#C5	Profibus DP: Fault or return of a DP station: OB86_MDL_ADDR: Logical base address of DP master OB86_Z23: Bits 0-7: No. of DP station Bits 8-15: DP master system ID Bits 16-30: Logical base address with an S7 slave or diagnostics address with a DP standard slave. Bit 31: I/O ID
B#16#38	B#16#C6	Expansion unit: Return, but error in module parameterization: OB86_MDL_ADDR: Logical base address of IM OB86_Z23: Of bits 1-21, those associated with the EU are set. In the expansion unit: – Modules exist with an incorrect ID. – Modules exist with missing or incorrect parameters. Bit 0: 0 Bits 1-21: EU 1-21 Bits 22-30: Reserved Bit 31: 0
B#16#38	B#16#C7	Profibus DP: Return of a DP station, but error in module parameterization: OB86_MDL_ADDR: Logical base address of DP master OB86_Z23: Bits 0-7: No. of DP station Bits 8-15: DP master system ID Bits 16-30: Logical base address of DP slave Bit 31: I/O ID
B#16#38	B#16#C8	Profibus DP: Return of a DP station, but deviation between expected and actual configurations: OB86_MDL_ADDR: Logical base address of DP master OB86_Z23: Bits 0-7: No. of DP station Bits 8-15: DP master system ID Bits 16-30: Logical base address of DP slave Bit 31: I/O ID

Table 6.45 Alarm events triggering OB 86 *(continued)*

OB86_EV_CLASS	OB86_FLT_ID	Event
B#16#39	B#16#CA	Profinet IO: System failure: OB86_MDL_ADDR: Logical base address of IO controller OB86_Z23: Bits 0-10: 0 Bits 11-14: IO system ID Bit 15: 1 Bits 16-31: 0
B#16#39 B#16#38	B#16#CB	Profinet IO: Station failure or return: OB86_RESERVED_1: B#16#C4: No other station faulty B#16#CF: Further stations failed/faulty OB86_MDL_ADDR: Logical base address of IO controller OB86_Z23: Bits 0-10: Station number Bits 11-14: IO system ID Bit 15: 1 Bits 16-30: Logical base address of station Bit 31: I/O ID
B#16#39 B#16#38	B#16#CC	Profinet IO: Station failure or fault eliminated: OB86_RESERVED_1: B#16#C4: No other station faulty B#16#CF: Further stations failed/faulty OB86_MDL_ADDR: Logical base address of IO controller OB86_Z23: Bits 0-10: Station number Bits 11-14: IO system ID Bit 15: 1 Bits 16-30: Logical base address of station Bit 31: I/O ID
B#16#39	B#16#CD	Profinet IO: Return of station, but deviation between expected and actual configurations: OB86_MDL_ADDR: Logical base address of IO controller OB86_Z23: Bits 0-10: Station number Bits 11-14: IO system ID Bit 15: 1 Bits 16-30: Logical base address of station Bit 31: I/O ID
B#16#39	B#16#CE	Profinet IO: Station return, fault in module parameterization: OB86_MDL_ADDR: Logical base address of IO controller OB86_Z23: Bits 0-10: Station number Bits 11-14: IO system ID Bit 15: 1 Bits 16-30: Logical base address of station Bit 31: I/O ID

6.3.2 Standard Functions for Communication with Profinet IO

The term “Standard functions” in this context refers to the functions for communication on Profibus DP and Profinet IO which are compatible with IEC 61131-3 and defined in the guidelines:

- “Profibus Communication and Proxy Function Blocks according to IEC 61131-3” (Table 6.46) and
- “Communication Function Blocks on Profibus and Profinet IO” (Table 6.48 and Table 6.49).

Table 6.46 Standard functions in accordance with guideline “Profibus Communication and Proxy Function Blocks according to IEC 61131-3”

Function	Simatic S7 block	Description
WRREC	SFB 53 “WRREC”	Write Record
RDREC	SFB 52 “RDREC”	Read Record
RALRM	SFB 54 “RALRM”	Receive Alarms

The guideline “Communication Function Blocks on Profibus and Profinet IO” differentiates between functions for use in the application program of a:

- Host controller (DP master/IO controller),
- Supervisor (DP master class 2/IO Supervisor) or
- Field device (DP slaves/IO Devices).

In Simatic S7 systems part of these standard functions are realized as function blocks.

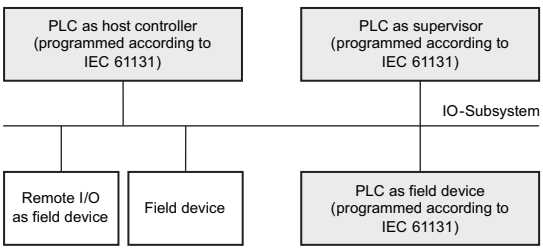


Fig. 6.10 Various roles of a PLC on Profinet IO

This chapter provides an overview of the above-mentioned functions for application in the user program of a Simatic S7 CPU (Tables 6.47 to 6.49).

Table 6.47 Standard functions for host controller in accordance with guideline "Communication Function Blocks on Profibus and Profinet IO

Function	Simatic S7 block	Description
GETIO	FB 20 "GETIO"	Get IO data object: Read all inputs of a DP standard slave/IO Device.
SETIO	FB 21 "SETIO"	Set IO data object: Write all outputs of a DP standard slave/IO Device.
GETIO_PART	FB 22 "GETIO_PART"	Get a part of IO data object: Read part of the inputs of a DP standard slave/IO Device.
SETIO_PART	FB 23 "SETIO_PART"	Set IO data object related to a part of a slot: Write part of the outputs of a DP standard slave/IO Device.
ICTRL	–	Interlocked control: Interlocked writing of a record.

Table 6.48 Standard functions for supervisor in accordance with guideline "Communication Function Blocks on Profibus and Profinet IO"

Function	Simatic S7 block	Description
RDIN	–	Read input data.
RDOUT	–	Read output data.

Table 6.49 Standard functions for field devices in accordance with guideline "Communication Function Blocks on Profibus and Profinet IO"

Function	Simatic S7 block	Description
RCVCO	–	Receive cyclic output data.
SBCCI	–	Subscribe cyclic input data.
PRVCI	–	Provide cyclic input data.
RCVREC	–	Receive process record.
PRVREC	–	Provide process record.
SALRM	–	Send alarm. Implemented on Profibus DP by SFB 75 "SALRM".

Read all inputs of a DP standard slave/IO Device using FB 20 “GETIO”

The FB 20 “GETIO” consistently reads out all inputs of a DP standard slave/IO Device, and writes them into the destination range defined in the parameter INPUTS. The system function SFC 14 “DPRD_DAT” is implicitly called for this purpose (see Table 6.50).

Table 6.50 Parameters of FBþ20 “GETIO”

Parameter	Declaration	Data type	Memory area	Description
ID	INPUT	DWORD	I, Q, F, D, L, constants	Low word: Logical address of DP slave/IO Device component. High word: Irrelevant
STATUS	OUTPUT	DWORD	I, Q, F, D, L	The parameter contains the return value RET_VAL of the SFC 14 “DPRD_DAT” in the form DW#16#40xxxx00.
LEN	OUTPUT	INT	I, Q, F, D, L	Number of read data in bytes.
INPUTS	IN_OUT	ANY VARTYPE: BYTE	I, Q, F, D	Destination range of read data.

Write all outputs of a DP standard slave/IO Device using FB 21 “SETIO”

The FB 21 “SETIO” consistently transmits the data from the source range defined in the parameter OUTPUTS to the addressed DP standard slave/IO Device. The system function SFC 15 “DPWR_DAT” is implicitly called for this purpose. If the output address range of the DP slave/IO Device is in the process image of the CPU, this is also updated (see Table 6.66).

Table 6.51 Parameters of FBþ21 “SETIO”

Parameter	Declaration	Data type	Memory area	Description
ID	INPUT	DWORD	I, Q, F, D, L, constants	Low word: Logical address of DP slave/IO Device component. High word: Irrelevant
LEN	INPUT	INT	I, Q, F, D, L, constants	Irrelevant
STATUS	OUTPUT	DWORD	I, Q, F, D, L	The parameter contains the return value RET_VAL of the SFC 15 “DPWR_DAT” in the form DW#16#40xxxx00.
OUTPUTS	IN_OUT	ANY VARTYPE: BYTE	I, Q, F, D	Destination range of data to be transmitted.

Read part of the inputs of a DP standard slave/IO Device using FB 22 “GETIO_PART”

The FB 22 “GETIO_PART” consistently reads out part of the process input image belonging to a DP standard slave/IO Device and writes it into the destination range defined in the parameter INPUTS. The system function SFC 81 “UBLKMOV” is implicitly called for this purpose (see Tables 6.52 and 6.53).

FB 22 “GETIO_PART” does not check whether the limits between various Profibus DP/Profinet IO components are violated in the process image of the CPU during the read procedure. Observation of these limits must be guaranteed by the correct supply of parameters OFFSET and LEN. Reading beyond limits may be possible on a vendor-specific basis, but is not guaranteed.

Table 6.52 Parameters of FBþ22 “GETIO_PART”

Parameter	Declaration	Data type	Memory area	Description
ID	INPUT	DWORD	I, Q, F, D, L, constants	Low word: Logical address of DP slave/IO Device component. High word: Irrelevant
OFFET	INPUT	INT	I, Q, F, D, L, constants	Number of the first byte to be read in the process image of the component.
LEN	INPUT	INT	I, Q, F, D, L, constants	Number of data to be read in bytes.
STATUS	OUTPUT	DWORD	I, Q, F, D, L	The parameter contains the return value RET_VAL of the SFC 81 “UBLKMOV” in the form DW#16#40xxxx00.
ERROR	OUTPUT	BOOL	I, Q, F, D, L	Fault display. FALSE: No fault TRUE: Fault
INPUTS	IN_OUT	ANY	I, Q, F, D	Destination range of the read data. Destination range < LEN: As many bytes are transmitted as INPUTS can accommodate. Destination range > LEN: The first LEN bytes of the destination range are written. ERROR is in both cases = FALSE.

Table 6.53 Status values of FBþ22 “GETIO_PART”

Status code (DW#16#...)	Description
40000000	No fault has occurred.
40809100	The source area is in a data block not relevant to execution.
408xyy00	General fault information corresponding to the general error code of parameter RET_VAL.

Write part of the outputs of a DP standard slave/IO Device using FB 23 “SETIO_PART”

The FB 23 “SETIO_PART” consistently transmits the data from the source area defined in the parameter OUTPUTS to a part of the process output image belonging to a DP standard slave/IO Device. The system function SFC 81 “UBLKMOV” is implicitly called for this purpose (see Tables 6.54 and 6.55).

FB 23 “SETIO_PART” does not check whether the limits between various Profibus DP/Profinet IO components are violated in the process image of the CPU during the write procedure. The user must ensure observation of these limits by correctly supplying the parameters OFFSET and LEN. Writing beyond limits may be possible on a vendor-specific basis, but is not guaranteed.

Table 6.54 Parameters of FBþ23 “SETIO_PART”

Parameter	Declaration	Data type	Memory area	Description
ID	INPUT	DWORD	I, Q, F, D, L, constants	Low word: Logical address of DP slave/IO Device component. High word: Irrelevant
OFFET	INPUT	INT	I, Q, F, D, L, constants	Number of the first byte to be written in the process image of the component.
LEN	INPUT	INT	I, Q, F, D, L, constants	Number of data to be written in bytes.
STATUS	OUTPUT	DWORD	I, Q, F, D, L	The parameter contains the return value RET_VAL of the SFC 81 “UBLKMOV” in the form DW#16#40xxxx00.
ERROR	OUTPUT	BOOL	I, Q, F, D, L	Fault display. FALSE: Fault TRUE: Fault
OUTPUTS	IN_OUT	ANY	I, Q, F, D	Source range of the data to be written. Source range < LEN: As many bytes are transmitted as OUTPUTS contains. Source range > LEN: The first LEN bytes are transmitted from OUTPUTS. ERROR is in both cases = FALSE.

Table 6.55 Status values of FBþ23 “SETIO_PART”

Status code (DW#16#...)	Description
40000000	No fault has occurred.
40809100	The source area is in a data block not relevant to execution.
408xyy00	General fault information corresponding to the general error code of parameter RET_-VAL.

Read record using SFB 52 “RDREC”

The record with the number INDEX is read by the component (module) addressed by ID of a Profibus DP slave or a Profinet IO Device using the asynchronous SFB 52 “RDREC” (ReaD RECord). The MLEN parameter specifies how many bytes of the record are to be read.

SFB 52 “RDREC” is executed asynchronously, i.e. processing may be carried out in several user program cycles. The status of the request processing is indicated by the BUSY output parameter and bytes 2 and 3 of the STATUS output parameter. Bytes 2 and 3 of STATUS correspond to the RET_VAL output parameter of the asynchronous SFC.

The parameters of the SFB 52 “RDREC” are listed in Table 6.56, the specific return values correspond to those of the SFB 54 “RALM”.

Table 6.56 Parameters of SFB 52 “RDREC”

Parameter	Declaration	Data type	Memory area	Description
REQ	INPUT	BOOL	I, Q, F, D, L, constants	TRUE: Triggering of read request
ID	INPUT	DWORD	I, Q, F, D, L, constants	Device (module). Bit 15: FALSE: Input/hybrid module TRUE: Output module With a hybrid module, the smaller of the two addresses must be specified.
INDEX	INPUT	INT	I, Q, F, D, L, constants	Record number. Profinet IO: Interpretation as unsigned integer (WORD).
MLEN	INPUT	INT	I, Q, F, D, L, constants	Max. length of record to be read in bytes. Profinet IO: Interpretation as unsigned integer (WORD).
VALID	OUTPUT	BOOL	I, Q, F, D, L	TRUE: Record has been read and is valid.
BUSY	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Reading finished TRUE: Reading in progress
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: No error has occurred TRUE: Error during reading
STATUS	OUTPUT	DWORD	I, Q, F, D, L	Call ID (bytes 2 and 3) or error code.
LEN	OUTPUT	INT	I, Q, F, D, L	Length of read record information in bytes. Profinet IO: Interpretation as unsigned integer (WORD).
RECORD	IN_OUT	ANY	I, Q, F, D, L	Destination range for read record.

Write record using SFB 53 “WRREC”

The record with the number INDEX is transferred by the component (module) addressed by ID of a Profibus DP slave or a Profinet IO Device using the asynchronous SFB 53 “WRREC” (WRite RECord). The LEN parameter contains the length of the record to be transferred in bytes.

Table 6.57 Parameters of SFB 53 "WRREC"

Parameter	Declaration	Data type	Memory area	Description
REQ	INPUT	BOOL	I, Q, F, D, L, constants	TRUE: Triggering of write request
ID	INPUT	DWORD	I, Q, F, D, L, constants	Logical address of DP slave/IO Device (module). Bit 15: FALSE: Input/hybrid module TRUE: Output module With a hybrid module, the smaller of the two addresses must be specified.
INDEX	INPUT	INT	I, Q, F, D, L, constants	Record number. With Profinet IO: interpretation as unsigned integer (word).
LEN	INPUT	INT	I, Q, F, D, L, constants	Max. length of record to be transferred in bytes. With Profinet IO: interpretation as unsigned integer (word).
DONE	OUTPUT	BOOL	I, Q, F, D, L	The record has been transferred.
BUSY	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Writing finished TRUE: Writing in progress
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: No error has occurred TRUE: Error during writing
STATUS	OUTPUT	DWORD	I, Q, F, D, L	Call ID (bytes 2 and 3) or error code.
RECORD	IN_OUT	ANY	I, Q, F, D, L	Source range for record to be written.

SFB 53 "WRREC" is executed asynchronously, i.e. processing may be carried out in several user program cycles. The status of the request processing is indicated by the BUSY output parameter and bytes 2 and 3 of the STATUS output parameter. Bytes 2 and 3 of STATUS correspond to the RET_VAL output parameter of the asynchronous SFC.

The parameters of the SFB 53 "WRREC" are listed in Table 6.57, the specific return values correspond to those of the SFB 54 "RALM".

Evaluate alarm using SFB 54 "RALRM"

SFB "RALRM" receives an alarm including all associated information from a central I/O module or a component (module) of a DP slave or IO Device, and makes this information available in its output parameters.

SFB 54 "RALRM" must only be called within that alarm OB which the CPU's operating system has started as a result of the alarm from the I/O to be investigated. The output parameters contain both the start information of the called OB as well as information from the alarm source.

If SFB 54 "RALRM" is called in an OB whose start event is not an alarm from the I/O, the SFB provides correspondingly less information at its outputs.

When calling SFB 54 “RALRM” in various OBs, different instance DBs must be used. If the evaluation of data resulting from an SFB 54 call is carried out outside the associated alarm OB, it is recommendable to use a separate instance DB per OB start event. If the destination range provided by TINFO or AINFO has been selected too small, the SFB 54 cannot enter the complete alarm information.

Calling of SFB 54 “RALRM” can be carried out in three different modes (Table 6.58). The respective mode is defined by the input parameter MODE (Table 6.59).

Table 6.58 Modes of SFBþ54 “RALRM”

MODE	Description
0	Display of component triggering the alarm in the output parameter ID.
1	Setting of output parameter NEW to TRUE.
2	Checking of whether the component specified in the input parameter F_ID triggered the alarm. No: NEW=FALSE Yes: NEW=TRUE and writing of all other output parameters

Table 6.59 Parameters of SFB 54 “RALRM”

Parameter	Declaration	Data type	Memory area	Description
MODE	INPUT	INT	I, Q, F, D, L, constants	Mode
F_ID	INPUT	DWORD	I, Q, F, D, L, constants	Logical start address of the component (module) from which alarms are to be received. Bit 15: FALSE: Input/hybrid module TRUE: Output module With a hybrid module, the smaller of the two addresses must be specified.
MLEN	INPUT	INT	I, Q, F, D, L, constants	Max. length of alarm information to be received in bytes.
NEW	OUTPUT	BOOL	I, Q, F, D, L	TRUE: A new alarm has been received.
STATUS	OUTPUT	DWORD	I, Q, F, D, L	Error code of SFB, DP master or IO controller.
ID	OUTPUT	DWORD	I, Q, F, D, L	Logical start address of the component (module) from which alarms are to be received. Bit 15: FALSE: Input/hybrid module TRUE: Output module
LEN	OUTPUT	INT	I, Q, F, D, L	Length of received alarm information in bytes.
TINFO	IN_OUT	ANY	I, Q, F, D, L	Task information Destination range for OB start and administration information.
AINFO	IN_OUT	ANY	I, Q, F, D, L	Alarm information Destination range for header and supplementary alarm information. The length of AINFO should be at least MLEN bytes.

Table 6.60
Contents of TINFO and AINFO parameters when calling SFB 54 “RALRM” in different OBs

OB	TINFO		AINFO	
	OB start information	Administration info.	Header info.	Supplementary alarm information
OB 4x (hardware interrupt)	yes	yes	yes	Central: no Distributed: as provided by DP slave/IO Device.
OB55 Status interrupt	yes	yes	yes	yes
OB 56 Update interrupt	yes	yes	yes	yes
OB 57 Manufacturer-specific interrupt	yes	yes	yes	yes
OB 70 Redundancy interrupt	yes	yes	no	no
OB 82 Diagnostic interrupt	yes	yes	yes	Central: record 1 Distributed: as provided by DP slave/IO Device.
OB 83 Insert/remove module interrupt	yes	yes	yes	Central: no Distributed: as provided by DP slave/IO Device
Controlled (by IO Supervisor)	yes	yes	yes	Only Profinet IO
Enabled (by IO Supervisor)	yes	yes	yes	Only Profinet IO
The configured module is not inserted	yes	yes	yes	Only Profinet IO
OB 88 Rack/station interrupt	yes	yes	no	no
Other OBs	yes	no	no	no

Depending on the OB in which the SFB 54 “RALRM” is called, the TINFO and AINFO parameters are only partially written. The information entered in each case is shown in Table 6.60.

Composition of output parameter STATUS

The output parameter STATUS contains fault information. A detailed description of the interpretation as ARRAY[1..4] OF BYTE can be found in the reference manual “System and standard functions for S7-300/400”.

Composition of output parameter TINFO

The TINFO (Task INFOrmation) parameter contains the start and administration information of the OB in whose context the SFB 54 “RALRM” has been called. The structure is shown in Tables 6.60 and 6.61 and in Figs. 6.11 to 6.13.

Table 6.61 Structure of output parameter TINFO with SFBþ54 “RALRM”

Byte	Description
0-19	Start information of OB in which the SFB 54 has been called.
20-21	Address of component triggering the alarm (module)
22-31	Administration information

	Byte 20								Byte 21							
Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	0								Rack number (0-31)							

Fig. 6.11 Address structure (bytes 20-21) of TINFO parameter with central structure

	Byte 20								Byte 21							
Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	0	DP master system ID (1-31)							Station number (0-127)							

Fig. 6.12 Address structure (bytes 20-21) of TINFO parameter with distributed structure with Profibus DP

	Byte 20								Byte 21							
Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	1	IO System ID (0-15)				Device number (0-2047)										

Fig. 6.13 Address structure (bytes 20-21) of TINFO parameter with distributed structure with Profinet IO

Table 6.62 Structure of output parameter TINFO

Byte	Data type	Description
20	BYTE	Central: 0 Distributed: Profibus DP: Bits 0-6: 1-31: DP master system ID Bit 7: 0 Profinet IO: Bits 0-2: 0-7: part of station number Bits 3-6: 0-15: actual IO System ID – 100Bit 7:1
21	BYTE	Central: 0-31: rack number Distributed: Profibus DP: 0-127: station number Profinet IO: 0-255: part of station number

Table 6.62 Structure of output parameter TINFO *(continued)*

Byte	Data type	Description
22	BYTE	Central: 0 Distributed: Bits 0-3: 0: Profibus DP slave 1: Profibus DPS7 slave 2: Profibus DPS7 V1 slave 3: Profibus DPV1 slave 4-127: reserved 128: Profinet IO >128: reserved Bits 4-7: Profile type (reserved)
23	BYTE	Central: 0 Distributed: Bits 0-3: Type of alarm information 0: transparent; alarm is from a configured distributed module (always with ProfinetþIO) 1: proxy; alarm of a non-DPV1 slave/non-IO Device or a non-configured slot. 2: alarm generated in the CPU >2: reserved Bits 4-7: Structure version: 0: initial >0: reserved
24	BYTE	Central: 0 Distributed: Flags of the DP master/IO controller interface module Bit 0: 0: alarm from an integral interface module 1: alarm from an external interface module Bits 1-7: Reserved
25		Central: 0 Distributed: Bit 0: Flags of the DP master/IO controller interface module: Profibus DP: EXT_DIAG_FLAG from the diagnostics frame or 0 if this bit is not present with the alarm. 1: DP slave faulty. Profinet IO: AR diagnostics state or 0 if no information is present with the alarm 1: IO Device faulty. Bits 1-7: Reserved
26-27	WORD	Central: 0 Distributed: Profibus DP/Profinet IO ID number for unambiguous identification of the DP slave/IO Device.
28-29	WORD	Central, Profibus DP: Not present Profinet IO: Vendor number (Vendor_ID)
30-31	WORD	Central, Profibus DP: Not present Profinet IO: Instance ID

In order to obtain the correct IO System ID, the value 100 (decimal) must be added to the signaled IO System ID.

Composition of output parameter AINFO

The AINFO (Alarm INFOrmation) parameter contains the description of an alarm, consisting of a header and supplementary alarm information. The structure is shown in Tables 6.63 to 6.65.

Table 6.63 Data structure of output parameter AINFO with alarms from Profinet IO

Byte	Meaning
0-25	Header (see Table 6.64)
26-1431	Optional supplementary alarm information: standardized diagnostics data for the respective alarm (see Table 6.65)

Table 6.64
Structure of header of output parameter AINFO with alarms from Profinet IO

Byte	Data type	Description
0, 1	WORD	Bits 0-7: Block type Bits 8-15: Reserved
2, 3	WORD	Block length
4, 5	WORD	Version: Bits 0-7: Low byte Bits 8-15: High byte
6, 7	WORD	ID of alarm type: 1: Diagnostics interrupt, up 2: Hardware interrupt 3: Removal interrupt 4: Insertion interrupt 5: Status interrupt 6: Update interrupt 7: Redundancy interrupt 8: Controlled by IO Supervisor 9: Released by IO Supervisor 10: Non-configured module inserted 11: Return of a submodule 12: Diagnostics interrupt, down 13-31: Reserved 32-127: Vendor-specific interrupt >128: Reserved
8-11	DWORD	Application Process Identifier (API)
12, 13	WORD	Slot number of component triggering the alarm (0-65535)
14, 15	WORD	Submodule slot number of component triggering the alarm (0-65535)
16-19	DWORD	Module ID
20-23	DWORD	Submodule ID
24-25	WORD	Alarm specification: Bits 0-10: 0-2047: sequence number Bit 11: General diagnostics FALSE: no channel diagnostics present. TRUE: channel diagnostics present. Bit 12: Status of vendor-specific diagnostics. FALSE: no vendor-specific status information present. TRUE: vendor-specific status information present. Bit 13: Status of submodule diagnostics. FALSE: no status information present, all errors have been eliminated. TRUE: at least one channel diagnostics and/or status information present.

Table 6.64
Structure of header of output parameter AINFO with alarms from Profinet IO *(continued)*

Byte	Data type	Description
24-25 *(continued)*	WORD	Bit 14: Reserved Bit 15: Status of application relation diagnostics: FALSE: none of the modules configured within this AR signals diagnostics. TRUE: at least one of the modules configured within this AR signals diagnostics.

The supplementary alarm information is optional and therefore not present with every alarm. It contains a maximum of 1406 bytes with detailed, standardized diagnostics data on the respective alarm (Table 6.65).

Table 6.65 Structure of supplementary alarm information of output parameter AINFO with alarms from Profinet IO

Byte	Data type	Description
0, 1	WORD	Format ID: The format ID provides information on how the following supplementary alarm information is structured, and is set by an IO Device depending on the type of diagnostics information. W#16#0000-W#16#7FFF: Vendor-specific diagnostics W#16#8000: Channel diagnostics W#16#8001: Channel diagnostics and/or vendor-specific diagnostics W#16#8002-W#16#FFFF: Reserved
With format ID W#16#8000: channel diagnostics Output of channel diagnostics for the faulty channels in blocks of 6 bytes.		
2, 3	WORD	Channel number of component triggering the alarm Possible values: W#16#0000-W#16#FFFF W#16#0000-W#16#7FFF: Channel number of submodule/module. W#16#8000: Proxy for the complete submodule. W#16#8001-W#16#FFFF: Reserved
4	BYTE	Bits 0-2: Reserved Bits 3-4: Type of error 0: reserved 1: UP error 2: DOWN error 3: DOWN error, further errors present. Bits 5-7: Type of channel 0: reserved 1: input channel 2: output channel 3: input/output channel
5	BYTE	Data format: 0: Optional data format 1: Bit 2: 2 bits 3: 4 bits 4: Byte 5: Word 6: Doubleword 7: 2 doublewords 8-255: Reserved

Table 6.65 Structure of supplementary alarm information of output parameter AINFO with alarms from Profinet IO *(continued)*

Byte	Data type	Description
6, 7	WORD	Type of error: (not every type of error is supported by every channel. Associated information can be found in the description of the diagnostics data for the corresponding device.) W#16#0000: Reserved W#16#0001: Short-circuit W#16#0002: Undervoltage W#16#0003: Overvoltage W#16#0004: Overload W#16#0005: Overtemperature W#16#0006: Open-circuit W#16#0007: Upper limit violated W#16#0008: Lower limit violated W#16#0009: Error W#16#000A-W#16#000F: Reserved W#16#0010-W#16#001F: Vendor-specific W#16#0020-W#16#00FF: Reserved W#16#0100-W#16#7FFF: Vendor-specific W#16#8000: Device diagnostics present W#16#8001-W#16#FFFF: Reserved
With format ID W#16#8001: channel diagnostics and/or vendor-specific diagnostics.		
2, 3	WORD	Block type
4, 5	WORD	Block length
6	BYTE	Version: High byte
7	BYTE	Version: Low byte
8, 9	WORD	Slot number
10, 11	WORD	Subslot number
12, 13	WORD	Channel number
14, 15	WORD	Channel properties
16, 17	WORD	Format ID: W#16#0000-W#16#7FFF: Vendor-specific diagnostics W#16#8000: Channel diagnostics W#16#8001-W#16#FFFF: Reserved
18-n	BYTE	Dependent on format ID
With format ID W#16#7FFF: vendor-specific diagnostics		
2-n	BYTE	Corresponding to vendor information.

6.3.3 System Functions and System Function Blocks with Profinet IO

System functions are made available by the operating system of a Simatic S7 CPU, and provide system-specific services. Certain blocks known from Profibus DP have a partially new implementation for Profinet IO since one of the features is that larger quantity frameworks are possible compared to Profibus. These new blocks can also be used with Profibus. For Simatic S7 CPUs with integral Profinet interface, Tables 6.66 to 6.69 provide an overview of:

- system functions which can be used with both Profinet IO and Profibus DP,

- system functions which have to be replaced by other functions when converting from Profibus DP to Profinet IO,
- system functions whose functions can be emulated by other functions when converting from Profibus DP to Profinet IO and
- system functions which can be used with Profibus DP but not with Profinet IO.

Table 6.66 SFCs and SFB which can be used with Profinet IO and Profibus DP

System function/ function block	Description
SFC 12 "D_ACT_DP"	Deactivate and activate DP slaves/IO Devices.
SFC 14 "DPRD_DAT"	Read consistent data from DP standard slaves/IO Devices.
SFC 15 "DPWR_DAT"	Write consistent data to DP standard slaves/IO Devices.
SFC 51 "RDSYSST"	Read out system state list (SSL) or SSL sublist extract.
SFC 70 "GEO_LOG"	Determine start address of a module.
SFC 71 "LOG_GEO"	Determine slot associated with a logical address.
SFB 81 "RD_DPAR"	Read predefined parameters.

Table 6.67 SFCs which cannot be used with Profinet IO but which can be replaced

System function	Description	Can be replaced by
SFC 5 "GADR_LGC"	Determine logical base address of a module.	SFC 70 "GEO_LOG"
SFC 13 "DPNRM_DG"	Read diagnostics data of a DP slave.	Event-based: SFB 54 "RALRM" Status-based: SFB 52 "RDREC"
SFC 49 "LGC_GADR"	Determine the slot associated with a logical address.	SFC 71 "LOG_GEO"
SFC 58 "WR_REC"	Write record.	SFB 53 "WRREC"
SFC 59 "RD_REC"	Read record.	SFB 52 "RDREC"
SFC 102 "RD_DPARA"	Read predefined parameters.	SFB 81 "RD_DPAR"

Table 6.68 SFCs which cannot be used with Profinet IO but which can be emulated

System function	Description	Can be emulated by
SFC 54 "RD_DPARM"	Read predefined parameters.	SFB 81 "RD_DPAR"
SFC 55 "WR_PARM"	Write dynamic parameters.	SFB 53 "WRREC"
SFC 56 "WR_DPARM"	Write predefined parameters.	SFB 81 "RD_DPAR" SFB 53 "WRREC"
SFC 57 "PARM_MOD"	Parameterize module.	SFB 81 "RD_DPAR" SFB 53 "WRREC"

Table 6.69 SFCs and SFB which cannot be used with Profinet IO

System function/	Description
SFC 7 "DP_PRAL"	Trigger process alarm with DP master.
SFC 11 "DPSYC_FR"	Synchronize groups of DP slaves.
SFC 72 "I_GET"	Read data from a communications partner within own S7 station.
SFC 73 "I_PUT"	Write data in a communications partner within own S7 station.
SFC 74 "I_ABORT"	Abort an existing connection to a communications partner within own S7 station.
SFC 103 "DP_TOPOL"	Determine the bus topology in a DP master system.
SFB 75 "SALRM"	Send alarm.

This chapter provides an overview of the above-mentioned functions for application in the user program of a Simatic S7 CPU.

Deactivate and activate DP slaves/Profinet IO Devices using SFC 12 "D_ACT_DP"

If DP slaves/IO Devices are configured in a CPU but are not actually present or currently required, the CPU nevertheless regularly accesses these DP slaves/IO Devices. With the DP slaves/IO Devices deactivated, these CPU access operations and the corresponding error functions no longer occur.

The SFCþ12 "D_ACT_DP" allows specific activation or deactivation of configured DP slaves/IO Devices as well as scanning of the status "Activated/Deactivated".

The following must be observed when deactivating:

- The process outputs of deactivated DP slaves/IO Devices are set to the configured substitute values or to 0 (safe state).
- Deactivated DP slaves/IO Devices are identified as faulty or missing on the fault LEDs of the DP master/IO controller or the CPU.
- Deactivation of a DP slave/IO Device does not result in starting of the program execution error OB (OB 85) or of the rack failure OB (OB 86). An entry is not made in the diagnostics buffer.
- The failure of a deactivated DP slave/IO Device is not recognized by the DP master/IO controller but is only determined when activating the DP slave/IO Device again.
- The I/O access error OB (OB 122) is called upon direct access to user data of deactivated DP slaves/IO Devices from the user program.
- Access to deactivated DP slaves/IO Devices using an SFC (e.g. SFCþ59 "RD_REC") result in the same error messages as access operations to non-available DP slaves/IO Devices.

Activation results in configuration and parameterization of the activated DP slaves/IO Devices by the associated DP master/IO controller. Activation is conclud-

ed when the exchange of user data is commenced. The following applies in addition:

- Activation of a DP slave/IO Device does not result in starting of the program execution error OB (OB 85) or of the rack failure OB (OB 86). An entry is not made in the diagnostics buffer.
- The attempt to activate a deactivated slave which is physically disconnected from the DP bus using the SFC 12 “D_ACT_DP” results in the error code W#16#80A2 after approximately one minute. The slave remains deactivated. If the DP slave is connected again to the DP bus at a later point in time, it must be reactivated using SFC 12 “D_ACT_DP”.

SFCþ12 “D_ACT_DP” operates asynchronously, i.e. processing may be extended over several user program cycles. The status of request processing is displayed in the output parameter BUSY.

Table 6.70 Parameters of SFCþ12 “D_ACT_DP”

Parameter	Declaration	Data type	Memory area	Description
REQ	INPUT	BOOL	I, Q, F, D, L, constants	TRUE: Carry out activation or deactivation
MODE	INPUT	BYTE	I, Q, F, D, L, constants	Request ID: 0: Status scanning activated/deactivated 1: Activate 2: Deactivate
LADDR	INPUT	WORD	I, Q, F, D, L, constants	Logical address of DP slave/IO Device
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC
BUSY	OUTPUT	BOOL	I, Q, F, D, L	Active ID: FALSE: Request finished TRUE: Request active

Table 6.71 Specific return values of SFCþ12 “D_ACT_DP”

Error code (W#16#...)	Description
0000	No fault has occurred.
0001	DP slave/IO Device is activated (only with MODE = 0).
0002	DP slave/IO Device is deactivated (only with MODE = 0).
7000	First call with REQ=FALSE: no request active; BUSY=FALSE.
7001	First call with REQ=TRUE: request triggered; BUSY=TRUE.
7002	Intermediate call (REQ irrelevant): request is still active; BUSY=TRUE.
8090	Specified logical address invalid or specified logical address is that of an I slave.
8092	The ongoing deactivation process of a DP slave/IO Device (MODE=2) cannot be aborted by activating it (MODE=1).
8093	The specified address does not belong to a DP slave/IO Device or unknown value for the MODE parameter.

Table 6.71 Specific return values of SFCþ12 “D_ACT_DP” *(continued)*

Error code (W#16#...)	Description
80A1	The component addressed by the specified address could not be parameterized. (This error code is only possible with MODE = 1.) The SFC only delivers this error information if a DP slave/IO Device to be activated fails again during parameterization. If only the parameterization of a single module was unsuccessful, the SFC delivers the error information W#16#0000.
80A2	The addressed component does not provide a feedback.
80A3	The DP master/IO controller does not support this function.
80A4	The CPU does not support this function with external DP masters/IO controllers.
80A6	Slot error in the DP slave/IO Device; it is not possible to access all user data (only with MODE=1). The SFC only delivers this error information if a DP slave/IO Device to be activated fails again following parameterization and before the end of the SFC. If only a single module is not available, the SFC delivers the error information W#16#0000.
80C1	The SFC has been started and is continued with a different logical address (only with MODE=1).
80C3	Temporary resource error: deactivation and activation of DP slaves/IO Devices is not currently possible. The CPU is currently processing the maximum number of activation/deactivation requests possible (only with MODE = 1 and MODE = 2) or the CPU is currently receiving a modified configuration.
8xyy	General error information corresponding to the general error codes of parameter RET_VAL.

Read consistent data of a DP standard slave/IO Device using SFC 14 “DPRD_DAT”

By calling the synchronous system function SFC 14 “DPRD_DAT” (Decentral Periphery ReaD DATa), RECORD is read by the module addressed in LADDR. The maximum readable data length is CPU-specific.

Table 6.72 Parameters of SFCþ14 “DPRD_DAT”

Parameter	Declaration	Data type	Memory area	Description
LADDR	INPUT	WORD	I, Q, F, D, L, constants	Logical address of the DP slave/IO Device in hexadecimal format.
RECORD	OUTPUT	ANY VARTYPE: BYTE	I, Q, F, D, L	Destination range for the read record.
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC.

Table 6.73 Specific return values of SFCþ14 “DPRD_DAT”

Error code (W#16#...)	Description
0000	No fault has occurred.
808x	System error with external DP interface module.
8090	No module has been configured for the specified logical address, or the limit regarding the length of the consistent data has not been observed, or the specified logical address is not hexadecimal.
8092	A type which is not BYTE has been specified in the ANY reference.

Table 6.73 Specific return values of SFCþ14 “DPRD_DAT” *(continued)*

Error code (W#16#...)	Description
8093	A DP slave/IO Device from which consistent data can be read does not exist for the logical address specified by LADDR.
80A0	An access error has been detected when accessing the I/O.
80B0	DP slave failure on an external DP interface module.
80B1	The length of the specified destination range is not the same as the user data length configured with Step 7.
80B2 80B3	System error with external DP interface module.
80C0	The data have not yet been read by the module.
80C2 80Fx 87xy	System error with external DP interface module.
8xyy	General error information corresponding to the general error codes of parameter RET_VAL.

Write data consistently to DP standard slave/IO Device using SFC 15 “DPWR_DAT”

By calling the synchronous system function SFC 15 “DPWR_DAT” (Decentral Periphery WRite DATa), RECORD is transmitted to the module addressed in LADDR. The maximum transmittable data length is CPU-specific.

Table 6.74 Parameters of SFCþ15 “DPWR_DAT”

Parameter	Declaration	Data type	Memory area	Description
LADDR	INPUT	WORD	I, Q, F, D, L, constants	Logical address of DP slave/IO Device in hexadecimal format.
RECORD	INPUT	ANY VARTYPE: BYTE	I, Q, F, D, L	Source range for the record to be transmitted.
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC.

Table 6.75 Specific return values of SFCþ15 “DPWR_DAT”

Error code (W#16#...)	Description
808x	System error with external DP interface module.
8090	No module has been configured for the specified logical address, or the limit regarding the length of the consistent data has not been observed, or the specified logical address is not hexadecimal.
8092	A type which is not BYTE has been specified in the ANY reference.
8093	A DP slave/IO Device to which the consistent data can be written does not exist for the logical address specified by LADDR.
80A1	An access error has been detected when accessing the I/O.
80B0	DP slave failure on an external DP interface module.
80B1	The length of the specified source range is not the same as the user data length configured with Step 7.

Table 6.75 Specific return values of SFCþ15 “DPWR_DAT” *(continued)*

Error code (W#16#...)	Description
80B2 80B3	System error with external DP interface module.
80C1 80C2 80Fx	The data of the previous write request on the module have not yet been processed by it.
85xy	System error with external DP interface module.
8xyy	General error information corresponding to the general error code of parameter RET_VAL.

Reading an SSL sublist or SSL sublist extract using the SFC 51 “RDSYSST”

SFC 51 “RDSYSST” can be used to read an SSL sublist or an SSL sublist extract. The assignments of the SSL_ID and INDEX parameters define which SSL sublists or sublist extracts are read.

SFC 51 “RDSYSST” is executed asynchronously, i.e. processing may be carried out in several user program cycles. The system function can be called more than once within a user program cycle. The maximum number of simultaneous calls depends on the CPU. A read request starts when the function is called by the input parameter REQ=TRUE. It is terminated as soon as the output parameter BUSY returns the value FALSE (see Table 6.76).

If several read requests are triggered in quick succession, the operating system ensures that they do not influence one another and that all requests are handled correctly. If the number of simultaneous read requests is limited by the system re-

Table 6.76 Parameters of SFCþ51 “RDSYSST”

Parameter	Declaration	Data type	Memory area	Description
REQ	INPUT	BOOL	I, Q, F, D, L, constants	TRUE: Triggering of read request
SSL_ID	INPUT	WORD	I, Q, F, D, L, constants	SSL ID of sublist or sublist extract
INDEX	INPUT	WORD	I, Q, F, D, L, constants	Type or number of an object in a sublist
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC
BUSY	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Read procedure finished TRUE: Read procedure running
SSL_HEADER	OUTPUT	STRUCT	D, L	STRUCT LENTHDR: WORD N_DR: WORD END_STRUCT LENTHDR: Length of read records in bytes. N_DR: Number of records in the block of read records.
DR	OUTPUT	ANY	I, Q, F, D, L	Destination range for the read SZL sublist or the read SZL sublist extract.

Table 6.77 Specific return values of SFCþ51 “RDSYSST”

Error code (W#16#...)	Description
0000	No error has occurred.
0081	Length of result block too small. (As many records as possible are nevertheless delivered. The SSL header indicates this number).
7000	First call with REQ=0: no data transfer active; BUSY=0.
7001	First call with REQ=1: data transfer triggered; BUSY=1.
7002	Intermediate call (REQ irrelevant): data transfer already active; BUSY=1.
8081	Length of result block too small (space insufficient for even one record).
8082	SSL_ID is incorrect or unknown in the CPU or SFC.
8083	INDEX incorrect or illegal.
8085	The information is not currently available as a result of system conditions, e.g. insufficient resources.
8086	Record cannot be read because of a system error (bus, modules, operating system).
8087	Record cannot be read because the module does not exist, or is not acknowledged.
8088	Record cannot be read because the actual module ID is different from that expected.
8089	Record cannot be read because the module does not have diagnostics capability.
80A2	DP protocol error (layer 2 error) (temporary error).
80A3	DP protocol error with user interface/user (temporary error).
80A4	Communication on the communications bus faulty (error occurs between CPU and external DP interface module, temporary error).
80C5	Distributed I/O not available or deactivated.
80C6	Transfer of record was canceled because of priority class abort (restart or background).
80D2	Record cannot be read because the module does not have diagnostics capability.
8xyy	General error information corresponding to the general error codes of the RET_VAL parameter.

sources, this is signaled in RET_VAL. This temporary error can be eliminated by repeating the request.

The call of an SSL sublist not supported by Profinet IO delivers the error ID 0x8083 (index incorrect or illegal) in the return value of the system function SFC 51 “RDSYSST”.)

Each SSL sublist within the SSL has its own number. Using the SSL ID, a sublist can be read either completely or only an extract thereof (Fig. 6.9).

Determine start address of a module using SFC 70 “GEO_LOG”

If the associated module slot is known for the channel of a signal module, the system function SFC 70 “GEO_LOG” (convert GEOgraphical address to LOGical address) can be used to determine the logical I/O start address of the module, i.e. the smallest input or output address, from the geographical address.

Table 6.78 Parameters of SFCþ70 "GEO_LOG"

Parameter	Declaration	Data type	Memory area	Description
MASTER	INPUT	INT	I, Q, F, D, L, constants	Area ID: 0: Racks 0-3 (central controller) 1-31: DP master system ID 100-115: IO system ID
STATION	INPUT	INT	I, Q, F, D, L, constants	Area ID = 0: Rack number Area ID > 0: Station number of field device
SLOT	INPUT	INT	I, Q, F, D, L, constants	Slot number
SUBSLOT	INPUT	INT	I, Q, F, D, L, constants	Submodule slot number: 0: No submodule >0: Submodule number (only Profinet IO)
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC
LADDR	OUTPUT	WORD	I, Q, F, D, L	Logical address of module Bit 15: FALSE: input address TRUE: output address

Table 6.79 Specific return values of SFCþ70 "GEO_LOG"

Error code (W#16#...)	Description
0000	No error has occurred.
8094	No subnet with the specified SUBNETID has been configured.
8095	Illegal value in STATION parameter.
8096	Illegal value in SLOT parameter.
8097	Illegal value in SUBSLOT parameter.
8099	Slot is not configured.
809A	Submodule address is not configured for the selected slot.
8xyy	General error information in line with the general error codes of the RET_VAL parameter.

Determine start address of a module using SFC 71 "LOG_GEO"

The system function SFC 71 "LOG_GEO" (convert LOGical address to GEOgraphical address) converts a logical I/O address into a geographical address, and determines the module slot associated with the logical address as well as the offset in the user data address space of the module.

SFC 71 "LOG_GEO" replaces the SFC 49 "LGC_GADR" and expands the latter's functionality for use with Profinet IO (see Tables 6.80 and 6.81).

Table 6.80 Parameters of SFCþ71 “LOG_GEO”

Parameter	Declaration	Data type	Memory area	Description
LADDR	INPUT	WORD	I, Q, F, D, L, constants	Logical address of module Bit 15: 0: Input address 1: Output address
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC
AREA	OUTPUT	INT	I, Q, F, D, L	Area ID: 0: S7-400 1: S7-300 2: Profibus DP, Profinet IO 3: S5 I/O area 4: S5 extended I/O area 5: S5 IM3 area 6: S5 IM4 area
MASTER	OUTPUT	INT	I, Q, F, D, L	Area: 0-1, 3-6: 0 2: 1-31/100-115 1-31: DP master system ID 100-115: Profinet IO system ID
STATION	OUTPUT	INT	I, Q, F, D, L	Area: 0-1, 3-6: Rack No. 2: Station number
SLOT	OUTPUT	INT	I, Q, F, D, L	Area: 0-1: Slot number 2: Slot number in station 3-6: Slot number of adapter casing
SUBSLOT	OUTPUT	INT	I, Q, F, D, L	Area: 0-1, 3-6: 0 2: Submodule No. (only Profinet IO)
OFFSET	OUTPUT	INT	I, Q, F, D, L	Area: 0-1: Difference between logical address and logical base address 2: Offset in user data address area of associated module 3-6: Address in S5-x area

Table 6.81 Specific return values of SFC 71 “LOG_GEO”

Error code (W#16#...)	Description
0000	No error has occurred.
8090	Specified logical address is invalid.
8xyy	General error information corresponding to the general error codes of the RET_VAL parameter

Read predefined parameters using SFB 81 “RD_DPAR”

By calling the asynchronous system function block SFB 81 “RD_DPAR” (ReaD Device PARameter), the record with the number INDEX is read out of the central or distributed module addressed by LADDR.

The output parameter VALID=TRUE indicates that the record has been successfully transferred to the destination range RECORD. In this case, the output parameter LEN contains the length of the read data in bytes. If the output parameter ERROR=TRUE, an error occurred during the read procedure. In this case, the output parameter STATUS contains the error information (see Tables 6.82 and 6.83).

SFBþ81 “RD_DPAR” operates asynchronously, i.e. processing may extend over several user program cycles. The status of request processing is displayed in the output parameter BUSY and bytes 2 and 3 of the output parameter STATUS. Bytes 2 and 3 of STATUS correspond to the output parameter RET_VAL of the asynchronously operating SFC.

Table 6.82 Parameters of SFBþ81 “RD_DPAR”

Parameter	Declaration	Data type	Memory area	Description
REQ	INPUT	BOOL	I, Q, F, D, L	TRUE: Trigger read request
LADDR	INPUT	WORD	I, Q, F, D, L, constants	Logical address of module Bit 15: FALSE: Input address TRUE: Output address
REQ	INPUT	BOOL	I, Q, F, D, L	TRUE: Trigger read request
LADDR	INPUT	WORD	I, Q, F, D, L, constants	Logical address of module Bit 15: FALSE: Input address TRUE: Output address
INDEX	INPUT	INT	I, Q, F, D, L, constants	Record number
VALID	OUTPUT	BOOL	I, Q, F, D, L	TRUE: New record has been found and is valid.
BUSY	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Read procedure finished TRUE: Read procedure running
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: No error occurred TRUE: Error occurred during read procedure
STATUS	OUTPUT	DWORD	I, Q, F, D, L	Call ID (bytes 2 and 3) or error code
LEN	OUTPUT	INT	I, Q, F, D, L	Length of read record information in bytes
RECORD	IN_OUT	ANY	I, Q, F, D, L	Destination range for the read record

Table 6.83 Specific return values from SFB 81 “RD_DPAR”

Error code (W#16#...)	Description
0000	No error has occurred.
7000	First call with REQ=0: no data transfer active; BUSY=0.
7001	First call with REQ=1: data transfer triggered; BUSY=1
7002	Intermediate call (REQ irrelevant): data transfer already active; BUSY=1
8090	Specified logical base address invalid: No assignment is present in SDB1/SDB2x, or it is not a base address.
8092	Only S7-400: A type specification other than BYTE has been defined in an ANY reference.
8093	Calling of the SFB is illegal for the module specified by LADDR.
80A1	Negative acknowledgement when sending the record to the module (module removed or faulty during transfer).
80A2	DP protocol error in layer 2, possibly hardware/interface error in DP slave
80A3	DP protocol error with user interface/user.
80A4	Communication faulty on communications bus.
80B0	SFB not possible for type of module, or the module does not recognize the record.
80B1	The length of the record to be transferred is incorrect (the length of the destination range produced by RECORD is too small).
80B2	The configured slot is not occupied.
80B3	Actual type of module is not same as expected type in SDB1.
80C1	The data of the previous write request on the module for the same record have not yet been processed by the module.
80C2	The module is currently processing the maximum possible number of requests for a CPU.
80C3	Required facilities (memory etc.) are currently occupied.
80C4	Temporary internal error. Request could not be executed. Repeat the request. If this error occurs frequently, it is recommendable to check the system for sources of electrical interference.
80C5	Distributed I/O not available or deactivated.
80C6	Transfer of record was canceled because of priority class abort (restart or background).
80D0	No entry for the module is present in the associated SDB.
80D1	The record number is not configured in the associated SDB for the module (record numbers Š 241 are rejected by Step 7).
80D2	According to the module ID, the module cannot be parameterized.
80D3	The SDB cannot be accessed since it does not exist.
80D4	Only S7-300: SDB structure error: SDB-internal pointer points outside SDB.
80D5	The record is static.
8xyy	General error information corresponding to the general error codes of the RET_VAL parameter.

6.3.4 Special Functions for Profinet IO

The functions described in this chapter are used in the respective central controller to update the process data when working with a Simatic Net CP as the IO controller/IO Device. Table 6.84 provides an overview of these functions.

Table 6.84 Special functions for Profinet IO

Function block/ function	Description
FC 11 "PNIO_SEND"	Transfer of process data to the Simatic Net CP.
FC 12 "PNIO_RECV"	Receipt of process data from the Simatic Net CP.

Process data transfer with FC 11 "PNIO_SEND"

FC 11 "PNIO_SEND" must be called in the user program of the Simatic S7 CPU:

- When using the CP as IO controller, FC 11 transfers the output data saved in a data block or memory area to the CP, which then transfers the data to the IO Devices. The function delivers the IOCS (IO Consumer Status) of the IO Device outputs as the status display.
- When using the CP as IO Device, FC 11 transfers the preprocessed input data saved in a data block or memory area (the input data of the IO controller from the Profinet IO view) to the CP, which then transfers the data to the IO controller. The function delivers the IOCS of the IO controller inputs as the status display.

The IOCS is transferred simultaneously with each output data during runtime, and provides information on the quality of the data content. It should be noted with the Simatic Net-CP 343-1 PN that the IOCS is not signaled synchronously with the data but is delayed by one user program cycle. The user data and IOCS are therefore not consistent.

The user program cycle and the I/O data exchange cycle are independent of one another. Data transfer between the process data of the CPU, the CP and the and the CP as IO controller/IO Device is carried out as follows:

- Processing of the data area specified in the SEND parameter.
- Consistent transfer of the output data area of length LEN, commencing with address 0 of the data area specified in the SEND parameter, from the CPU to the CP by calling FC 11 "PNIO_SEND". Depending on the size of the data area transferred, the block processing time may take several user program cycles.
- Transfer of data from the Simatic Net CP to the IO Devices or IO controller; output of the IOCS signaled by the IO Devices/IO controller.
- Evaluation of the CHECK_IOCS parameter, and also of the IOCS parameter if applicable, by the user program of the CPU.

Independent of the data transfer consistency between CPU and CP, the data consistency within the IO System is only guaranteed for the respective I/O slot.

The provision of substitute values is supported during startup and in the case of faults.

During startup, when the CPU's status changes from STOP to RUN, the outputs can be initialized, for example, by setting a "startup" bit memory in the startup OB 10x. This bit memory is evaluated in cyclic mode (OB1) in order to call the FC 11 "PNIO_SEND" with initialization values if necessary (Table 6.85).

In the case of faults (removal/insertion or station failure/return), a module failure can be determined by evaluating IOCS and IOPS. Corresponding substitute input values of the CPU can then be applied to the CPU's process input image.

Table 6.85 Parameters of the FC 11 "PNIO_SEND"

Parameter	Declaration	Data type	Memory area	Description
CPLADDR	INPUT	WORD	I, Q, F, D, L, constants	Module start address from the configuration of the CP in HW-Config. The address must not be changed until a request has been completed.
SEND	IN_OUT	ANY VARTYPE: BYTE	M, D	Address and length of the output data area. The transfer always commences with address 0 of the output data area. Operation of CP as IO controller: the length should correspond to the total length of the distributed I/O configured in HW-Config, where gaps in the addresses are also transferred. Operation of CP as IO Device: the data structure results from the slot sequence of the input modules configured on the IO controller line for this IO Device and their length without gaps in the addresses.
LEN	INPUT	WORD	I, Q, F, D, L, constants	Length of output data to be transferred in bytes. Operation of CP as IO controller: the data are transferred in the sequence of logical addresses. Operation of CP as IO Device: the data are transferred in the slot sequence like the input modules are configured on the IO controller line for this IO Device. Consistency between the length programmed for LEN and the configuration of the IO Devices is not checked by FC 11 "PNIO_SEND".
DONE	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request being executed or request completed with error. TRUE: Request completed without error.
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request being executed or request completed without error. TRUE: Request completed with error.

Table 6.85 Parameters of the FC 11 "PNIO_SEND" *(continued)*

Parameter	Declaration	Data type	Memory area	Description
STATUS	OUTPUT	WORD	I, Q, F, D, L	Detailed information on execution of request.
CHECK_IOCS	OUTPUT	BOOL	I, Q, F, D, L	Supplementary information on IOCS: FALSE: All IOCS bits have the GOOD status. TRUE: At least one IOCS bit has the BAD status. The IOCS parameter must be evaluated in this case.
IOCS	OUTPUT	ANY VARTYPE: BYTE	M, D	One status bit is transferred for each byte of output data. FALSE: IOCS=GOOD TRUE: IOCS=BAD The length value depends on the value of the LEN parameter. The minimum length of the ANY pointer is (LEN+7)/8. The area always commences with the IOCS bit of start address 0. Operation of CP as IO controller: in the case of gaps in the addresses, the corresponding IOCS bit is set to GOOD! Operation of CP as IO Device: gaps in the addresses are not transmitted.

Importing of process data using FC 12 "PNIO_RECV"

FC 12 "PNIO_RECV" must be called in the user program of the Simatic S7 CPU.

- When using the CP as IO controller, FC 12 imports the input data of the IO Devices from the CP and saves them in a data block or memory area. The function delivers the IOPS (IO provider status) of the IO Device inputs as the status display.
- When using the CP as IO Device, FC 12 imports the output data of the IO controller from the CP and saves them in a data block or memory area. The function delivers the IOPS (IO provider status) of the IO controller outputs as the status display.

The IOPS is transmitted simultaneously with each item of input data during runtime, and provides information on the quality of the data content.

The user program cycle and the IO data exchange cycle are independent of one another. Data transfer between the process data of the CPU and the CP as IO controller/IO Device is carried out as follows (Table 6.86):

- Receipt of input data from the IO Devices/IO controller.
- Consistent transfer of the input data range of length LEN, commencing with address 0 of the data range specified in the RECV parameter, and with signaling of the IOPS from the CP to the CPU by calling FC 12 "PNIO_RECV". Depending on

the size of the data area transferred, the block processing time may take several user program cycles.

- Evaluation of the CHECK_IOPS parameter, and also of the IOPS parameter if applicable, by the user program of the CPU.
- Processing of the input data received without errors (IOPS=GOOD) in the user program of the CPU, or reaction to input data with IOPS=BAD if applicable.

Independent of the data transfer consistency between CPU and CP, the data consistency within the IO System is only guaranteed for the respective I/O slot.

Table 6.86 Parameters of FC 12 “PNIO_RECV”

Parameter	Declaration	Data type	Memory area	Description
CPLADDR	INPUT	WORD	I, Q, F, D, L, constants	Module start address from the configuration of the Profinet CP in HW-Config. The address must not be changed until a request has been completed.
RECV	IN_OUT	ANY VARTYPE: BYTE	M, D	Address and length of the input data area: The transfer always commences with address 0 of the input data area. Operation of CP as IO controller: The length should correspond to the total length of the distributed I/O configured in HW-Config, where gaps in the addresses are also transferred. Operation of CP as IO Device: The data structure results from the slot sequence of the output modules configured on the IO controller line for this IO Device and their length without gaps in the addresses.
LEN	INPUT	WORD	I, Q, F, D, L, constants	Length of logical output addresses to be transferred in bytes: Operation of CP as IO controller: The data are transferred in the sequence of logical addresses. Operation of CP as IO Device: The data are transferred in the slot sequence similar to the configuration of the output modules on the IO controller line for this IO Device. Consistency between the length programmed for LEN and the configuration of the IO Devices is not checked by FC 12 “PNIO_RECV””
NDR	OUTPUT	BOOL	I, Q, F, D, L	New Data Received: FALSE: Request being executed or request completed with error. TRUE: Request completed without error.
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request being executed or request completed without error. TRUE: Request completed with error.
STATUS	OUTPUT	WORD	I, Q, F, D, L	Detailed information on execution of request.

Table 6.86 Parameters of FC 12 "PNIO_RECV" *(continued)*

Parameter	Declaration	Data type	Memory area	Description
CHECK_IOPS	OUTPUT	BOOL	I, Q, F, D, L	Supplementary information on IOPS: FALSE: All IOPS bits have the GOOD status. TRUE: At least one IOPS bit has the BAD status. The IOPS parameter must be evaluated in this case.
IOPS	OUTPUT	ANY VARTYPE: BYTE	F, D	One status bit is transferred for each byte of input data. FALSE: IOPS=GOOD TRUE: IOPS=BAD The length value depends on the value of the length of the LEN parameter. The minimum length of the ANY pointer is (LEN+7)/8. The range always begins with the IOPS bit of output address 0. Operation of CP as IO controller: In the case of gaps in the addresses, the corresponding IOPS bit is set to GOOD! Operation of CP as IO Device: Gaps in the addresses are not transmitted.
ADD_INFO	OUTPUT	WORD	I, Q, F, D, L	Reserved for additional diagnostics information.

Read/write record using FB 52 "PNIO_RW_REC"

FB 52 "PNIO_RW_REC" must be called in the user program of the Simatic S7 CPU, and permits the reading and writing of records on an IO Device when the CP is operated as an IO controller (Table 6.87). The function block can only execute one of the two functions at a time.

Table 6.87 Parameters of the FB 52 "PNIO_RW_REC"

Parameter	Declaration	Data type	Memory area	Description
CPLADDR	INPUT	WORD	I, Q, F, D, L, constants	Module start address from the configuration of the CP in HW-Config. The address must not be changed until a request has been completed.
WRITE_REC	INPUT	BOOL	I, Q, F, D, L, constants	FALSE: Read record TRUE: Write record The parameter must not be changed during the runtime of the function block.
ID	INPUT	WORD	I, Q, F, D, L, constants	Logical address of the IO Device (module). Bit 15: FALSE: Input/hybrid module TRUE: Output module With a hybrid module, the shorter of the two addresses must be specified.
INDEX	INPUT	WORD	I, Q, F, D, L, constants	Record number
DONE	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request running, or request completed with error. TRUE: Record transmitted successfully.

Table 6.87 Parameters of the FB 52 "PNIO_RW_REC" *(continued)*

Parameter	Declaration	Data type	Memory area	Description
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request running, or request completed error-free. TRUE: Request completed with error.
STATUS	OUTPUT	WORD	I, Q, F, D, L	Detailed information on execution of request (see below).

Alarm evaluation using FB 54 "PNIO_ALARM"

FB 54 "PNIO_ALARM" must be called in the user program of the Simatic S7 CPU, and permits evaluation of alarms when the CP is operated as an IO controller and if the parameter ADD_INFO ¦ 0 is in the FC12 "PNIO_RECV".

The alarms are passed on to the user program in the same sequence as they are signaled. However, older alarms which are invalid due to more recent ones, but which have not yet been signaled to the user program, are not deleted by the newer alarms (Table 6.88).

Table 6.88 Parameters of the FB 54 "PNIO_ALARM"

Parameter	Declaration	Data type	Memory area	Description
CPLADDR	INPUT	WORD	I, Q, F, D, L, constants	Module start address from the configuration of the CP in HW-Config. The address must not be changed until a request has been completed.
DONE	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request running, or request completed with error. TRUE: Alarm information transmitted successfully. If DONE = TRUE, the parameter NEW must be checked in addition.
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request running, or request completed without error. TRUE: Request completed with error.
NEW	OUTPUT	WORD	I, Q, F, D, L	FALSE: Request running, or no new alarm received. TRUE: New alarm received and acknowledged.
STATUS	OUTPUT	WORD	I, Q, F, D, L	Detailed information on execution of request (see below).
ID	OUTPUT	WORD	I, Q, F, D, L	Logical address of the IO Device (module). Bit 15: FALSE: Input/hybrid module TRUE: Output module With a hybrid module, the shorter of the two addresses must be specified.
LEN	OUTPUT	INT	I, Q, F, D, L	Length of the received alarm information (AINFO)
MODE	IN_OUT	DWORD	I, Q, F, D, L	Reserved

Table 6.88 Parameters of the FB 54 "PNIO_ALARM" *(continued)*

Parameter	Declaration	Data type	Memory area	Description
TINFO	IN_OUT	ANY VARTYPE: BYTE, WORD, DWORD	I, Q, F, D	Task information Destination range for the alarm administration information. The error OB start information (TINFO bytes 0...19) is mapped by the CP firmware as far as possible.
AINFO	IN_OUT	ANY VARTYPE: BYTE, WORD, DWORD	I, Q, F, D	Alarm information Destination range for supplementary header and alarm information: If the destination range is smaller than the length of the alarm information, the latter is truncated accordingly.

Specific return values of FC 11 "PNIO_SEND", FC 12 "PNIO_RECV", FB 52 "PNIO_RW_REC" and FB 54 "PNIO_ALARM"

The above-named functions/function blocks facilitate a detailed analysis of the cause of failure via the STATUS parameter. The individual meaning of the status values only differs marginally between the functions/function blocks. Table 6.89 lists possible status reports.

Table 6.89 Set of specific return values of FC 11 "PNIO_SEND", FC 12 "PNIO_RECV", FB 52 "PNIO_RW_REC" and FB 54 "PNIO_ALARM"

DONE/ NDR	ERROR	STATUS W#16#...	Description
FALSE	FALSE	8180	Data transfer/acceptance running, or CP is in the STOP state.
TRUE	FALSE	0000	Data transfer/accepted error-free. FB 54 "PNIO_ALARM": NEW = FALSE: No alarm data present. NEW = TRUE: Alarm data transmitted successfully, and alarm acknowledged.
FALSE	TRUE	8183	Profinet IO configuration missing or incorrect CPLADDR, or the CP is in the STOP state. In addition when operating the CP as IO Device: The connection between IO controller and IO Device is interrupted, the IO controller cannot be accessed, or the total lengths are inconsistent (configuration and LEN parameter).
FALSE	TRUE	8184	System error or illegal type of parameter.
FALSE	TRUE	8185	LEN parameter larger than the source range SEND, or destination range too small.
FALSE	TRUE	8F22	Area length error when reading a parameter (e.g. DB too short).
FALSE	TRUE	8F23	Area length error when writing a parameter (e.g. DB too short).
FALSE	TRUE	8F24	Area error when reading a parameter.
FALSE	TRUE	8F25	Area error when writing a parameter.
FALSE	TRUE	8F28	Alignment error when reading a parameter.
FALSE	TRUE	8F29	Alignment error when writing a parameter.

Table 6.89 Set of specific return values of FC 11 “PNIO_SEND”, FC 12 “PNIO_RECV”, FB 52 “PNIO_RW_REC” and FB 54 “PNIO_ALARM” *(continued)*

DONE/ NDR	ERROR	STATUS W#16#...	Description
FALSE	TRUE	8F30	Parameter located in write-protected 1st current data block.
FALSE	TRUE	8F31	Parameter located in write-protected 2nd current data block.
FALSE	TRUE	8F32	DB number in parameter is too large.
FALSE	TRUE	8F3A	Destination range is not loaded (DB).
FALSE	TRUE	8F42	Acknowledgment delay when reading a parameter from the I/O area.
FALSE	TRUE	8F43	Acknowledgment delay when writing a parameter to the I/O area.
FALSE	TRUE	8F44	Access to a parameter to be read during block processing is disabled.
FALSE	TRUE	8F45	Access to a parameter to be written during block processing is disabled.
FALSE	TRUE	8F7F	Internal error, e.g. illegal ANY reference.
FALSE	TRUE	8090	Module with this address does not exist.
FALSE	TRUE	80A0	Negative acknowledgment when reading from the module.
FALSE	TRUE	80A1	Negative acknowledgment when writing to the module.
FALSE	TRUE	80A3	General Profinet IO context management error.
FALSE	TRUE	80A9	IO Device or module signals an illegal type.
FALSE	TRUE	80B0	Module does not recognize the record.
FALSE	TRUE	80B1	The specified record length is incorrect, or the CP enters the STOP state.
FALSE	TRUE	80B4	IO Device or module signals access to an illegal area.
FALSE	TRUE	80B6	IO Device or module denies access.
FALSE	TRUE	80B8	The module signals an illegal parameter.
FALSE	TRUE	80C0	The record cannot be read.
FALSE	TRUE	80C1	The specified record is currently being processed.
FALSE	TRUE	80C2	There is a requests bottleneck.
FALSE	TRUE	80C3	Resources (memory) occupied.
FALSE	TRUE	80C4	Communications error (occurs temporarily; repetition in the user program is therefore appropriate).

6.4 Profinet CBA User Program Interfaces

The technological interface for communication between Profinet controllers is represented in Profinet CBA by an interface DB. A range of system functions for Simatic S7 systems allows consistent access to the interface DB and thus the reading and writing of the variables of this interface (Fig. 6.14).

In addition, the Profinet system library contains functions for simple integration of intelligent Simatic S7 Profibus devices into Profinet CBA configurations. All blocks relevant to Profinet CBA are listed in Tables 6.90 to 6.92.

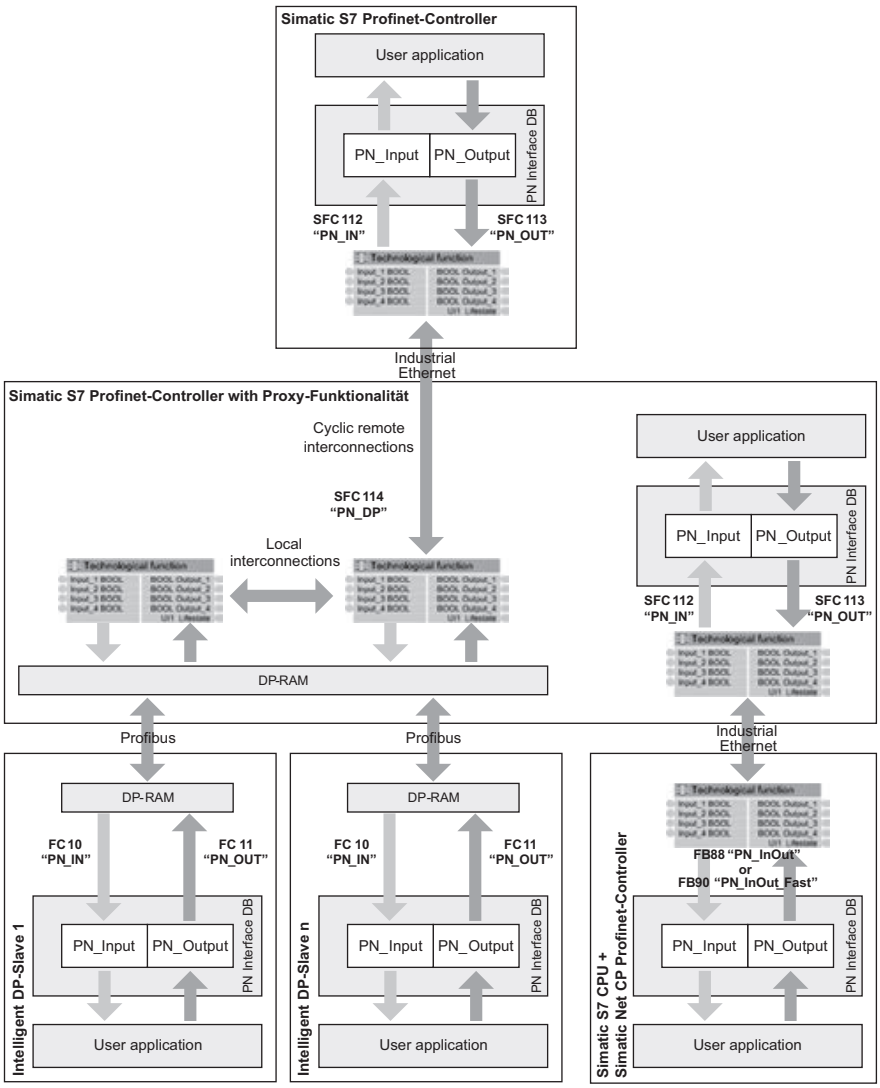


Fig. 6.14 Principle of operation of Profinet CBA functions with Simatic S7

This chapter provides an overview of the functions and interfaces of the user program of a Simatic S7 CPU which are significant to use of Profinet CBA.

6.4.1 Organization Blocks with Profinet CBA

All organization blocks can be basically used with Profinet CBA as previously. It is even essential for certain OBs to be present in the user program. However it is not necessary for these OBs to explicitly contain a fully programmed code. It is sufficient if the BE command (block end) is present as the only command in the OB. If these organization blocks are missing (Table 6.93), the corresponding device is

set to the STOP status when an error or alarm occurs.

The structure of the local data of the above-mentioned OBs is not changed when used with Profinet CBA.

Table 6.90
System functions for updating the interface DB in use with Simatic S7 Profinet controllers

System function	Description
SFC 112 "PN_IN"	Updating of all input values of the interface DB of a Profinet controller by the input values of its technological function. In order to use the SFC, the option "Updating the PN Interface" must be set to "via user program (Copy blocks)" when assigning the components.
SFC 113 "PN_OUT"	Updating of all outputs of the technological function of a Profinet controller by the output values in its interface DB. In order to use the SFC, the option "Updating the PN Interface" must be set to "via user program (Copy blocks)" when assigning the components.
SFC 114 "PN_DP"	Updating of all local and remote interconnections to the Profibus slaves of a Profinet CBA controller incorporated via a proxy. The functionality of the SFC 114 "PN_DP" is provided in Simatic S7 WinLC PN by the application. SFC 114 "PN_DP" is not supported there. In order to use the SFC, the option "Updating the PN Interface" must be set to "via user program (Copy blocks)" when assigning the components.

Table 6.91
Functions for updating the interface DB in use with Simatic Net CP as Profinet controller

Function block	Description
FB 88 "PN_InOut"	Exchange of data between the interface DB and the connection values of the technological function of a Simatic S7 CPU with Simatic Net Profinet CPs.
FB 90 "PN_InOut_Fast"	The functionality is basically the same as for the FB 88 "PN_InOut". But this function block is optimized for the use of designated S7-400 CPUs together with corresponding Simatic Net CPs.

Table 6.92 Functions and DBs for updating of the interface DB in use with Simatic S7 Profibus devices with programmable functionality

System function/ function block	Description
FC 10 "PN_IN"	Updating of all input values of the interface DB of a Profibus device by the input values of its technological function.
FC 11 "PN_OUT"	Updating of all outputs of the technological function of a Profibus device by the output values in its interface DB.
DB2 "PN_IO_DB"	Contains important information for copying data between the interface DB and the technological interface with Profibus slaves.

Table 6.93 OBs required for Simatic S7 Profinet controllers and DP slaves

OB	Function	Used in
82	Diagnostics alarm	Profinet controllers, Profibus devices
85	Program execution error	Profinet controllers as DP masters
86	Rack failure	Profinet controllers, Profibus devices

6.4.2 System Functions with Profinet CBA

Special blocks for updating the interface DB in the respective device have been developed for use of Simatic S7 CPUs with integral Profinet interface as Profinet controllers.

Whereas the user program directly accesses the variables of the interface DB by means of these blocks, the operating system of a Profinet controller updates the so-called Profinet interface when accessing by the communications partners takes place. The Profinet interface, also referred to as shadow memory, is administered by the operating system and is an exact likeness of the interface DB. Since the user program and communications partners cannot access the same memory areas, access conflicts at the inputs and outputs of the interface DB are prevented in this manner.

Matching between the interface DB and the Profinet interface takes place as standard at the cycle control point. However, it is possible to switch off this automatic

Fig. 6.15
Settings when assigning the components for updating of Profinet data by SFC 112/113/

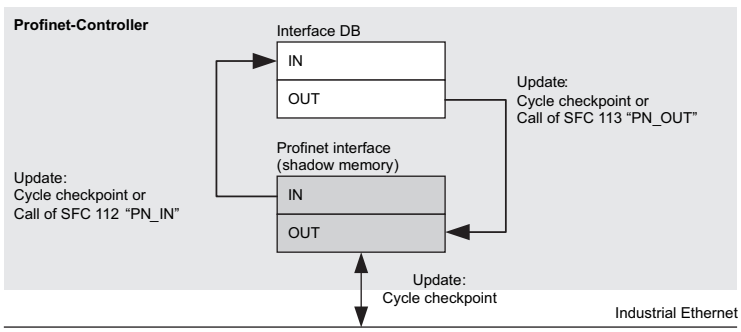


Fig. 6.16 Updating the Profinet interface

feature and to carry out the updating by calling the SFCs 112-114 in the user program, for example in order to influence the CPU's time response better (see Figures 6.15 and 6.16).

Updating of interface DB inputs using SFC 112 "PN_IN"

The system function must be called in the user program of the Profinet controller if the option "Automatic updating of the Profinet interface when assigning the components" has been deselected for the Profinet controller.

SFC 112 "PN_IN" copies the input data received by means of Profinet communication from the Profinet interface of the Profinet controller into the input area of the interface DB. Following completion of the SFC, the current input data are available in the user program (see Tables 6.94 and 6.95).

Table 6.94 Parameters of SFC 112 "PN_IN"

Parameter	Declaration	Data type	Memory area	Description
DBNO	INPUT	WORD	I, Q, F, D, L, constants	0: Updating of all interface DBs >0: Number of the interface DB
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC

Table 6.95 Specific return values of SFC 112 "PN_IN"

Error code W#16#...	Description
0000	No error has occurred.
8001	Invalid or missing Profinet CBA configuration.
8002	The number of the interface DB does not agree with the component configuration.
8004	The number of the interface DB agrees with the component configuration, but the interface DB is not loaded.
8006	The interface DB is write-protected in the CPU or has been compiled with the keyword UNLINKED.
80B1	Length error when reading or writing. The component configuration does not match the loaded interface DB.
8xyy	General error information corresponding to the general error codes of the RET_VAL parameter.

Writing of interface DB outputs to the Profinet interface using SFC 113 "PN_OUT"

The system function must be called in the user program of the Profinet controller if the option "Automatic updating of the Profinet interface when assigning the components" has been deselected for the Profinet controller.

SFC 113 "PN_OUT" copies the output data generated in the user program from the interface DB into the Profinet interface of the Profinet controller. Following completion of the SFC, the current output data are available at the outputs of the technological function of the device (Tables 6.96 and 6.97).

Table 6.96 Parameters of SFC 113 “PN_OUT”

Parameter	Declaration	Data type	Memory area	Description
DBNO	INPUT	WORD	I, Q, F, D, L, constants	0: Updating of all interface DBs >0: Number of the interface DB
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of SFC

Table 6.97 Specific return values of SFC 113 “PN_OUT”

Error code W#16#...	Description
0000	No error has occurred.
8001	Invalid or missing Profinet CBA configuration.
8002	The number of the interface DB does not agree with the component configuration.
8004	The number of the interface DB agrees with the component configuration, but the interface DB is not loaded.
8006	The interface DB has been compiled with the keyword UNLINKED.
80B1	Length error when reading or writing. The component configuration does not match the loaded interface DB.
8xyy	General error information corresponding to the general error codes of the RET_VAL parameter.

Updating of interconnections to Profibus devices using SFC 114 “PN_DP”

Except with Simatic WinLC PN, the system function must be called in the user program of the Profinet controller if the proxy function for Profibus devices is to be used for the controller and the option “Automatic updating of the Profinet interface when assigning the components” has been deselected. SFC 114 “PN_DP” updates:

- all local interconnections between the inputs and outputs of the technological functions of Profibus devices on the Profibus segment of a Profinet controller
- all cyclic remote interconnections to the inputs and outputs of the technological functions of Profibus devices on the Profibus segment of a Profinet controller.

The system function is executed asynchronously, i.e. processing may extend over several SFC calls. Updating of the interconnections is started by REQ=TRUE. The output parameters RET_VAL and BUSY indicate the request status (see Table 6.98). The request has been processed when all interconnections have been updated (Table 6.99).

Table 6.98 Parameters of SFC 114 “PN_DP”

Parameter	Declaration	Data type	Memory area	Description
REQ	INPUT	BOOL	I, Q, F, D, L, constants	TRUE: Triggering of updating request
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of the SFC
BUSY	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Updating finished TRUE: Updating running

Table 6.99 Specific return values of SFC 114 “PN_DP”

Error code W#16#...	Description
0000	The request has been carried out without errors.
7000	First call with REQ=FALSE. No updating of the interconnections is triggered. BUSY=FALSE.
7001	First call with REQ=TRUE BUSY=TRUE
7002	Intermediate call (REQ irrelevant). Updating of the interconnections has not been completed. BUSY=TRUE
8001	Invalid or missing Profinet CBA configuration.
8095	Further updating of the interconnections has been triggered in a higher priority class. However, updating is still in progress in the class of lower priority.
8xyy	General error information corresponding to the general error codes of the RET_VAL parameter.

6.4.3 Special Function Blocks and Functions with Profinet CBA

This section describes blocks for updating the input/output data of the interface DB of Simatic S7 CPUs which participate in the Profinet communication

- via a Simatic Net CP or
- as a Profibus device with programmable functionality.

The blocks are part of the Profinet system library.

Updating of the Profinet interface using FBþ88 “PN_InOut” or FBþ90þ“PN_InOut_Fast”

The function blocks transfer the data between the Profinet interface on a Simatic Net Profinet CP and the interface DB in the Simatic S7 CPU. They can be called more than once within a user program cycle.

The two function blocks are executed asynchronously, i.e. processing may extend over several user program cycles. A transfer request starts when the block is called, and ends when terminated by DONE=TRUE or ERROR=TRUE (see Tables 6.100 and 6.101). To guarantee data consistency, the inputs/outputs in the interface DB may only be modified or read following completion of the request (DONE=TRUE).

FBþ88 “PN_InOut” or FBþ90 “PN_InOut_Fast” have a practically identical response at the interface to the user program. However, FBþ90 “PN_InOut_Fast” can only be used with certain types of Simatic Net CPs of the S7-400 range. If the FBþ90 “PN_InOut_Fast” is permissible for the type of CP used, it is advisable to actually use it because shorter response times can be achieved than with the FBþ88 “PN_InOut”.

Table 6.100 Parameters of FBþ88 “PN_InOut” and FB 90þ“PN_InOut_Fast”

Parameter	Declaration	Data type	Memory area	Description
LADDR	INPUT	WORD	I, Q, F, D, L, constants	Module start address from the configuration of the Profinet CP in HW-Config. The address must not be changed until a request has been completed (DONE=1 or ERROR=1).
DONE	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request being executed or request completed with error. TRUE: Request completed without error.
ERROR	OUTPUT	BOOL	I, Q, F, D, L	FALSE: Request being executed or request completed without error. TRUE: Request completed with error.
STATUS	OUTPUT	WORD	I, Q, F, D, L	Detailed information on execution of request.

Table 6.101
Specific return values of FBþ88 “PN_InOut” and FBþ90þ“PN_InOut_Fast”

DONE	ERROR	STATUS W#16#...	Description
TRUE	FALSE	0000	Request completed without error.
FALSE	FALSE	0000	No request being processed.
FALSE	FALSE	8181	Request running. Only with FB 90: Establishment of connection to addressed module running.
FALSE	TRUE	8183	Only with S7-300: Request has not yet been started; acceptance of data is not yet possible.
FALSE	TRUE	8184	Faulty instance DB: Usually triggered by illegal writing of instance DB by the user program. Only with FB 90: Faulty send or receive request.
FALSE	TRUE	8085	Only with FB 90: Interface DB faulty.
FALSE	TRUE	8090	Only with S7-400: Parameterization error; an incorrect module address has been specified; the address points to an empty slot. Only with FB 90: In the following cases, the value 8181 h request running) is displayed in STATUS although no communication is taking place: – The address points to a slot which is occupied by a different type of module, or – The addressed module is not configured for Profinet CBA operation.
FALSE	TRUE	80A1	Only with FB 90: Communications error: – Station-internal connection to the addressed module is being canceled. – The quantity framework for CPU connections has been exceeded. – The interface is being reinitialized.

Table 6.101
Specific return values of FBþ88 “PN_InOut” and FBþ90þ“PN_InOut_Fast” *(continued)*

DONE	ERROR	STATUS W#16#...	Description
FALSE	TRUE	80B0	Only with S7-300: Block error: The record number is incorrect. This status can also occur during a restart or hot restart following power off/on.
FALSE	TRUE	80B1	Only with S7-300: Block error: The record length or offset is incorrect.
FALSE	TRUE	80B3	Only with S7-300: Parameter error: Incorrect CP address.
FALSE	TRUE	80C1	Only with S7-300: Temporary error: The specified record is currently being processed.
FALSE	TRUE	80C2	Only with S7-300: Temporary error: There is a congestion of requests; the record cannot yet be read.
FALSE	TRUE	80C3	Only with S7-300: Temporary error: Resources (memory) occupied.
FALSE	TRUE	80C4	Only with S7-300: Communications error: Occurs temporarily; repetition in the user program is therefore appropriate.
FALSE	TRUE	80D0	Only with S7-300: Configuration error: The maximum number of input and output data blocks has been exceeded, the interface DB is too large.
FALSE	TRUE	80D1	Only with S7-300: Configuration error: – The interface of the configured component does not agree with that used in the program (outputs). – An incorrect module has been inserted; the Profinet service is not supported.
FALSE	TRUE	80D2	Only with S7-300: Configuration error: – The interface of the configured component does not agree with that used in the program (outputs). – An incorrect module has been inserted; the Profinet service is not supported. – Parameter error: Incorrect CP address
FALSE	TRUE	8322 8623	Only with FB 90: The interface DB is faulty.
FALSE	TRUE	8332	Only with FB 90: The number of the interface DB is too large.
FALSE	TRUE	833A 863A	Only with FB 90: Access to the interface DB is not possible (e.g. because the interface DB has been deleted).
FALSE	TRUE	8Fyy 8xyy	General error information corresponding to the general error codes of the RET_VAL parameter.

The following also applies:

- The interface parameters of the two function blocks are identical.
- A number of additional displays are present in the STATUS parameter for the FBþ90 “PN_InOut_Fast”.
- There are device-specific differences in the quantity framework of the interface DB.

Updating of the interface DB of Simatic-S7 Profibus devices with programmable functionality using FC 10 “PN_IN” and FC 11 “PN_OUT”

FC 10 “PN_IN” copies the data coming from the Profinet controller from the I/O transfer area of the CPU into the inputs (PN_INPUT) of the interface DB.

FC 11 “PN_OUT” copies the outputs (PN_OUTPUT) of the interface DB into the I/O transfer area of the CPU.

The functions must be called in OB1 in the user program of a Profibus device: FC 10 “PN_IN” as the first call at the beginning, and FC 11 “PN_OUT” as the last call at the end of OB1 (see Tables 6.102 and 6.103).

Both functions are included in the Profinet system library in Step 7.

Table 6.102 Parameters of FC 10 “PN_IN” and FC 11 “PN_OUT”

Parameter	Declaration	Data type	Memory area	Description
DB_NO	INPUT	BLOCK_DB	DB	0: Updating of all interface DBs >0: Number of the interface DB
PN_InOut_DB	INPUT	BLOCK_DB	DB	Number of the data block containing the copy information.
RET_VAL	OUTPUT	INT	I, Q, F, D, L	Return value of FC

Table 6.103 Specific return values of FC 10 “PN_IN” and FC 11 “PN_OUT”

Error code W#16#...	Description
0000	No error has occurred.
8001	PN_InOut_DB is not yet filled in, i.e. the component has not been created, or has been incorrectly created, or an incorrect PN_InOut_DB has been parameterized.
8002	Incorrect PN_InOut_DB parameterized.
8003	A number has been specified at the input PN_InOut_DB which is too high for the PN_InOut_DB.
8004	The component must be created again or loaded again: – PN_InOut_DB not loaded or- Interface DB not loaded or – Incorrect PN_InOut_DB parameterized or- Inconsistent PN_InOut_DB.
8005	Number for interface DB is too high. Select a small number, and create the component again. Incorrect PN_InOut_DB parameterized.
8006	The interface DB is write-protected in the CPU.
8007 8008	Inconsistent component. The component must be created again.

Table 6.103 Specific return values of FC 10 “PN_IN” and FC 11 “PN_OUT” *(continued)*

Error code W#16#...	Description
8009	Error when reading the system status.
8010	Master at STOP or not accessible.
8022	Area length error when reading a parameter: inconsistent PN_InOut_DB. Create the component again.
8023	Area length error when writing a parameter: inconsistent PN_InOut_DB. Create the component again.
8030	The interface DB is write-protected in the CPU.
807F	Internal error: inconsistent PN_InOut_DB. The component must be created again.
808x	System error with external DP interface module.
8090	– No module has been configured for the specified logical base address, or – the limitation for the length of consistent data has not been observed, or – the start address in the LADDR parameter has not been specified in hexadecimal notation.
8093	A DP module from which consistent data can be read does not exist at the logical address specified by LADDR.
80A0 80A1	An access error has been detected when accessing the I/O. The master cannot be accessed.
80B0	Slave failure on external DP interface module.
80B1	The length of the specified destination range is not equal to the user data length configured with Step 7.
80B2 80B3	System error with external DP interface module.
80C0	The data have not yet been read by the module.
80C1	The data of the previous write request on the module have not yet been processed by the module.
80C2 80Fx 85xy 87xy	System error with external DP interface module.
8322	Area length error when reading a parameter (interface DB has been changed in the shadow project and than loaded into the CPU).
8323	Area length error when writing a parameter (interface DB has been changed in the shadow project and than loaded into the CPU).

7 Profinet Devices and Networking

Profinet's performance does not exclusively depend on the automation equipment but very much so on the environment in which it (the equipment) is used. This primarily includes a powerful communications network. The demands placed on this communications system in an industrial environment differ significantly from those for conventional office communication. This applies to almost all associated aspects such as active and passive network components, connected data terminals, network concepts and topologies, availability, data quantities and environmental conditions, to mention just a few. Table 7.1 lists the most important differences.

Table 7.1 Different requirements between office and industrial applications

	Office sector	Production and field sector
Installation conditions	Fixed basic installation in buildings	Largely plant-dependent cabling
	Routing in false floors	Plant-specific cable routing
	Variable device connection at the workstation	Connection points are rarely changed
	Precut/preassembled device cables	Device connections for field assembly
	Mainly standard workstations (desk with PC, ...)	Each machine/plant requires an individual degree of networking
	Tree network topologies	Frequently linear network topologies and (redundant) ring topologies
Transmission performance	Large data packets (e.g. pictures)	Small data packets (measured values)
	Medium network availability	Very high network availability
	Transmission time in seconds range	Transmission time in microseconds range
	Mainly acyclic transmission	High share of cyclic transmission
	No isochronous mode	Isochronous mode
Ambient conditions	Normal temperatures	Extreme temperatures
	Low dust load	High dust load
	No moisture	Moisture possible
	Hardly any vibrations	Vibrating machines
	Low EMC load	High EMC load
	Low mechanical danger	Danger of mechanical damage
	Low UV radiation	UV radiation outdoors
	Hardly any chemical danger	Chemical loading through oily or corrosive atmospheres

The different demands and conditions show that the cabling structures in the industrial sector must satisfy significantly higher demands than in the office sector. The installation guidelines for Profinet are oriented on the international ISO/IEC 11801 standard and on its European equivalent EN 50173. These standards define application-independent IT networking for application in commercial premises which may comprise individual buildings or several buildings on a site. Both standards assume that the buildings are used with conditions similar to offices. The specific requirements of a shop floor or a process engineering plant are not considered. Profinet is therefore based on international standards for the network installation sector, and abstains from the extra definition of standards. The appropriate standards for the sectors mainly associated with Profinet can be found in Chapter 7.10.8.

The Profinet cabling is oriented according to the ISO/IEC 11801 and EN 50173 standards. However, the industrial conditions of use necessitate components appropriate to the special environmental demands such as temperature, moisture, shock, vibration, EMC, dust and operation. The directive “Installation Guideline Profinet” of the PNO therefore defines industry-compatible cabling for Fast Ethernet on the basis of the fundamental IEC 11801 definitions. This provides detailed information and descriptions for the industrial sector as applicable to device and component manufacturers as well as installation engineers.

A Profinet network largely consists of active and passive network components. These are the hardware components of a network. The following chapter provides various background information concerning the structure of your Profinet communications network.

7.1 Passive Network Components

The components associated with the connection system (cables, plugs, sockets and cabinets) are referred to as passive components. These pass on a signal without actively influencing it. All other network components belong to the active components, and actively influence the signal. These particularly included hubs and repeaters, bridges, switches and routers.

7.2 Transmission Media in Line-based Electrical Networks

The Profinet transmission technology fundamentally corresponds to the Fast Ethernet standard with a full duplex data transfer rate of 100 Mb/s in a switched network. Transmission technologies with lower data transfer rates (10 Mb/s) do not satisfy the demands for transmission performance in automation systems. Collision-free data transmission and real-time properties cannot be guaranteed in slower networks. In Profinet networks, the line-based signal transmission is over symmetrical copper or fiber-optic cables. The following types of cable are suitable for transmission of electrical signals in Profinet:

- 100Base-TX: electrical transmission system at 100 Mb/s (Fast Ethernet) with two pairs of conductors
- 1000Base-TX: electrical transmission system at 1000 Mb/s (Gigabit Ethernet) with four pairs of conductors

The following types of fiber-optic cables are suitable for optical transmission of signals in Profinet:

- 100Base-FX: optical transmission at 100 Mb/s (Fast Ethernet) on two multimode or singlemode fiber-optic conductors. The wavelength used is 1310 nm.
- 1000Base-SX: optical transmission at 1000 Mb/s (Gigabit Ethernet) on two multimode fiber-optic conductors. The wavelength used is 850 nm.
- 1000Base-LX: optical transmission at 1000 Mb/s (Gigabit Ethernet) on two singlemode fiber-optic conductors. The wavelength used is 1310 nm.

Shielded cables and connection elements must be used without exception. A differentiation is made between fixed connections and removable connections. The removable connections are designed as RJ45 or M12 plug connectors. A device connection is always designed as a socket. The cables for the device connection (patch cables) are provided with plugs at both ends.

7.2.1 Electrical Signal Transmission with Profinet using 100Base-TX

Twisted copper cables (100Base-TX) are used for the electrical signal transmission at a rate of 100 Mb/s (Fast Ethernet) in full duplex mode. The transmission procedure for 100Base-TX is defined in the IEEE 802.3i/IEEE 802.3u standards of the Institute of Electrical and Electronics Engineers. The transmission medium is a symmetrical and shielded twisted-pair or star-quad copper cable with a characteristic impedance of 100 Ohm. The conductors are color-coded: conductor pair 1 is yellow/orange, and is used for sending. The white/blue conductor pair is used as the receive line. Twisted-pair connections are always point-to-point connections between a transmitter block and a receiver block. The transmission properties of this cable must comply with the requirements of CAT 5. The ISO/IEC 11801 standard defines cables/categories for classification of twisted cables. Ethernet cables are mainly characterized by two parameters: the cable category and the channel class. The various categories specify certain transmission characteristics of the TP cables such as impedance, bandwidth, attenuation and near-end crosstalk. A total of five categories (1, 2, 3, 4 and 5) are defined and standardized. The transmission properties improve as the category increases. The characteristic impedance is 100 Ohm. The maximum connection length between data terminal and network component or between two network components (e.g. switch ports) must not exceed 100 m. To guarantee the transmission properties, the transmission link should consist of just one section of cable. In special cases (e.g. use of two cabinet inlets), the transmission link may consist of up to three sections.

The connections are usually made with an RJ45 plug system with securing collar (see Chapter 7.2.5). The securing collar together with the hood provide a close fitting and locking with the IE FC RJ45 Plug 180 conforming to Profinet, resulting in

Table 7.2 Contact and conductor assignments

Signal	Function	Conductor color	Contact assignment in the RJ45 connector	Contact assignment in the M12 connector
TD +	Transmission data +	Yellow	1	1
TD -	Transmission data -	Orange	2	3
RD +	Receiver data +	White	3	2
RD -	Receiver data -	Blue	6	4

Table 7.3 Profinet standards for electrical transmission

Property	Value
Standard	IEC 61158
Cable sort	2-pair, symmetrical and shielded copper cable
Cable type	100Base-TX, CAT 5
Characteristic impedance	100
Transmission rate	100 Mb/s
Max. segment length	100 m
Max. number of sections	3
Connections	RJ45 plug connector, M12 plug
Maximum number of connections	6 pairs of plugs/sockets per connection

a rugged, industry-compatible station connection offering relief of tension and bending on the RJ45 socket. This is an 8-pole connector system whose structure complies with ISO/IEC 8877:1992. A maximum of six pairs of plugs/sockets are permissible per connection. For example, two pairs of plugs/sockets are required for a control cabinet inlet. The contact assignments of the RJ45 are compatible with the Ethernet standard, i.e. compatible with ISO/IEC 8802-3. It should be ensured that devices only envisaged for use within the control cabinet are always equipped with the RJ45. Alternatively, the M12 plug connector can be used for the IP65/67 degree of protection (see Chapter 7.2.7). This 4-pole M12 plug connector has D-coding. The contact assignments on the data terminal and the color coding of the cable are specified in Table 7.2.

The most important values for the electrical signal transmission are summarized again in Table 7.3 for improved clarity.

7.2.2 1000Base-TX

The 1000Base-TX standard (Gigabit Ethernet) is available for future Profinet applications. This standard is characterized as follows:

- The **transmission rate** of the electrical ports is 1 Gb/s.
- The **transmission procedure** for 1000Base-TX is defined in the IEEE 802.3ab standard. Autonegotiation is optional with 1 Gb/s. Two communications procedures are possible: half duplex and full duplex.

- **Transmission medium**: data transmission is carried out on an eight-core twisted-pair cable. A Cat 6 (4×2) twisted-pair cable is required for data transmission at 1 Gb/s. With Cat 5 (2×2) cables, only a maximum transmission rate of 100 Mb/s is possible. If two ports with Gigabit capability are connected together using a Cat 5 (2×2) cable, both ports must be set to 100 Mb/s and full duplex modes. A crossed TP cable is additionally required in this case.
- The maximum **transmission range** (segment length) is 100 m.
- The **connection** is made using an 8-pole RJ45 socket.

7.2.3 Technical Implementation – FastConnect

The technical implementation of the Profinet standard described uses cables and systems which correspond to the standard and are certified. An option is the FastConnect (FC) system for the Industrial Ethernet of Simatic Net which has been developed further for Profinet. This system makes the structured cabling of the office sector industry-compatible for use on the shop floor. FC cables can be assembled rapidly and easily on site. Industrial Ethernet FC establishes the connection of the RJ45 system environment to the rugged installation systems used in industrial environments. Significant time and cost savings together with a reduction in the sources of error during installation are some of the advantages of the IE FC system. The components of Industrial Ethernet FC are:

- IE FC Cable 2 × 2 Cat5 Plus: certified fast assembly cables with copper conductors
  (IE FC Standard Cable, IE FC Trailing Cable, IE FC Marine Cable).
- IE FC RJ45 Plug: this plug has a compact and rugged design, and allows use of the FC RJ45 Plug in industrial environments and on devices from the office sector.
- IE FC RJ45 Modular Outlet for connecting the RJ 45 system to the installation system in the industrial environment, provided with insulation displacement contacts.
- IE FC Stripping Tool, a preset tool for removal of insulation.
- IE TP Cords: precut/preassembled connecting cables with RJ45 plugs on both ends.

These matched components permit connection of the installation cables in compliance with the standard within just a few minutes. Data terminals or network components can be connected in the control cabinet or in a control room to the FC Outlet RJ45 using various precut/preassembled patch cables (cords) with RJ45 connection system (Fig. 7.1). In the field, the IE FC Standard Cable is then used for connecting further stations or outlets.

Possible system configurations are presented in Chapter 7.2.11.

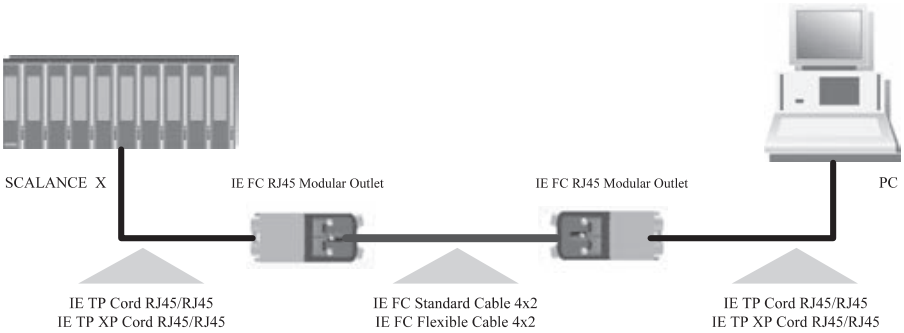


Fig. 7.1
The FastConnect system: a data terminal (Scalance X) is connected to a Modular Outlet using preassembled Cords. The Outlets are connected using IE FC cables.

7.2.4 Bus Cables for Fast Assembly – IE FC Cables

The Industrial Ethernet FastConnect cables 2×2 have a radially symmetric design with 100 Ω characteristic impedance for structured cabling on the shop floor and have a special design for fast assembly. They permit use of the FastConnect Stripping Tool with which an exact length of the outer sheath and braided shield can be removed in one working step, permitting fast and easy connection of the IE FC Outlet RJ45 and the IE FC RJ45 plugs. As a result of the double shielding, these cables are particularly suitable for routing in industrial environments with electromagnetic interferences. Simple connection to the insulation displacement contacts of the FC RJ45 Plug is possible without the need for special tools. A uniform grounding concept can be implemented by means of the external shield of the bus cable and the grounding concept of the IE FC Outlet RJ45. The FC TP Standard Cable contains solid conductors, the FC TP Trailing Cable and the FC TP Marine Cable have stranded conductors. These cables are all better than category 5 (Cat 5e) of the international ISO/IEC 11801 and EN 50173 cabling standards, and therefore conform completely with Profinet (Fig. 7.2).

Shielded TP installation cables for connection to Industrial Ethernet FC Outlet RJ45 / FC RJ45 Plug are available for designing Industrial Ethernet networks (4-core). The cables conform with Profinet and have been assigned UL approval.

Fig. 7.2
FC cables: IE FC 2 × 2 Standard Cable, IE FC 4 × 2 Standard Cable, IE FC 2 × 2 Trailing Cable, IE FC Hybrid Cable

The IE FC Cable 4 × 2 is suitable for 8-core cabling which permits two Industrial Ethernet connections for Fast Ethernet with 100 Mb/s to be routed in one cable. At the same time, this cable can be expanded to Gigabit technology with transmission rates of 100 or 1000 Mb/s with Ethernet, which requires eight cables. Different types of cable are available for the various applications:

- **IE FC Standard Cable GP 2×2 (type A):** standard bus cable with solid conductors and special design for fast assembly; four solid conductors are twisted into a star-quad.
- **IE FC Standard & Flexible Cable GP 4×2** for design of an 8-core cabling system with Gigabit capability. As a result of the 8-core cabling, two Industrial Ethernet connections can be currently implemented, and future capability is provided for upgrading to a Gigabit Ethernet connection.
- **IE FC Flexible Cable GP 2×2 (type B):** flexible bus cable for special applications requiring occasional movement; four conductors (stranded) are twisted into a star-quad.
- **IE FC Trailing Cable GP 2×2 (type C):** highly flexible bus cable for special applications requiring permanent movement, e.g. with permanently moving machine components; four conductors (stranded) are twisted into a star-quad.
- **IE FC Torsion Cable GP 2×2 (type C); IE FC Torsion Cable 2×2:** highly flexible bus cable for special applications requiring permanent movement, e.g. with robots; stranded conductors.
- **IE FC Marine Cable 2×2:** bus cable for special use on ships; four conductors (stranded) are twisted into a star-quad, halogen-free and certified for marine engineering.
- **IE FC Hybrid Cable:** flexible bus cable for providing a station with communication lines (2×2) and power supply lines (2×2) for simultaneous application of data and power to field devices. Power transmission is separate, and only depends on the cable cross-section and length.

7.2.5 IE FC RJ45 Plugs

The Industrial Ethernet FC RJ45 Plugs permit fast and simple assembly of Industrial Ethernet FastConnect installation cables 2×2 (4-core twisted-pair cables) in industrial environments and to equipment from the office sector. They permit connection of an Industrial Ethernet FC cable to data terminals and network components. The plugs have a rugged, industry-compatible metal enclosure which optimally protects the data communication from interferences. Using the IE FC RJ45 Plugs, direct point-to-point connections (100 Mb/s) can be established for Industrial Ethernet between two data terminals or network components up to 100 m without patch cords. The Industrial Ethernet FC RJ45 Plug is available in two designs (Fig. 7.3):

- With 180° (straight) cable outlet
- With 90° (angled) cable outlet (for ET 200S).

Fig. 7.3
IE FC Plugs: 90° version, 180° version

All plugs comply with the EN 50173 (RJ45)/ISO IEC 11801 standard. As a result of the compact design, the connectors (IE FC Plug 180°) can be used both on devices with single sockets and on those with multiple sockets (blocks). Crossed lines can be produced by swapping the send and receive pairs in a plug.

As a result of the four integral insulation displacement contacts, connection of the FC versions is simple and error-free. The stripped end of the cable is inserted into the opened barrel contacts, and these are subsequently pressed down to provide secure conductor contacts. With the enclosure open, color codes on the contact cover facilitate simple connection of the conductors to the contacts. Users can check the contacts they have made through the transparent plastic cover.

Fig. 7.4
The securing collar concept provides close fitting and locking

Data terminals with an additional securing collar on the enclosure provided additional strain relief for the connector and the installation cable. The securing collar with its close fitting and locking with the IE FC RJ45 Plug 180 guarantees rugged and industry-compatible connection of the station, offering strain and bending relief for the twisted-pair socket (Fig. 7.4).

7.2.6 Hybrid Connector

Distributed field devices with IP 67 degree of protection frequently require the connection of both data cables and a 24-V supply. The RJ Industrial Hybrid Connector for Ethernet networks combines data conductors and power supply in one

Fig. 7.5
Hybrid connector with combined RJ45 data plug and 4-pole power supply

cable. However, the data and power supply are clearly separated from one another in the connector geometry. This means that the costs for installation and industry-compatible field devices with hybrid cabling are significantly reduced.

An RJ45 with FastConnect is integrated as the data connector in the plug. The four 24-V contacts are also designed as FastConnect. This design means that it is possible to connect a shielded Ethernet cable in combination with four conductors with a cross-section of 1.5 mm^2 to a plug connector without special tools (Fig. 7.5). The hybrid connector is used, for example, in Scalance W modules (Chapter 7.4) for supply of data and power.

7.2.7 M12 Connector

The RJ45 connector is frequently used in office applications as the Ethernet connection (round plug connector with 12-mm thread diameter). The M12 connector with IP 67 degree of protection specified by the PNO for use in harsh industrial environments is a connector which is already widely used in industry and has been proven as a reliable version for connecting sensors/actuators and for data transmission. The 4-pole M12 connector with IP65 protection has a D-coding. This M12 connector appropriate for data transfer is standardized in IEC 61076-2-101. Sockets are used on the device side, the cables are fitted with plugs. The advantage of the round design is certainly the simple sealing to comply with the IP67 degree of protection (Fig. 7.6). A disadvantage with this connector compared to the RJ45 solution is that it is more difficult to handle and requires more space.

Fig. 7.6
M12 connector

7.2.8 IE FC Outlets

The IE FC Outlets are used for the transition from the 4-core or 8-core Industrial Ethernet FC cables 2×2 or 4×2 to precut/preassembled TP Cords using RJ45 sockets. A patch cable with RJ45 plugs is connected to one side of the Outlet, and the industry-compatible IE FC cable to the other. With the enclosure open, color codes on the contact element facilitate connection of the individual conductors to the insulation displacement contacts. The FC Stripping Tool is used for assembly.

The Outlets are available in two versions:

- IE FC Outlet RJ45: for 4-core Industrial Ethernet FC cables for a Fast Ethernet connection with 100 Mb/s.
- IE FC RJ45 Modular Outlet: for 8-core Industrial Ethernet FC cables for two Fast Ethernet connections with 100 Mb/s or a Gigabit connection with 1000 Mb/s.

The FC Outlet RJ45 with rugged metal enclosure is secured on a DIN rail or mounted directly in the field. Multiple connections and patch blocks are implemented by combining several Outlets. Color coding prevents faults when connecting the conductors. The FC Outlet RJ45 corresponds to Category 5 of the ISO/IEC 11801 and EN 50173 international cabling standards. It is connected directly to the FC TP cable. Various precut/preassembled RJ45 patch cords are available for the connection between FC Outlet RJ45 and network component or data terminal. Several Outlets are combined into blocks, the so-called patch blocks. These patch blocks handle the function of a terminal block.

The IE FC RJ45 Modular Outlet is used for the transition from the 8-core Industrial Ethernet FC cables 4×2 to precut/preassembled TP Cords using RJ45 sockets. A patch cable with RJ45 plugs is connected to one side of the Outlet, and the industry-compatible IE FC cable to the other. The 8-core cabling system with Outlets permits transmission rates of 10, 100 and 1000 Mb/s with Ethernet and with the service-independent cabling from the office sector. As a result of the 8-core ca-

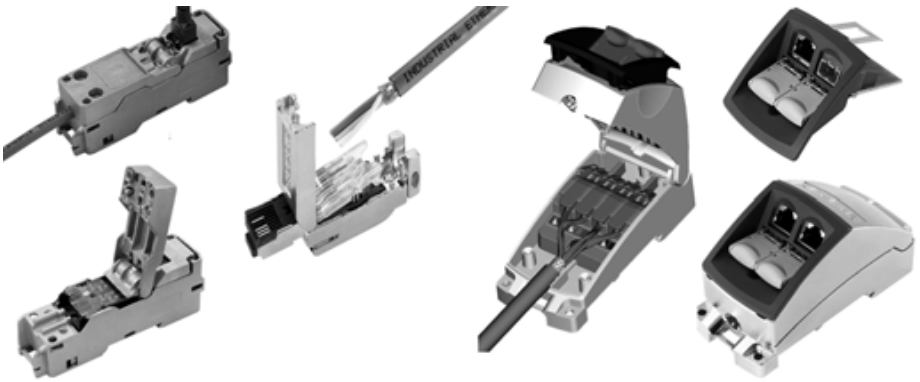


Fig. 7.7
IE FC Outlet RJ45, IE FC RJ45 Modular Outlet (opened);
top: Power Insert, bottom: IE FC RJ45 Modular Outlet with Insert 2FE

bling, two Industrial Ethernet connections can be implemented for Fast Ethernet. In addition, it is also possible to upgrade to a Gigabit Ethernet connection in the future. The transition from the 4-core Industrial Ethernet FC TP cabling system to the 8-cable system with Gigabit capability is thus implemented. By replacing the Modular Outlet Insert, it is possible to convert from network structures operating with transmission rates of 100 Mb/s to those with transmission rates of 1000 Mb/s. The FC RJ45 Modular Outlet basic module can be equipped with three different inserts (Fig. 7.7):

- IE FC RJ45 Modular Outlet Insert 2FE with 2 x RJ45 sockets for 100-Mb/s systems
- IE FC RJ45 Modular Outlet Insert 1GE with 1 x RJ45 socket for 1000-Mb/s systems
- IE FC RJ45 Modular Outlet Power Insert with 1 x 24 V, 1 x RJ45 socket for Scalance W industrial and IWLAN system.

7.2.9 FastConnect Stripping Tool

The Industrial Ethernet FastConnect Stripping Tool (IE FCS) is the stripping tool for the IE FC cables. It can be used to remove the exactly required lengths of outer sheath and shield on the FC cables in one operation as a result of the exactly preset cutting depths and distances of the knives. Sources of error resulting from inexact stripping of the cable when assembling the Outlets are thus eliminated. The Stripping Tool can be used to connect the IE Outlet RJ45 and the IE FC RJ45 Plug complying with Profinet rapidly and without problem to the Industrial Ethernet FC cable (Fig. 7.8).

Fig. 7.8
IE FC Stripping Tool: the cable is inserted, the sheath slit around the circumference, and the appropriate lengths stripped off

7.2.10 IE TP Cords

IE TP Cords are used to connect data terminals with RJ45 connection to the Industrial Ethernet FC cabling system. These so-called patch cables are factory-tested, and are available as precut/preassembled cables with 2×2 cores for 10 or 100 Mb/s and 4×2 cores for 10, 100 and 1000-Mb/s Ethernet with an RJ45 plug at each end. They are designed for use in an environment with a low EMC load, for example in

offices or inside control cabinets. The flexibility of the patch cables permits easy assembly. The cables correspond to Category 5e (2×2) and Cat 6 (4×2) of the ISO/IEC 11801 and EN 50173 international cabling standards.

A maximum of 10 m Twisted Pair Cord may be inserted between two devices. In the case of structured cabling with two TP Cords, this length must be distributed between the two patch cables.

Color-coded RJ45 connectors serve to distinguish crossed and non-crossed cables (crossed: RJ45 plugs red at both ends; non-crossed: RJ45 plugs green at both ends).

The IE TP Cords are available as precut/preassembled cables in the following versions:

- IE TP Cord RJ45/RJ45 with 2 × RJ45 plugs
- IE TP XP Cord RJ45/RJ45 with 2 × RJ45plugs, crossed send and receive lines.

7.2.11 System Configurations in Electrical Networks with Outlets

The following example indicates a number of different possibilities of how you can design your Profinet with the presented cabling structures (see also Fig. 7.9).

A Scalance X400 Switch is used as distributor. The following connections have been implemented as examples:

- Scalance X400 Switch > IE TP Cord > three-fold IE FC Outlets RJ 45 > 1 × 100-Mb/s connection with IE FC Standard Cable 2×2 > IE FC Outlet RJ 45 > IE TP Cord > S7-400
- Scalance X400 Switch > IE TP Cord > three-fold IE FC Outlets RJ 45 > 1 × 100-Mb/s IE connection with FC Standard Cable 2×2 > IE FC Outlet RJ 45 > IE TP Cord > OP Panel
- Scalance X400 Switch > IE TP Cord > three-fold IE FC Outlets RJ 45 > 1 × 100-Mb/s IE FC connection with Standard Cable 2×2 > IE FC Outlet RJ 45 > IE TP Cord > S7-300
- Scalance X400 Switch > IE TP Cord + 24 V DC > IE FC RJ 45 Modular Outlet with Power Insert > 1 x 100-Mb/s and power connection with IE FC Hybrid Cable > IE FC RJ 45 Modular Outlet with Power Insert > IE TP Hybrid Cable > Scalance W788-1 PRO
- Scalance X400 Switch > IE TP Cord > IE FC RJ 45 Modular Outlet with 1 GE (Gigabit Ethernet) > 1 × 1000-Mb/s connection with IE FC Standard 4×2 Cable > IE FC RJ 45 Modular Outlet with 1 GE (Gigabit Ethernet) > IE TP Cord > PC
- Scalance X400 Switch > 2 × IE TP Cord > IE FC RJ 45 Modular Outlet with 2 FC (2 × Fast Ethernet) > 2 × 100 Mb/s connection with IE FC Standard 4×2 Cable > IE FC RJ 45 Modular Outlet with 2FC (2 × Fast Ethernet) > 2 x IE TP Cord > 2 × S7-300

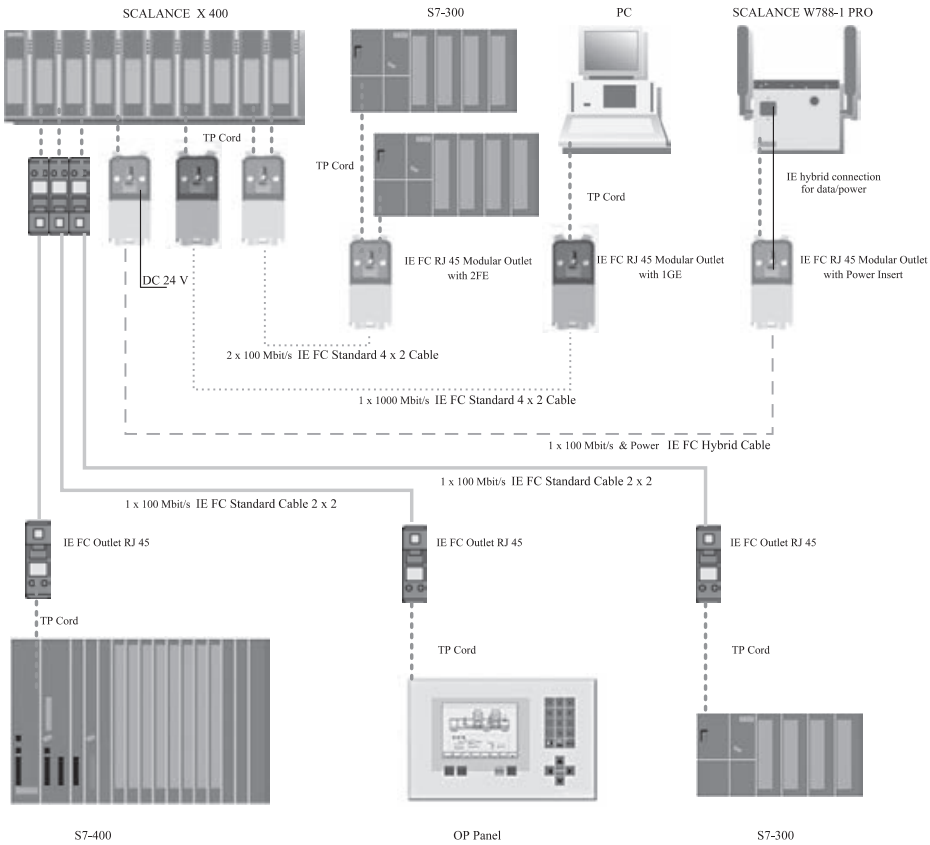


Fig. 7.9 Possible configurations in electrical networks with Outlets

7.3 Optical Signal Transmission

Particularly for fast connections with 100 Mb/s and 1000 Mb/s over large distances, the data are transmitted as light pulses through a glass-fiber (fiber-optic) cable. In factories and in the vicinity of large machines, fiber-optic cables are the best (and frequently the only) possibility for establishing a reliable Profinet, since the light is absolutely insensitive to any type of electromagnetic field. The glass fiber is also immune to differences in potential, as occur for example between different sections of buildings, since no conducting components exist which could have a detrimental effect on signals. Furthermore, the plug connectors exhibit great advantages compared to conventional copper systems since aging problems with metal oxidation and transfer resistances are completely absent in this case.

In addition, the use of fiber-optic (FO) cables permits greater distances to be covered since the signal attenuation of an FO cable is significantly lower than that of a copper cable. This means that the length restrictions of copper cabling can be exceeded.

Further advantages of the FO system:

- Electromagnetic interferences do not exist. External electrical or magnetic fields do not interfere at all with data transmission, not even if an FO cable is routed parallel to a power cable. Therefore fiber-optic cables are particularly suitable for data transmission in electromagnetically contaminated rooms such as a machine hall. Electrical isolation exists between the stations and segments. Unnoticed damage to the fibers is practically impossible.
- The bandwidth of an FO cable is far greater than that of a copper cable. The transmission rates can be extended almost without limit as a result of several carrier waves with different wavelengths (color spectrum).
- No lightning protection elements are necessary.
- Lower weight than copper cable.
- Highly resistant to tapping since listening in is only possible with complex technical equipment.
- The signal attenuation is much less than with a copper cable. This means that very large distances, up to several hundred kilometers, can be covered.
- Fiber-optic cables are resistant to tapping since listening in is only possible with complex technical equipment.
- It is practically impossible for fiber damage to go unnoticed.
- No crosstalk (unintentional signal interference on adjacent fibers).
- No radiated emission along the cable.
- Fiber-optic cables are not influenced by electric or electromagnetic interference fields.
- No grounding necessary.
- Can be routed in hazardous areas (no generation of sparks).
- It is possible to transmit signals on components at high potential, for example with high-voltage DC transmission systems.
- Low weight.
- Simple routing.

Of course, optical signal transmission also has a number of disadvantages:

- Increased assembly requirements.
- Connector technology (contamination, adjustment).
- Relatively sensitive to mechanical stress.
- More expensive equipment.
- Complex measuring technology.
- No 90° angles possible.

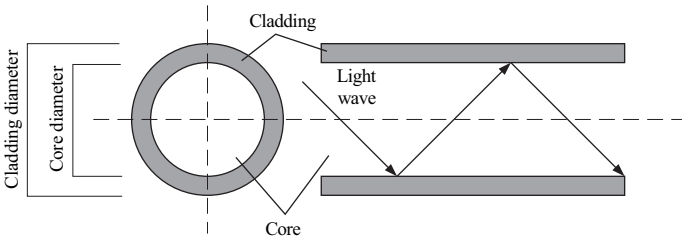


Fig. 7.10 The light wave transmitted through the core of the fiber-optic cable is reflected by the edges of the core

A fiber-optic cable comprises a cylindrical core and a cladding. The inner core of a glass-fiber cable consists of a special semiconductor material (Fig. 7.10) which is nowadays either glass (usually quartz glass) or plastic. The internal conductor (fiber) is usually enclosed by cladding which only serves to protect the cable from mechanical stress. In addition, a lacquer is present between the cladding and the outer coating of a fiber-optic cable in order to protect the fiber against moisture. The optical transmission of information on fiber-optic cables takes place according to the principle of total internal reflection. The optically-conducting core is surrounded by an optically thinner cladding at whose surface the light is completely reflected and thus routed through the cable.

The technology applied means that only point-to-point connections can be established using fiber-optic cables, i.e. a transmitter is connected to only one receiver. Therefore two fibers are required to link two stations (one for each transmission direction). In practice, this means: a direct line always exists from one network component to a port of a further network component. The task of a network component is to regenerate and distribute received signals by connecting the data to output ports again. This task is handled in the optical Profinet network by the Scalance X switches with optical ports.

7.3.1 100Base-FX

In the case of optical signal transmission, optical fibers are used through which light pulses are directed. The 100Base-FX standard (ISO/IEC 8802-3u), fiber-optic with multimode cables of 50/125 µm (ratio between core diameter/outer diameter) and 62.5/125 µm, is used with Profinet. The actual transmission medium is a two-fiber cable made of glass fibers or plastic through which the light pulses are directed. Data transmission is carried out using multimode or singlemode FO cables. The wavelength is always 1310 nm. Two types of FO cables can be used:

- **Multimode FOC:** the core diameter is 50 µm, the light source is an LED. Many modes (light beams) are used for the signal transmission. The differences in propagation times of the light pulses (dispersion) result in a greater limitation in the maximum range.
- **Singlemode FOC:** the core diameter is 9 or 10 µm, the light source is a laser diode. Only one mode (light beam) is used for the signal transmission, resulting

Table 7.4 Summary of the Profinet standard for optical transmissions

Property	Value
Fiber type	Multimode glass fiber
Cable sort	2-fiber cable
Cable type	100Base-FX, CAT 5
Fibers	50/125 µm and 62.5/125 µm
Largest permissible loss per section (at 1310 nm)	11 dBm with 50/125 µm 6 dBm with 62.5/125 µm
Transmission rate	100 Mb/s
Minimum modal bandwidth	500 MHz·km
Max. segment length	Multimode FOC: 3000 m Singlemode FOC: 26 km
Connections	SC-D BFOC/2.5 according to IEC 60874-10
Maximum number of connections	Always point-to-point connection

in a significantly lower dispersion. Therefore the maximum range with a singlemode FOC is greater than with a multimode FOC. The outer diameter of the FOC is 125 µm independent of the type used.

The optical transmission rate is 100 Mb/s. As a result of the technology used, only point-to-point connections can be established using fiber-optic cables, i.e. one sender is only connected to one receiver. Therefore two fibers are required for linking two stations (one for each transmission direction). This means that one direct line is always connected from a network component to a port of another network component.

The maximum length of the connection between data terminal and network components, or between two network components (e.g. switch ports), depends on the fiber-optic cable selected. The range with Simatic fibers for 100Base-FX and multimode FOC is 3 km and for 100Base-FX-LD and singlemode FOC 26 km. The connection is made using BFOC/2.5 sockets according to IEC 60874-10 or SC plugs according to IEC 874-19.

7.3.2 1000Base-SX and 1000Base-LX

As with electrical transmissions, the Profinet standard intends to use Gigabit connections 1000Base-SX (wavelength 850 nm) and 1000Base-LX (wavelength 1310 nm) for future applications. This standard is characterized as follows:

- The **transmission rate** of the optical Gigabit ports with 1000Base-SX and 1000Base-LX is 1 Gb/s.
- The **transmission procedure** for 1000Base-FX and 1000Base-LX is defined in the IEEE 802.3z standard, and set to a transmission rate of 1000 Mb/s and the full duplex procedure.
- **Transmission medium**: data transmission according to 1000Base-SX is carried out on a multimode FOC. The wavelength is 850 nm. The core diameter of the

multimode FOC is 50 µm, the light source is an LED. Many modes (light beams) are used for the signal transmission. The differences in propagation times of the light pulses (dispersion) result in a greater limitation in the maximum range. Data transmission according to 1000Base-LX is carried out on a singlemode FOC. The wavelength is 1310 nm. The core diameter of the singlemode FOC is 9 or 10 µm, the light source is a laser diode. Only one mode (light beam) is used for the signal transmission, resulting in a significantly lower dispersion. The maximum range with a singlemode FOC is therefore greater than with a multimode FOC.

- The maximum **transmission range** (segment length) when using Simatic Net multimode FOC with SC duplex connectors is 750 m with 1000Base-SX, or 10 km with 1000Base-FX and a singlemode FOC.
- The **connection** is made using SC duplex sockets.

7.3.3 Fiber-optic Cables – Designed for Industry

Various types of fiber-optic cables (FOC) are available from the Simatic Net product range for industrial applications (see Fig. 7.11):

- **Fiber-optic standard cable:** universal cable for indoor and outdoor use. It contains two multimode graded index fibers of type 62.5/125 µm and is available sold by the meter up to 4000 m or precut/preassembled with four BFOC plugs in lengths up to 1000 m.
- **Indoor fiber-optic cable**: the halogen-free, crush-proof and non-flammable FOC is designed for use in buildings. It contains two multimode graded index

Fig. 7.11
Various fiber-optic cables for industrial applications: standard cable, trailing cable and marine duplex cable (from left to right)

fibers of type 62.5/125 µm and is precut/preassembled with four BFOC plugs in length intervals of 0.5 m up to 100 m.

- **Flexible fiber-optic trailing cable:** this FOC has been designed for special applications requiring permanent movement, e.g. with permanently moving machine components. The trailing cable can be used indoors or outdoors. It contains two multimode graded index fibers of type 62.5/125 µm. Integral dummy elements guarantee a round conductor cross-section.
- **SIENOPYR marine duplex fiber-optic cable:** this hybrid cable with two FOCs and two additional copper conductors is designed for fixed routing on ships and in offshore units in all rooms and on exposed decks. It contains two multimode graded index fibers of type 62.5/125 µm. In addition, it contains two stranded, rubber-insulated copper conductors with a cross-section of 1 mm^2. These can be used e.g. for power supply to connected devices. The round cross-section of the cable facilitates sealing of cable inlets.

Various types of plastic fiber-optic cables are also available. Plastic fiber-optic cables are used for bus systems in automation engineering and in machine and plant construction when high safety requirements exist for the data transmission, when space is limited, and for short transmission links (up to 50 meters).

Plastic fiber-optic cables (POF, Polymer Optical Fiber) are rugged, round cables with a green outer coating and Kevlar strain relief elements as well as two plastic fibers with a rugged polyamide inner cladding. They are designed for indoor/outdoor applications with cable lengths up to 50 m. In this case, both the fiber core and the cladding are made of plastic. Decisive advantages of plastic fiber-optic cables compared to those of glass are higher flexibility (high alternating bending stress capacity with small bending radii) as well as cheaper connection and transmission technology. Furthermore, this type of fiber also exhibits all significant advantages of a fiber-optic connection: high EMC, reliable electrical isolation, no crosstalk, low weight etc. The cables are suitable for assembly in the field. The following Simatic Net cables are available:

- POF Standard Cable GP (General Purpose) for indoor and outdoor applications
- POF Trailing Cable.

7.3.4 FO Plug Connections and Permanent Connections

The optical interfaces of Profinet devices must comply with the ISO/IEC 9314-3 (for multimode fibers) and ISO/IEC 9314-4 (for singlemode fibers) standards. Removable and permanent connections are available for optical cables. Various plug connections are offered for a removable connection, whereas permanent connections are always made by “splicing” two fibers. Splicing is mainly used to extend fiber-optic cables or to repair breakages. A professional splicing connection should exhibit a low attenuation (low optical loss) and be stable. Plug connectors for FOCs should only be assembled by trained personnel using special tools. Correct assembly results in a very low insertion loss and high repeatability even after several plugging cycles.

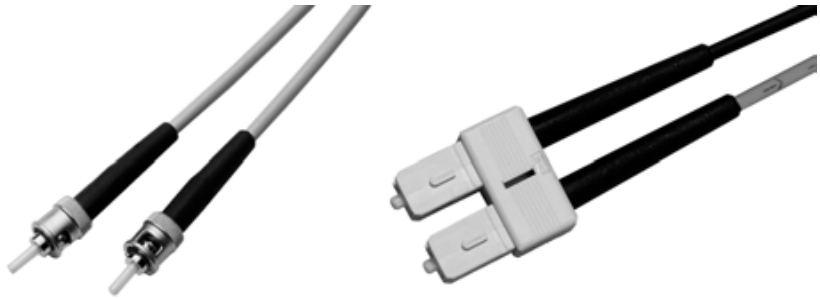


Fig. 7.12 ST (BFOC/2.5) and SC connectors for optical fibers

ST plug connectors: also called BOFC connectors, are used for Industrial Ethernet fiber-optic networks (Fig. 7.12). This type of FO connector specified by AT&T (BFOC/2.5 according to IEC 874-10) is suitable for both singlemode and multimode fibers. This plug connection is frequently preferred because of the bayonet joint. This special type of locking permits rapid connection and is resistant to shock and vibration. The rapidly produced connection represents a great advantage even when using FO patch cables for the jumpering block of a cabinet distribution board.

SC connectors: the SC connector system according to IEC 874-19 is used for newer cabling structures. The SC connector is a polarized push/pull connector with small dimensions and high packing density. This FO connector has a square design, and can be used for both multimode and singlemode fibers. The connector can be used for simplex, duplex and multiple connections. The SC connector is characterized by its compact size and uniformly repeatable connection quality. The design of the connector system means that it is twistproof and provides automatic locking.

7.4 Radio Networks with Profinet

With Profinet you can also design radio networks in line with industrial requirements (Industrial WLAN). Data transmission rates of 1 Mb/s or 54 Mb/s without full duplex operation are permissible with Industrial WLAN.

In contrast to line-based networks with copper or fiber-optic cables, a wireless LAN uses air as the transmission medium. Transmission of information through the air is achieved using electromagnetic waves.

It can be generally stated that radio networks are used wherever mobility and flexibility are important. Complex plants can be commissioned more rapidly, since the requirements for installation of the communications network are reduced. Furthermore, radio networks are the ideal solution if mobile stations are difficult to integrate into the network using cables. Examples include the mobile recording of data for production and logistics applications, the transfer of servicing data via

mobile terminals, or the commissioning of complex plants using mobile programming devices. In this manner, the engineer linked via a wireless connection can be positioned at the optimum plant location, following up any modifications better by observing them directly on site, and accessing servicing and maintenance plans.

Furthermore, radio networks are a cost-effective and reliable alternative to complex and mechanically prone systems such as trailing cables and communication with moving stations (e.g. mobile controllers and devices), storage and retrieval machines, conveyor systems, production belts, sliding tables. It is worth emphasizing that there is no wear on rotating or moving machines or plant components.

Also extremely interesting is the wireless coupling of communications segments in remote, hard to reach or aggressive environments, making fast commissioning or cost-effective networking possible, where the routing of cables would be extremely expensive (e.g. streets, train lines etc.).

7.4.1 Radio Technology

Radio technology comprises the propagation and reception of electromagnetic waves. Radio waves propagate in all three dimensions. All types of obstacles and objects influence the propagation due to reflection, scattering, absorption, interference and diffraction. The propagation properties are always frequency-dependent. Thus low-frequency electromagnetic waves have different propagation properties than very high-frequency electromagnetic waves. Oversimplified, the response of high-frequency electromagnetic waves can be compared with that of light waves.

Reflection of waves

The reflection of radio waves by objects is of great importance for radio networks such as wireless LAN applications. The electromagnetic waves are reflected or absorbed by walls, furniture, persons etc. The signal is thus attenuated, and each material exhibits a frequency-dependent attenuation. For example, an electrically

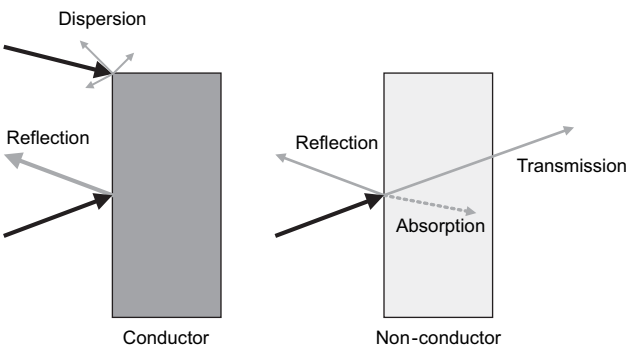


Fig. 7.13 The behavior of radio waves at obstacles

conducting object completely reflects the impinging waves. On the other hand, a non-conducting object reflects part of the wave and absorbs the rest. The impinging radio waves are scattered in practically all directions by edges.

Interference and diffraction

The superimposition of several radio waves and their effect on the signal shape are referred to as interference. The superimposition results in amplification or attenuation of the received signals. The causes of interference are usually complex, and frequently cannot be changed. As a remedy, the most common receivers are nowadays equipped with antenna diversity. In this case, the receiver has two receiving antennae positioned apart by approximately a quarter of the wavelength. At least one antenna then usually receives a signal of sufficient quality.

Channels

In the case of a WLAN, a radio signal is not emitted at only one frequency. By modulating a signal sequence at a carrier frequency, a certain range above and below the carrier frequency is also used depending on the modulation procedure applied. For this reason it is not possible to pack different transmitters as close to a frequency band as desired without interference.

To achieve interference-free operation, the frequency bands of the radio traffic are therefore divided into so-called channels which are distributed at a certain distance from one another within the band. For example, the 2.4 GHz range of the ISM band with IEEE 802.11b/g is divided into 13 channels between 2.412 GHz and 2.472 GHz, where the respective distance between adjacent channels is 5 MHz.

7.4.2 WLAN Topologies

Two types of network are basically distinguished for wireless LAN topology: ad hoc networks, and topologies in infrastructure mode.

- Ad hoc networks – direct connection between two stations
- Infrastructure mode – connection of stations via a common access point
- Mixed networks
- Multichannel configuration
- Wireless distribution system (WDS)

Ad hoc networks

The fastest and simplest manner to operate a WLAN is a so-called ad hoc network (Fig. 7.14). In such a spontaneous network (Independent Basic Service Set, IBSS), the stations communicate directly with one another, and it must therefore be possible for them to reach each other. Such networks can be created rapidly and simply, and are usually used for the temporary exchange of data over small distances such as the short-term networking of several computers during a meeting.

Fig. 7.14
Ad hoc network

Identification for differentiation of several radio networks is carried out using so-called Service Set Identifiers (SSID). These can be freely selected by the user. Every ad hoc network always has one SSID.

Infrastructure networks

In infrastructure mode, an access point coordinates the communication between the stations of a network. In the most simplest case, a group of IEEE 802.11 stations is located in the radio area of one single access point. An access point is a WLAN station with at least one WLAN interface and usually one LAN interface. In the home office sector, a WLAN router with one WLAN interface and one DSL interface is commonly used. Such a network is referred to as a Basic Service Set.

If several access points are connected via Ethernet, and if the same network name (ESSID) is set on all of them, one refers to an Extended Service Set (ESS). This structure increases the range of the radio network. The changeover from one access point to the next is referred to as roaming, and overlapping of the radio areas of the access point is a prerequisite for interruption-free changeover (Fig. 7.15). In infrastructure mode, the stations must log-on at the access point and transmit on the channel which this specifies.

Wireless Distribution System (WDS)

The Wireless Distribution System is a special infrastructure network where the access points are not connected together by cables but by means of a radio network. The inevitable result is that the distance is smaller than the range of the access points, and the data transfer rate is of course also reduced since the two access points have to share the air used as the transfer medium.

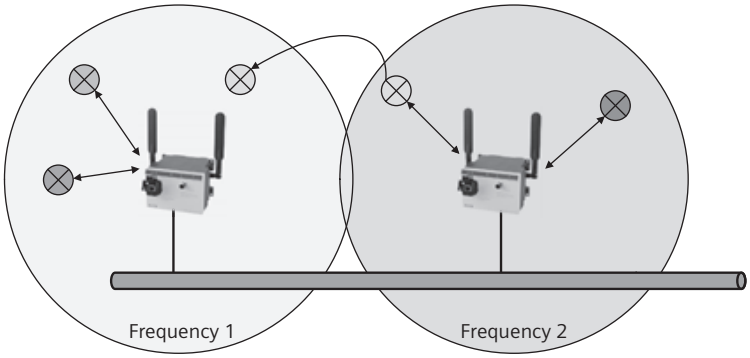


Fig. 7.15 Infrastructure network

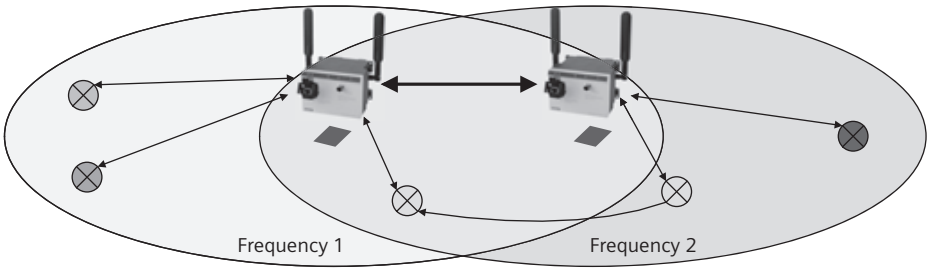


Fig. 7.16 Wireless Distribution System WDS

7.5 Security with WLAN

The topic of security is of particular importance for a WLAN which is based on freely-propagating electromagnetic waves. Everyone located within the range of an access point has the opportunity to monitor the data traffic on the transfer medium (air), and also to possibly influence it. The IEEE 802.11i working group therefore logically adopted a standard (in 2004) which includes definition of encryption algorithms as well as authentication and authorization procedures. The most important terms are explained briefly below.

7.5.1 Wired Equivalent Privacy (WEP)

The Wired Equivalent Privacy (WEP) procedure is the oldest encryption procedure, and also the least secure. It is based on the RC4 algorithm, and is described in the IEEE 802.11 standard. It can be used in different key lengths, typical lengths being 64 or 128 bits. Only the first 24þbits in each case are transmitted publicly for the so-called initialization vector. This is used to make packets with the same content look different. The hurdle to be overcome during an attack therefore consists of 40 or 104þbits.

The initialization vector of only 24þbits is one of the weak points of the WEP procedure, since it is repeated at the latest after approximately 16 million packets. With a modern WLAN of high load, this is achieved within a few hours. The key can then be calculated from two packets encrypted with the same key. In order to crack the WEP, it is not even necessary to monitor the data traffic for hours since so-called weak RC4 keys can occur. The initialization vector can then be determined from these RC4 keys. Since the initialization vector is transmitted in plain text, these keys are easy to detect. An attacker need not monitor 16 million packets. The probability is high that the key can be calculated much earlier. For these reasons, the WEP procedure is generally no longer considered to be sufficiently secure.

7.5.2 WEPplus

WEPplus is a WEP progression, originally developed by Agere Systems. The enhancement was triggered by the so-called weak initialization vectors which make it possible to crack WEP within a few minutes. The idea upon which WEPplus is based is simple – the known weak initialization vectors are no longer used. With WEPplus, potential attackers must now wait for packets with the same initialization vector in order to crack the encryption. WEPplus is compatible with WEP. However, security is only improved if all the WLAN stations support WEPplus.

7.5.3 Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) is specified in RFC 2284 and RFC 2716, and is an authentication protocol. The objective of this method is to embed new methods of user authentication into existing protocols without having to modify all protocols. EAP is only a generic term for various methods. It must be checked in individual cases whether a method is supported by the client, the network components and the authentication server before it can be used. In wireless networks, an attempt is made to link the user log-on via an EAP method to the management of the encryption keys between client and access point. In association with the WEP encryption protocol, for example, the EAP opens up the possibility of defining the WEP session key and changing it periodically so that an overflow of the initialization vector can no longer occur. In order to use the EAP in the WLAN, a so-called Remote Authentication Dial-In User Service (RADIUS) server is required.

7.5.4 Wi-Fi Protected Access (WPA)

The Wi-Fi Protected Access (WPA) was derived at an early point in time from the draft of the IEEE 802.11i standard. This early separation became necessary when market pressures for replacement of the relatively insecure WEP became increasingly great. WPA comprises the following extensions:

- Use of the Temporal Key Integrity Protocol (TKIP) for improved data encryption. The previously weak initialization vector was increased to 48 bits, and temporary keys and a checksum algorithm named Michael were introduced. Finally, additional sequence numbers were used.

- Use of authentication servers with EAP methods for client identification.
- Use of Pre Shared Keys (PSKs) if an authentication server is not possible. With PSK, the client and the access points are informed of a common password for identification. In order to log-on with the access point, the client must identify himself/herself as an authorized user through knowledge of this password, which is not transmitted. Only then is the encryption by the TKIP established. With the VPNs, IPSec also uses this method. PSK is appropriate as a simple method for cases where a user wishes to avoid the overhead of an authentication server.

Since the 802.11i standard has been adopted in the meantime, this is no longer applicable, and thus WPA2 with AES is the preferred standard.

7.5.5 IEEE 802.11i (WPA2)

The IEEE 802.11i standard, also referred to as WPA2, is the current security standard for WLANs. The most conspicuous innovation of IEEE 802.11i, which was not anticipated by WPA, is the introduction of the Advanced Encryption Standard (AES) as a new and improved encryption procedure. The implementation of TKIP in WLAN devices in accordance with IEEE 802.11i is now only an option. Further innovations in IEEE 802.11i are associated with roaming. The objective is to keep the transfer time as short as possible when changing cells. Two measures have been introduced for this purpose. The first is the so-called Pairwise Master Key (PMK) caching, the second is to already commence the log-on procedure at the new access point when the first deterioration in the received level is detected. At the same time, the authentication methods of the Extensible Authentication Protocol (EAP) and the application of PSKs as already introduced with WPA also apply.

7.6 Scalance W

The Scalance W product range is designed for application of an IWLAN (Industrial Wireless Local Area Network). IWLAN is particularly suitable for complex industrial applications where reliable radio communication is essential. In the event of production losses due to machine downtimes or insufficiently monitored processes, the Scalance devices provide reliable radio links with versatile redundancy mechanisms. Radio transmission can then be applied to production and process automation. Ingenious mechanisms for access protection and reliable data transmission, together with antennae diversity, provide a stable radio link.

The high added value of an IWLAN radio network results because data can be transmitted for safe operation of a process (e.g. through reservation of the data transfer rate) and that “noncritical” communication is also possible (IEEE 802.11). Security mechanisms offer protection against espionage, tapping and data falsification. The radio infrastructure can be provided in expansive company grounds (outdoor areas) where high reliability is required.

IWLAN additionally features the following points:

- Reservation of the data transfer rate (expansion of IEEE 802.11b/g and IEEE 802.11a standards) for selected stations for prediction (deterministic) of access to the radio medium and for definition of maximum transmission times, i.e. IWLAN offers deterministic data traffic on the basis of the shared-medium WLAN.
- Cyclic monitoring of the radio link between access point and station for fast detection of faulty statuses and to immediately initiate countermeasures if the connection is interrupted or the radio cell left.
- Redundancy mechanisms for reliable radio infrastructure.
- Automatic switching down to lower data transfer rates in the event of reduced connection quality. Modulation tolerant to faults is taken into account in the 802.11 b,g,a standard. The data transfer rate is reduced in defined steps in order to retain the radio link even over larger distances or with reflections from metallic objects.
- Antenna diversity for very good reception in complex radio environments.
- Optional use of remote antennae for customized requirements.
- Automatic roaming if the connection to the Industrial Ethernet is interrupted (rapid roaming).
- Cyclic monitoring of the link (linkcheck).
- Monitoring for IP connections (IP alive).
- Saving of costs through one single radio network for reliable operation of a process (IWLAN) and for data critical to the process (e.g. alarming), as well as for noncritical communication via wireless LAN (e.g. servicing and diagnostics).
- High protection of investments since all products conform to the globally recognized IEEE 802.11 industrial standard and are suitable for 2.4 GHz and 5 GHz.
- Integral diagnostics functionality: Web-based management tool (HTTP server) for configuration and diagnostics with standard browsers, LEDs for signaling operating and fault statuses, signaling of faults to a network management tool using SNMP trap or e-mail.
- Industrial approvals such as UL, FM, EMC, explosion protection Zone 2

When used outside the control cabinet, and directly in the plant, the components without fans are provided with a rugged enclosure with IP65 degree of protection, and designed for operation from minus 20 to plus 60 degrees Celsius. Typical ranges between two radio components are 30 meters indoors and 100 meters outdoors – depending on sources of interference in the environment resulting from reflection by metals.

A high degree of data security is achieved with the modern mechanisms of Wi-Fi Protected Access (WPA). Using the WPA, users can provide authorization and identification by means of a secret key which automatically changes at regular intervals. WPA uses the TKIP (Temporal Key Integrity Protocol) for this in order to

change the temporary key every 10,000 packets (data transmission units). This guarantees much greater security than the standard WEP where the key has to be changed manually.

Security against foreign penetration into the network is achieved by the authentication. The server verifies the client's identity before permitting access to the network. Access is refused to unknown clients. In order to use the security functions according to WPA, all involved clients (including operating system) must support these functions.

The Advanced Encryption Standard (AES) is provided for encryption of the data. All encryption mechanisms are already included in the products. If a security concept, e.g. with Virtual Private Networks (VPN) is desired nevertheless, the products can be integrated into it without problem. Scalance W can be upgraded to the IEEE 802.11h standard.

7.6.1 The Components of Scalance W

The Industrial Wireless LAN is a radio network offered by Simatic Net which allows use by stations on the basis of 802.11b/g and a, but which also supports special stations with particular reliability requirements, such as PLCs for example. IWLANs can be designed with the following components (Fig. 7.17):

- Scalance W788-1PRO (access point)
- Scalance W788-2PRO (dual access point)
- Scalance W788-1RR (access point iPCF)
- Scalance W788-2RR (dual access point iPCF)

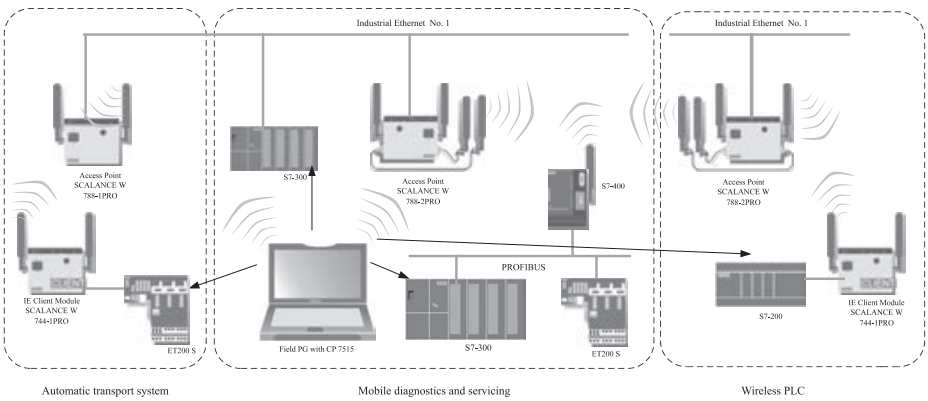


Fig. 7.17
The components of Scalance W in use: the field PG with CP 7515 in the center communicates via IWLAN with the ET200S in the automatic transport system (via Scalance W788-1 PRO and Scalance W744-1PRO), via Scalance W788-2 PRO with the S7-300, via the IWLAN/PB-Link PN IO with a Profibus network with ET200S and S7-300, as well as with a wireless S7-200 PLC via two Scalance W788-2 PRO

- Scalance W744-1PRO (Ethernet client module)
- Scalance W746-1PRO (Ethernet client module)
- Scalance W747-1RR (Ethernet client module iPCF)
- CP 7515 PC-Card for interfacing field PGs or notebooks
- IWLAN/PB Link PN IO
- Accessories such as power supplies, IWLAN RCoax cable and remote antennae
- Sinema E engineering software

7.6.2 Scalance W788-1PRO

The Scalance W788 is equipped with an Ethernet interface and a wireless LAN interface. This device is therefore suitable for the following applications:

- Passing on of data from one station to another without a connection having to exist to a wire-based Ethernet.
- Transition from a wire-based network to a wireless network.
- Wireless bridge between two networks.
- Bridge between two different frequencies.
- Scalance W788-2PRO: as a result of the second WLAN interface, a redundant radio link can also be implemented between two Scalance W788-2PRO.

Scalance W788 is characterized by the following features (Fig. 7.18):

- The Ethernet interface supports 10 Mb/s and 100 Mb/s, in each case with full duplex and half duplex, as well as autocrossover and autopolarity.
- The wireless interface is compatible with the IEEE 802.11a, IEEE 802.11b and IEEE 802.11g standards. In 802.1a and 802.1g modes, the gross transmission rate is up to 54 Mb/s. In turbo mode, the transmission rate is up to 108 Mb/s (not

Fig. 7.18
Scalance W788: two removable antennae, hybrid connector for Ethernet and power supply, redundant power supply, two additional sockets for remote antennae

permissible in all countries and operating modes). Devices with increased reliability requirements (IWLAN) can be operated in the same radio network as standard wireless LAN products (IEEE 802.11). Operation is carried out in the 2.4 GHz and 5 GHz frequency bands.

- Support of the WPA, WPA-PSK and IEEE 802.1x authentication standards as well as the WEP, AES and TKIP encryption procedures.
- Suitable for incorporation of a RADIUS server for authentication.
- Device-based and application-based monitoring of the radio link.
- The interoperability of Scalance W788 devices with Wi-Fi devices from other vendors has been tested in detail.
- The access point provides reservation of the data transfer rate (expansion of IEEE 802.11b/g and IEEE 802.11a standards) for selected stations for prediction (deterministic) of access to the radio medium and for definition of maximum transmission times. An automatic switch is made to lower data transfer rates at a reduced connection quality. In addition, the radio link between access point and station is monitored in order to rapidly detect faulty statuses. Antenna diversity helps provide very good reception in complex radio environments.

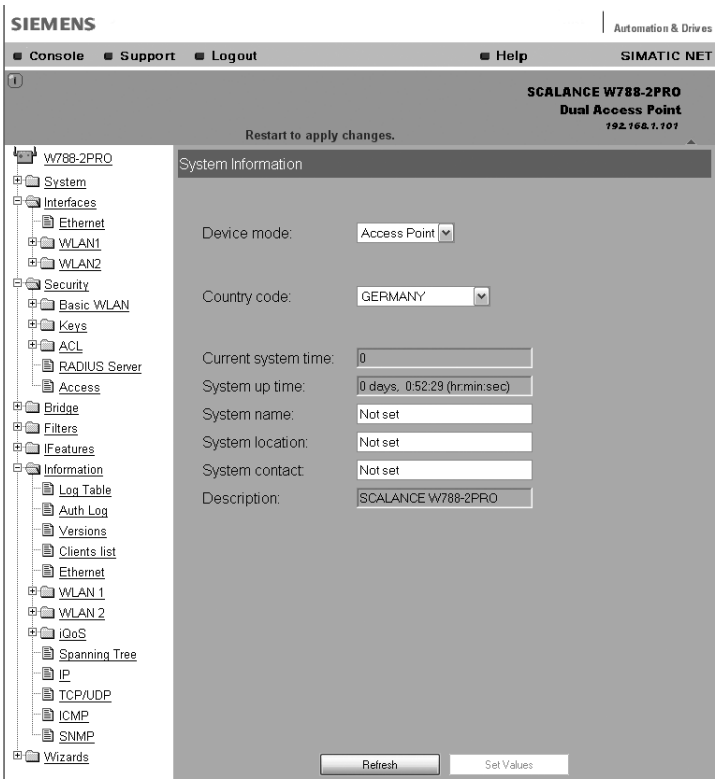


Fig. 7.19 The Web interface of the Scalance W

A radio card (compatible with IEEE 802.11b/g and IEEE 802.11a) is integrated in the device in a rugged metal enclosure, optimized for resistance to shock and vibration and high mechanical requirements. Two ANT795-4MR omnidirectional antennae are connected on the housing by means of a screw connection (R-SMA). These two antennae can be replaced by antennae from the Scalance W700 range, where antennae diversity is retained. Using a hybrid line with "Power over Ethernet" (PoE), data transfer and the power supply for the access point are implemented on a common line. The supply voltage is 24 V DC (redundant), and a 220-V version is also available. The Industrial Ethernet connection is made using the same line, and is powered via the IE FC Standard Cable 4 x 2 with the IE FC Modular Outlet with Power Insert. Using the Web-based management tool, configuration and diagnostics are carried out using standard browsers for the complete Scalance W range (Fig. 7.19).

The access point offers two operating modes:

- Infrastructure mode: a radio network can already exist with just one access point or any number of access points so that area networks can be established within buildings. Within these networks providing ample area coverage, the stations move with automatic transfer from one access point to the next (roaming) without interruption. This is carried out transparent to the application. The access point provides an Industrial Ethernet interface for connection to the wire-based network. Stations such as mobile PLCs, the MOBIC Internet Pad or field PGs can move freely within the radio cells, and exchange data with other stations (Fig. 7.20). Wi-Fi compliance confirms the interaction with products from other vendors.
- Point-to-point mode: in this mode, two Ethernet segments are connected together by a radio link if cables are difficult to install (e.g. over streets). Scalance W788-1PRO can work with up to eight point-to-point connections. Redundant radio networks with high reliability can be provided using the implemented

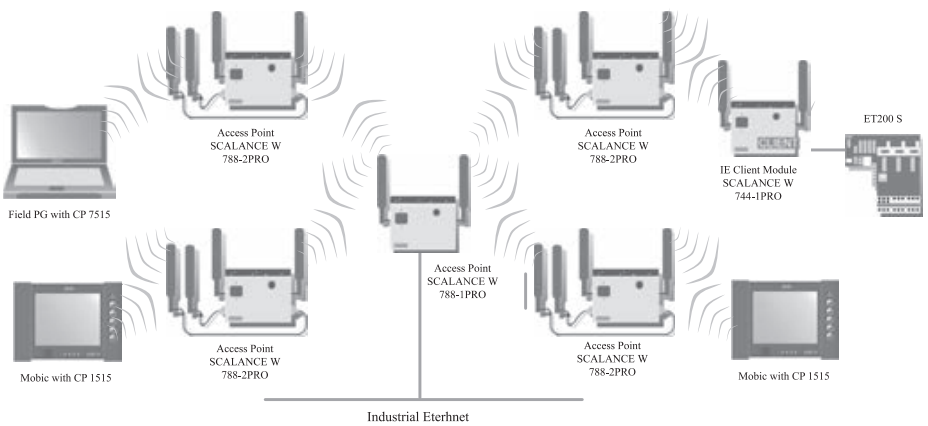


Fig. 7.20 Infrastructure mode

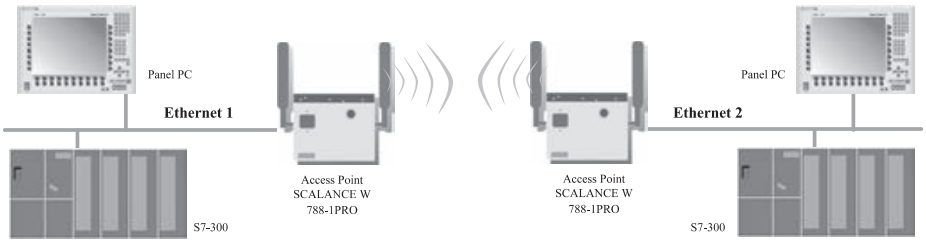


Fig. 7.21 Point-to-point mode

spanning tree function. This function particularly prevents redundant network paths (loops) in the LAN in switched environments. Networks should only have one path to any possible destination. This prevents the duplication of data packets with repeated arrival at the destination, since this could result in malfunctions and reduce the network performance. On the other hand, redundant network paths are desirable in the event of faults. The spanning tree algorithm copes with these requirements. By replacing the two antennae with optionally available directional antennae, ranges of several 100 m can be achieved outdoors (Fig. 7.21).

7.6.3 Scalance W788-2PRO

The Scalance W788-2PRO dual access point has two interfaces for Industrial Wireless LAN. This means that many applications can be implemented: for example, redundant point-to-point connections or wireless backbone with one radio card, and establishment of an infrastructure with the other radio card at the location of the dual access point. The Scalance W788-2PRO dual access point is identical to Scalance W788-1PRO with the following additional features:

- Second radio card for WLAN 802.11b,g and 802.11a
- 2x R-SMA connections for remote antennae
- Redundancy mode for very reliable point-to-point connection with two separate radio cards
- Point-to-point mode: in this case, the two radio interfaces are operated in point-to-point mode for each Scalance W788-2PRO, resulting in a redundant radio network (implementation of redundant paths with spanning tree) (Fig. 7.22). If a fault occurs on a connection, the radio network automatically finds a redundant path. This guarantees a high degree of operational reliability.
- “Redundancy mode”: in this case, two Industrial Ethernet segments are coupled, and the data stream is transmitted in parallel from both radio cards (Fig. 7.23). If the frequency band for one radio card is selected at 2.4 GHz and for the other at 5 GHz, a radio link with maximum reliability is implemented.

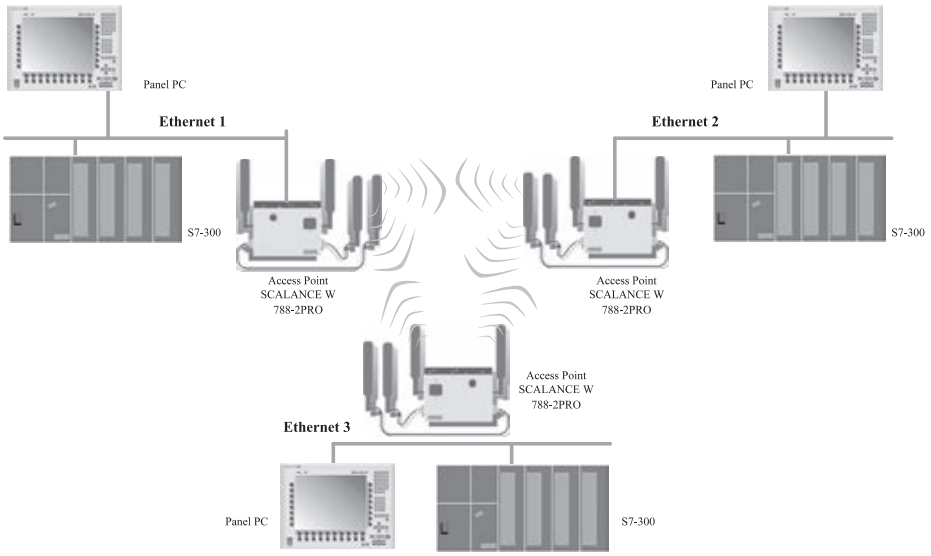


Fig. 7.22 Point-to-point mode

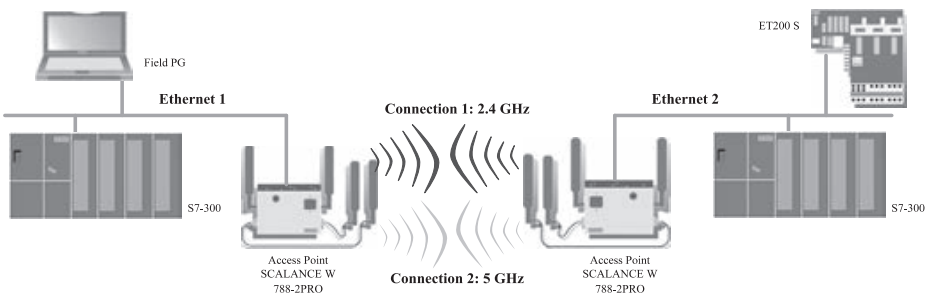


Fig. 7.23 Redundancy mode

7.6.4 Scalance W744-1PRO

The Scalance W744-1PRO Ethernet client module establishes the radio link from (exactly) one mobile device with Ethernet interface to the radio network. The device is typically used to integrate a wire-based Ethernet device (e.g. Simatic S7 PLC) into a wireless network.

Scalance W744-1PRO and Scalance W788-1PRO have identical designs and the same connections, but differ in their function: Scalance W788-1PRO implements the radio network within which Scalance W744-1PRO can freely move. The Ethernet client module is automatically transferred from one access point to the next in a manner transparent to the application (roaming).

The Scalance W744 is equipped with an Ethernet interface and a wireless LAN interface. This device is therefore suitable for the following applications:

- Linking of a device with Ethernet interface (e.g. Simatic PLC with Industrial Ethernet communications processor) to a WLAN.
- Transition from a wire-based network to a wireless network. One station is supported on the wire-based network.

A simple ad hoc mode is also available. This is the simplest radio link between exactly two mobile devices. A Scalance W744-1PRO can communicate with another Scalance W744-1PRO or with a radio card (e.g. CP 7515) (Fig. 7.24).

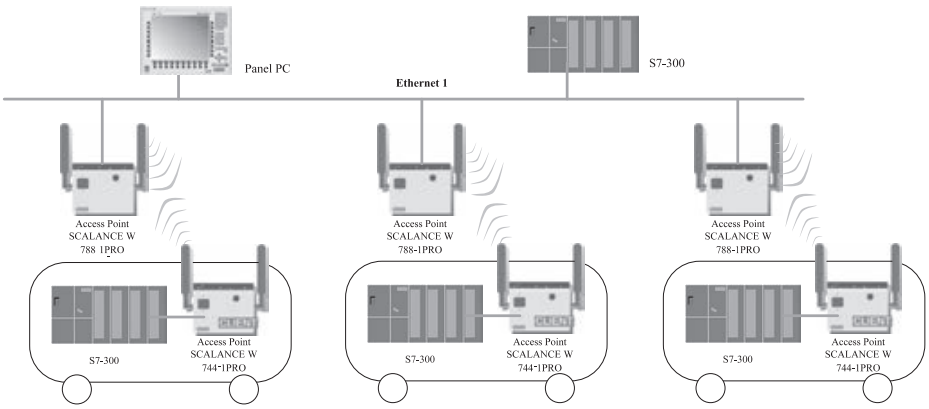


Fig. 7.24 Scalance W744-1PRO used with an automatic transport system

7.6.5 iPCF with Scalance W

In addition to the functionality of the Scalance W788-xPRO, the Scalance W788-1RR/2RR access point also possesses the so-called rapid roaming function which permits particularly fast transfer of information. Rapid roaming is an extension of Industrial Wireless LAN and offers real-time radio communication even if stations move beyond the range of radio cells and updating times up to 20 ms are required. Rapid roaming is based on the iPCF procedure and is an own development of Siemens AG. It only operates together with stations for which iPCF (Industrial Point Coordination Function) is implemented.

With Wireless LAN according to IEEE 802.11 and a very high number of stations, the maximum throughput in a radio cell cannot be achieved because of the resulting collisions. A further limitation is the handover times achievable with 802.11 standard mechanisms. With commercially available WLAN products, these have a magnitude of several hundred milliseconds. Industrial applications exist which require a deterministic response with a high number of stations and high throughput in a radio cell. In addition, a deterministic response is required when changing the cell with handover times of below 100 milliseconds. The expansion iPCF was developed in order to satisfy these requirements. iPCF is available with the following products:

- Scalance W788-1RR and Scalance W788-2RR
- Scalance W747-1RR
- IWLAN/PB Link

iPCF ensures orderly execution of the complete data traffic of a radio cell, controlled by the access point. The throughput can be optimized even with a high number of stations by avoiding collisions. In addition, iPCF permits a very fast change in radio cell.

Use of iPCF is particularly recommendable if a high data throughput is to be implemented with a high number of stations or if very short handover times are required. For operation with PNIO data traffic (Profinet IO), the iPCF procedure was additionally optimized in that the PNIO traffic is handled with high priority.

The basic principle of iPCF is that the access point cyclically scans all stations in the radio cell. Scanning simultaneously includes the downlink traffic for this station. The station sends the uplink data in the reply. The access point scans a new station at least every 5 ms. Scanning of a station can be seen by all other stations in the radio cell. In this manner, a client can determine the quality of the radio link to the access point even if it is not communicating itself with the access point. If it does not receive a frame from the access point for a certain time, it commences searching for a new access point. In iPCF mode, the time response when searching for a new access point as well as when registering with this new access point is optimized. Handover times of significantly less than 50 ms are achieved.

However, it is possible to set both iPCF and standard WLAN simultaneously for an access point with two WLAN interfaces. iPCF has been optimized for use of RCoax cables on the access point, and only achieves its optimum performance in this configuration.

7.6.6 CP 7515

The CP 7515 communications processor is a PC card (32-bit CardBus) for operation in an Industrial Wireless LAN (IWLAN) with reliable communication (Fig. 7.25). The CP 7515 can be used in a standard WLAN according to IEEE 802.11b/g and IEEE 802.11a at 2.4 GHz and 5 GHz. The CP 7515 is used to link field PGs or notebooks in the industrial environment to a radio network. In addition, access is possible to Industrial Ethernet, e.g. to the Simatic S5/S7, in conjunction with the SOFTNET packages for Industrial Ethernet. The communications processor can be used in industrial environments (IWLAN) as well as in the office sector. To this

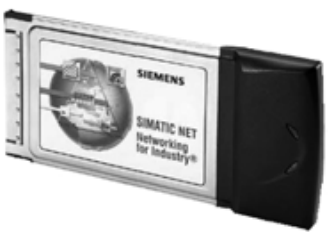


Fig. 7.25 CP 7515

end, the CP is inserted into the 32-bit CardBus slot of a mobile device (e.g. Internet pads, PG/notebooks).

In IWLAN radio networks with access points from the Scalance range, and in addition to the standardized transmission of data, the CP 7515 radio card offers the possibility for reserving the data transfer rate, thus providing deterministic data traffic. In order to increase the reliability of the radio link even further, its quality is monitored cyclically, and a message generated in the event of an error. The CP 7515 exhibits the following features:

- Reliable through reservation of data transfer rate, and cyclic monitoring of the connection (IWLAN).
- Advanced data security through WPA and encryption with AES.
- Compatible with IEEE 802.11a and IEEE 802.11g for data transmission at up to 54 Mb/s with dynamic adaptation of the data transmission rates 16, 9, 12, 18, 24, 36, 48 and 54 Mb/s.
- Compatible with IEEE 802.11b for Ethernet data transmission at up to 11 Mb/s with dynamic adaptation of the data transmission rates 1, 2, 5.5 and 11 Mb/s.
- Operation in two different frequency bands (2.4 ~ 2.5 GHz and 5.15 ~ 5.85 GHz).
- Guarantees high data security through encryption of data with 64/128/152 bits.
- Supports infrastructure mode for coupling via an access point or ad hoc mode for direct coupling to another PC using peer-to-peer communication.
- Two integrated antennae (antennae diversity) for reliable reception in complex radio environments are integrated in the card.
- Communications services using ISO or TCP/IP transport protocol: PG communication, S7 communication, S5-compatible communication (SEND/RECEIVE). The protocols for S7 communication and S5-compatible communication are configured in Step 7 version 5.2 SP1 or later or NCM PC version 5.2 SP1 or later. The NCM PC configuration tool is included in the scope of delivery of the SOFTNET-S7 and SOFTNET-PG software packages for Industrial Ethernet.
- Integration into existing security concepts with authentication according to IEEE 802.1x and a RADIUS server or Virtual Private Network (VPN) is possible without problem.
- Installation and parameterization with management tool for Windows: client manager for adjustment of operating parameters and for diagnostics of the parameterization or transmitted power.
- Integration in Step 7/NCM PC.

7.6.7 IWLAN/PB Link PN IO

The IWLAN/PB Link PN IO (Fig. 7.26) is a compact router which connects Industrial Wireless LAN and Profibus together. The link is either the Profibus master interface or Profinet I/O proxy.

Fig. 7.26
IWLAN/PB Link PN IO

As a router, it serves as a Profinet I/O proxy. In this case it provides the connection between the Profinet IO controllers on Industrial Ethernet and the Profinet IO Devices (DP slaves on the Profibus). From the viewpoint of the Profinet IO controller on Industrial Ethernet, there is no difference between access to Profinet IO Devices connected via Industrial Wireless LAN and the IWLAN/PB Link PN IO to Industrial Ethernet and access to Profibus DP slaves connected to Profibus DP. In this case, IWLAN/PB Link PN IO takes over the role of a proxy for the DP slaves connected to Profibus DP. DP slaves according to Profibus DP-V0 are supported, as well as DP slaves according to the DP-V1 standard and Siemens DP slaves in the case of firmware release V1.1.0 and later.

As Profibus master interface, it serves for flexible integration of systems from the field level into an IWLAN radio infrastructure according to IEEE 802.11b/g and IEEE 802.11a with up to 54 Mb/s at 2.4 GHz or 5 GHz, e.g. with Scalance W access points.

In standard mode, the IWLAN/PB Link PN IO provides the following services:

- PG/OP communication: this is used to load programs and configuration data, to implement test and diagnostics functions, and to operate and monitor a plant (HMI systems).
- Parameterization of field devices (record routing): you can use the IWLAN/PB Link PN IO as a router for records intended for field devices (DP slaves). Devices which are not directly connected to the Profibus and thus do not have direct access to the field devices (DP slaves) can then transmit records to the field devices via IWLAN/PB Link PN IO. An example of a tool which generates such records for parameterization of field devices is the Simatic PDM (Process Device Manager).
- Router to a DP master system with equidistance: the IWLAN/PB Link PN IO serves as a router between the industrial WLAN and the field devices on a DP master system. The IWLAN/PB Link PN IO is operated here as an active station together with a DP master on a Profibus parameterized with equidistance.

- Cross-subnetwork S7 connections for HMI mode: the IWLAN/PB Link PN IO passes on the communication via S7 connections. This service is used, for example, with HMI applications (PC stations).

Further properties and services:

- Compatible with IEEE 802.11a and IEEE 802.11g for data transmission at up to 54 Mb/s with dynamic adaptation of the data transmission rates 1, 6, 9, 12, 18, 24, 36, 48 and 54 Mb/s.
- Passing on of time-of-day frames (configurable option): the IWLAN/PB Link PN IO can pass on the time-of-day frames received from a real-time transmitter.
- C-Plug as interchangeable medium for configuration data: the IWLAN/PB Link PN IO supports saving of configuration data on an interchangeable medium (C-Plug). Simple replacement of a faulty module is then possible by inserting the C-Plug into the new module.
- PRESET-PLUG: the PRESET-PLUG is used to assign a defined default setting to an IWLAN/PB Link PN IO and to Scalance W devices in a simple manner.
- WLAN security properties: the IWLAN/PB Link PN IO supports the WPA, WPA-PSK and IEEE 802.1x authentication standards and the WEP, AES and TKIP encryption procedures.
- IWLAN/PB Link PN IO supports iPCF mode: use of iPCF is particularly recommendable if a high data throughput is to be implemented with a high number of stations, or if very short handover times are required. The iPCF procedure has been additionally optimized for use with Profinet IO data traffic in that the Profinet IO data traffic is handled with high priority.
- The parameters required for the IWLAN/PB Link PN IO, e.g. the addresses, are assigned using Step 7, and all routing information required is generated automatically.

The IWLAN/PB Link PN IO permits use of IWLAN with RCoax and WLAN antennae for wireless or contact-free data transmission. Connection of a WLAN antenna or alternatively an antenna for operation with RCoax cable (leaky wave conductor, see Fig. 7.29 and Chapter 7.6.8) permits communication with automation systems in mobile applications. This means that solutions with power rail booster for Profibus using wiper contacts can be replaced by contact-free data transmission.

7.6.8 Accessories for WLAN Devices

PS791-1PRO power supply: the PS791-1PRO power supply is an AC/DC supply for the Scalance W700 and Scalance X208PRO products (Fig. 7.27). It permits flexible integration into various systems since the high efficiency guarantees low thermal dissipation, and power failures are bypassed. The wide input voltage range means that worldwide use is possible.

Antennae and accessories: ANT793-8DR, ANT795-4MR and ANT795-6MR remote antennae provide reliable radio links for the Scalance W700 products (Fig. 7.28).

Fig. 7.27
Power supply

They are optimally suitable for the Scalance W788-1PRO, Scalance W788-2PRO and Scalance W744-1PRO products. Assembly is very simple since the antennae are already provided with cable and R-SMA connector. The antennae of Simatic Net, all of which provide IP65 degree of protection, have either a directional characteristic (20° vertical, 20° horizontal) or an omnidirectional characteristic (360° horizontal, 30° vertical).

Fig. 7.28 Various antennae for the Scalance system

LP798-1PRO lightning protection element: the lightning protection element expands the possible applications of Scalance W700 products with remote antennae, especially outdoors.

TI795-1R antenna terminating resistor: if application of the second antenna is relinquished when using Scalance W700 products, an antenna terminating resistor must be connected to the second R-SMA socket.

IWLAN RCoax cable: with radio communication, electromagnetic waves are sent and received by antennae. Conditions exist, however, where the send or receive area can only be poorly covered – or not at all – by the radiation and reception range of conventional antennae. These include certain buildings and tunnels. Using so-called leaky wave cables (Fig. 7.29), the radiation can be exactly matched to the spatial conditions.

Fig. 7.29
IWLAN RCoax cable

RCoax is a coaxial cable with exactly positioned slits in the outer conductor. The fact is utilized here that cables also emit electromagnetic waves if they have an appropriate physical design. Radio waves can then be coupled in and out simply and reliably, irrespective of the position relative to the cable. This leaky wave conductor is used as an antenna by Scalance W access points. It provides a reliable radio link in defined areas since the transmitted power is led along the RCoax cable. In this manner, transmitter frequencies as well as power/location can be exactly managed in shop floors in which wireless systems are used in the production. This technology is highly suitable for tunnels, channels, hazardous areas and every type of track vehicle, since the generation of sparks along wiper contacts can no longer occur. The distance between a moving device and RCoax can be between several centimeters (overhead conveyors) up to 10 m (e.g. in channels and tunnels).

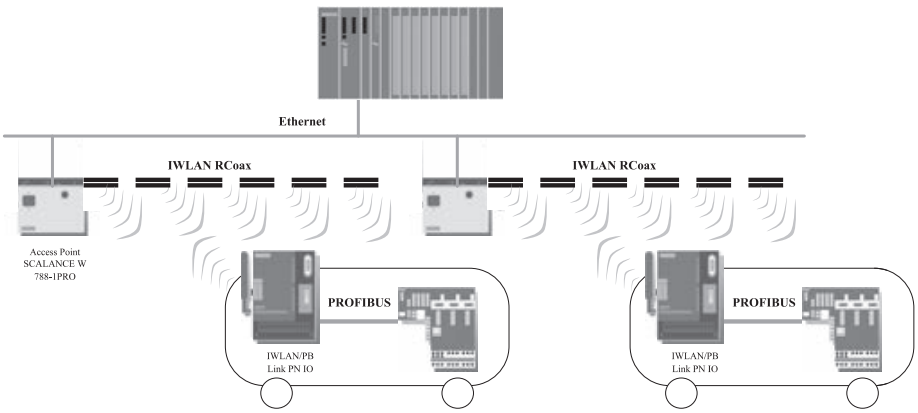


Fig. 7.30 IWLAN RCoax cable application: contact-free data transmission for vehicle controls

Application examples:

- Storage and retrieval systems: wireless, and thus wear-free data transmission, results in increased plant availability. With storage and retrieval systems, data light barriers requiring high maintenance can be replaced by an IWLAN.
- Overhead conveyors: as a replacement for contact conductors, the IWLAN/PB Link PN IO in association with RCoax leaky wave conductors permits non-contact data transmission. Vehicle controls for overhead conveyors can then be implemented cost-effectively (Fig. 7.30).

7.6.9 Configuration and Parameterization of Scalance W

Initial assignment of an IP address to the devices can be carried out using DHCP or the primary setup tool. This tool is able to assign an IP address to non-configured devices. The only requirement is that these devices can be accessed over Ethernet. Integration in Step 7 is not currently possible.

The primary setup tool uses the DLC protocol for communication with the modules. This protocol is not included in the delivery of Windows XP, and must therefore always be subsequently installed for this operating system. The files of the primary setup tool and the DLC protocol are supplied as software with the devices. Further information is provided in the device manual.

Scalance W access points have an integral HTTP server for Web-based management. If the Scalance W is addressed by an Internet browser, it returns HTML pages to the client computer depending on the user inputs. Users enter their configuration data in the HTML pages sent by Scalance W. The Scalance W evaluates this information, and generates dynamic reply pages. The particular advantage of this principle is that no special software is required at the client end apart from an Internet browser. Once an IP address has been assigned to the device by the primary setup tool, it is possible to carry out further configuration by means of Web-based management. Further information on Web-based management is provided in the device manual.

Please note: if you construct Profinet with Industrial WLAN, you must change the updating time (send cycle). The parameter can be found in Step 7 / HW-Config in the object properties of the I/O master system. We recommend that you set 32 ms there as the updating time. A change in the updating time has an effect on all IO Devices on the associated I/O master system.

7.6.10 Sinema E (Simatic Network Manager Engineering)

As described in the previous sections, an exact prediction of the propagation of a radio field depends on a wide variety of factors: conducting and non-conducting objects in the transmission area can reflect, absorb, transmit or diffract radio waves. The Sinema E software package is available for planning of the radio field, and permits simulation of the field before the hardware is installed.

As a first step in Sinema E, the user models the environment within which the WLAN is to be installed. This includes the walls, windows, doors, ceilings and

floors in the building, with consideration of their thickness and composition, as well as larger fixtures and furniture. In a further step, the active components, access points and clients are positioned within the modeled office or industrial landscape. Devices, antennae and radio obstacles can be selected from a component catalog and adapted to requirements. An idea of the signal quality to be expected can be achieved by a subsequent simulation. The GUI allows even complex environments to be mapped relatively simply (Fig. 7.31).

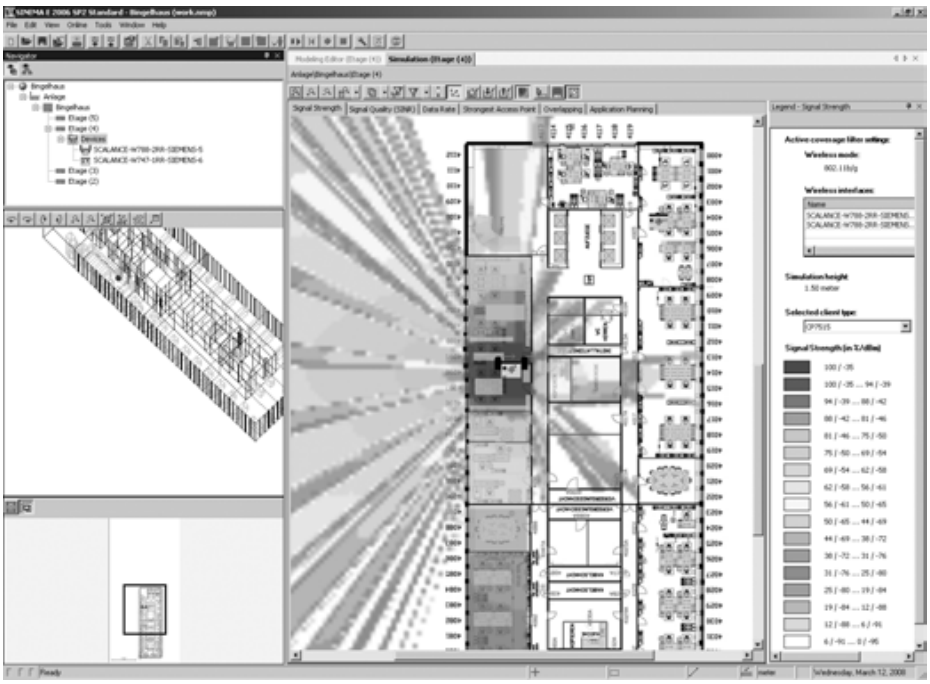


Fig. 7.31 Configuration of part of a building in Sinema E

The simulation is carried out in three dimensions and also allows evaluation of the radiation response over several floors. Using the access points and clients distributed by the user in the modeled building, Sinema E simulates the resulting radio field and displays it in graphic form so that it immediately becomes evident whether the coverage and data transfer rate of the radio cell are sufficient. The frequency of the transmitters as well as the characteristics of the antennae used, for example the RCoax Cables, are taken into consideration.

Report module

From the configuration developed during the simulation, this module generates a parts list containing the ordering data of all devices selected from the module catalog. When designing the radio network, the report also provides the coordinates at which the individual devices should be located. This facilitates trouble-free in-

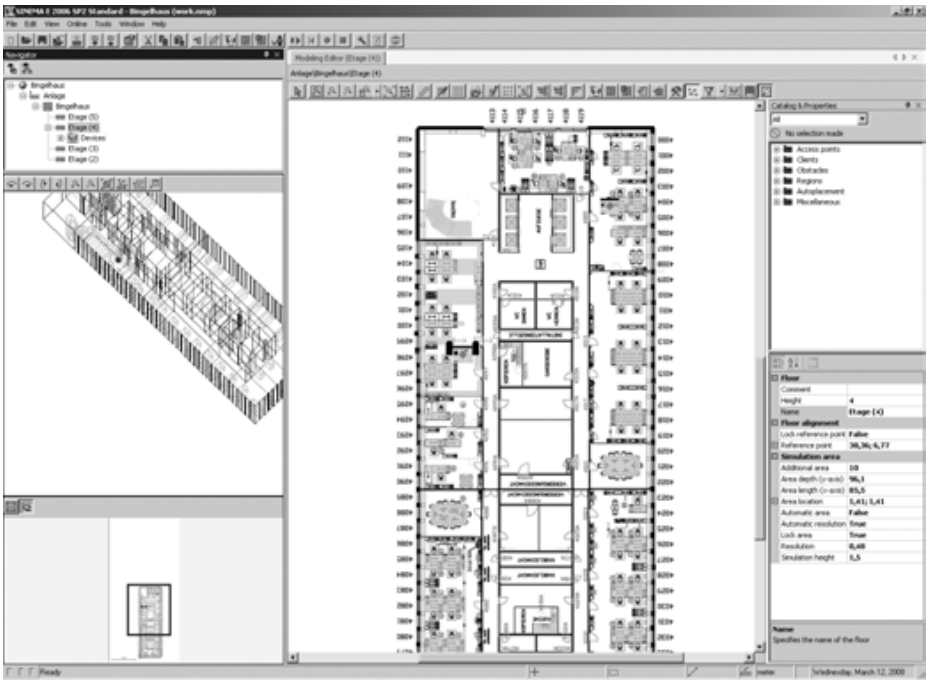


Fig. 7.32 Simulation of radio signal strength in Sinema E

stallation of the individual components. The report also includes the implemented simulations in the form of informative graphics showing the signal strength and data transfer rate as well as interferences (Fig. 7.32). As a result, the report is also an acceptance document for commissioning, and can be used for guarantee and servicing purposes.

Material/Region Builder

The Material/Region Builder is a Sinema E module with which complex radio obstacles or machine components such as turbines can be measured in reality, saved, and reused in the current simulation as well as in future simulations. This avoids the repetition of measurements, and permits the creation of user-specific libraries of radio obstacles with their exact geometries and characteristics.

7.7 Active Network Components

Depending on the size, expansion and complexity of a network, a large number of further active components which influence the signals are required in addition to the cabling and the corresponding connection system. The functionality, quality and performance of a network largely depend on the active network components used.

Profibus is a linear network. The communication stations are connected to the bus by a passive conductor. In contrast to this, the Industrial Ethernet consists of point-to-point connections: each station is directly connected to exactly one other station. If a station is to be connected to several other stations, it is connected to the port of an active network component, e.g. a switch. Further communication stations (also switches) can be connected to the other ports of the switch. The connection between a station and the switch is still a point-to-point connection.

Devices are identified as network components which are located in the transmission path between the data terminals and which regenerate received signals and pass them on to a specific destination. Network components with Profinet are switches and routers. They are used to provide the network topology (star, linear, tree, ring) and permit data communication between individual segments. Network components suitable for Profinet must be designed for Fast Ethernet (100 Mb/s) and full duplex transmission. In full duplex mode, a network component simultaneously receives and sends data at the same port. No collisions occur, and therefore no bandwidth is lost through possible collisions. The network configuration is greatly simplified since checking of the route lengths within a collision domain is omitted. In order to guarantee compatibility with old plants or individual, older data terminals or hubs, the interfaces should also support operation of 10BASE-TX (10 Mb/s, CSMA/CD). In addition, Profinet devices must also support the autocrossover function (automatic adaptation of send and receive lines, possibly with automatic exchanging of the two lines) as well as autonegotiation (automatic adaptation to the transmission rate). This specification with autocrossover guarantees simple installation since the connection cables can be used at both ends with the same connectors and same assignments.

7.7.1 NICs – Network Interface Cards for Programming Devices and PCs

An NIC (network interface card) is a network adapter which connects the stations to the transmission medium of the network. In a computer, this is a card which permits access to the connected network. It conditions the data from the computer, and converts them accordingly for the transmission medium, and vice versa. Simatic Net provides various communications processors for PCs and portable devices. These mainly differ in their communications performance and in the design. The PC modules are key components in the automotive industry for interfacing robots to Profinet.

The CP 1616 PCI module with integral ASIC ERTEC 400 and 4-port real-time switch permits connection of programming devices/PCs to Profinet IO. High-performance control tasks on the PC are then easy to solve (e.g. PC-based Control, Numeric Control, Robot Control). The hardware is designed for IRT capability. The module works as both an IO controller and IO Device.

The Simatic Net CP 1616 allows connection to Industrial Ethernet or Profinet for Simatic programming devices/PCs and PCs with PCI slot with 10/100 Mb/s for any operating systems (via Development Kit), as a PN IO controller and/or PN IO Device (RT and IRT) (Fig. 7.33). The CP provides high-performance support for control tasks on the PC (PC-based Control, Numeric Control, Robot Control). The CP is par-

Fig. 7.33
CP 1616 with integral ASIC ERTEC 400 and 4-port real-time switch

ticularly suitable for IRT-critical applications (isochronous real-time) which extend into the range of strict isochronous controls in the motion control sector. The integral 4-port real-time switch (ERTEC 400) permits low-cost system solutions and the design of various topologies for local networks. In line with industrial requirements, the 4-port real-time switch permits the design of line topologies with spur lines and eliminates the need for external switch components. The facility for independent connection of an external power supply means that the switch function is also available with the PC switched off. The CP 1616 offers the following communications services: Profinet controller, support of IRT for motion control applications.

Comprehensive diagnostics are provided using Step 7 or SNMP, including general diagnostics and statistics functions, connection diagnostics, diagnostics of assigned Profinet field devices, integration into network management systems through support of SNMP V1 MIB-II, integration into network management systems through support of SNMP, comprehensive diagnostics facilities for installation, commissioning and operation of the module.

The following software packages are available for Windows operating systems:

- IO Base (is provided with the CP 1616) for:
  - Profinet controller: connection of field devices to Industrial Ethernet with Profinet.
  - Provision for isochronous mode access to real-time data for Profinet via IRT (available soon). Guarantees extremely short cycle times with precise clock-pulse rates. Exact jitter values, isochronous mode and cycle time allow high-performance motion control applications.

  - Direct memory access to the process data. The process data of the IO Devices are always consistent. The IO programming interface provides the PC programmer with function calls for data exchange.
  - The interface design permits easy portability to other operating system environments (e.g. VxWorks, QNX, RMOS, RTX).
  - The IO Base interface of the CP 1616 is compatible with the interface for Softnet PNIO.
- DK-1616 development kit for operating systems other than Windows: the DK-1616 allows integration of the CP 1616 communications processor into any operating system environment. It includes the driver source code required for this, as well as the description.
- OPC interface: the OPC server included in the respective software package can be used as the standard programming interface for Profinet, S7 communication and S5-compatible communication in order to link automation engineering applications to OPC-capable Windows applications (Office, HMI systems and similar).
- Programming interface using C library: the IO Base interface can be used for applications wishing to directly use the Profinet controller functionality via C/C++. The design of this interface is based on the DP-Base interface of the Profibus modules CP 5613 and CP 5614. This permits simple portability of existing Profibus DP master applications to Profinet IO controller applications.

CP 1604 – time functionality in PC/104 format

The PC/104-plus card with integral ASIC ERTEC 400 and 4-port real-time switch allows the connection of PC/104-based systems to Profinet. The CP 1604 has the same functionality as the CP 1616, but has the PC104/PLUS module format. It supports both Profinet real-time properties, namely real-time RT and isochronous real-time IRT (hardware is designed for real-time capability; firmware update will follow). IRT is particularly suitable for time-critical applications which extend into the sector of strict isochronous controls in the motion control sector.

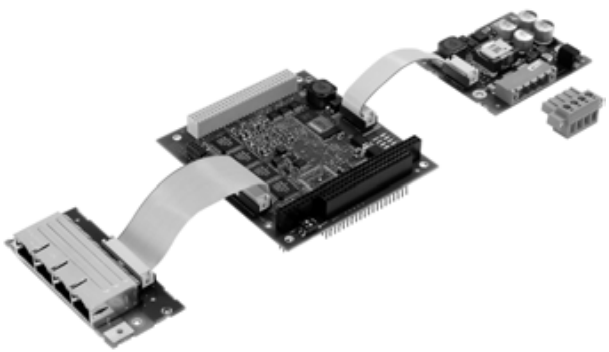


Fig. 7.34 CP 1604 with RJ45 connection and power supply

The CP 1604 can be used as a Profinet IO controller and/or Profinet IO Device which contains the process image (input and output data) in the memory area on the CP (Fig. 7.34). High-performance data exchange with the IO Devices is carried out autonomously by the CP 1604. It supports the real-time properties of Profinet for RT and IRT (available soon). The real-time properties of the CP 1604 guarantee extremely short cycle times with precise clock-pulse rates. In line with industrial requirements, the 4-port real-time switch permits the design of line topologies with spur lines and eliminates the need for external switch components. The facility for independent connection of an external power supply means that the switch function is also available with the PC switched off.

7.7.2 CP – Communications Processors for PLCs in the S7 World

In automation systems from the Simatic range (Simatic S7-300 and S7-400), so-called communications processors (CP) handle the task of an NIC. CPs are available for many data terminals, and offload the CPU module by means of their own processor and also make additional connections possible. The communications processors described below are currently available to users for the Profinet interfacing of a Simatic programmable controller. Further devices are currently being developed.

CP 343-1 Lean

The CPþ343-1þLean (Fig. 7.35) is the communications module for the SimaticþS7-300 for connection to Industrial Ethernet and Profinet IO with 100 Mb/s. With its own processor, the CPþ343-1 Lean relieves the CPU of communications tasks and permits further supplementary connections. The CP 343-1 Lean (CX10) has an integral 2-port switch (ERTEC 200) and thus Profinet IO Device functionality. It is therefore highly suitable for use in networks with a line topology. The module can

Fig. 7.35
CP 343-1 Lean

also be replaced without the need for a programming device. The CP 343-1 Lean offers communication functionalities of the S7-300 with:

- Programming devices, computers, HMI devices, open IE communication (TCP/IP and UDP) as well as programming device/operator panel communication
- Other Simatic S7 systems
- Simatic S5 PLCs
- Profinet IO controllers

The CPþ343-1þLean autonomously handles the data traffic over Industrial Ethernet. Multi-protocol use of the TCP/IP and UDP transport protocols as well as Profinet IO is possible. The CPþ343-1þLean has a preset, unique Ethernet address and can be started up directly over the network. It operates in multi-protocol mode for the following communications services:

- Programming device/operator panel communication: all S7 stations connected on the network can be remote-programmed using the programming device/operator panel communication.
- S7 routing: it is possible using S7 routing to achieve cross-network use of the programming device communication.
- S7 communication: to link the S7-300 (server only) to S7-400, HMI devices and PCs (SOFTNET-S7 or CPþ1613 A2 with S7-1613).
- Open IE-compatible and S5-compatible communication: on the basis of layerþ4, the S5-compatible communication with SEND/RECEIVE offers a simple and optimized interface for data communication. Up to 8þKB data can be transmitted per call. This interface permits the use of TCP transport connections, UDP as well as Multicast for UDP. Open IE-compatible and S5-compatible communication is used for communication with Simatic S5, Simatic S7-400/300 and computers/PCs. The required function blocks are part of NCMþS7 for Industrial Ethernet and must be integrated into the S7 user program. Direct access to the CPU data of the Simatic S7 (as with the CPþ1430 TCP and SimaticþS5) is possible using S5-compatible communication with FETCH/WRITE. It is therefore possible to keep using existing HMI systems. If UDP is used as the transmission protocol, the Multicast function can be used in order to simultaneously transmit and receive data in configured Multicast circuits.
- Profinet IO Device functionality: in order to exchange data like a field device (input and output data in this case) from the user program of the S7-300 station with a Profinet IO controller, the CPþ343-1 Lean can be operated as a Profinet IO Device. This high-performance data exchange using Profinet IO communications mechanisms is handled autonomously by the CPþ343-1 Lean.
- Diagnostics: comprehensive diagnostics is provided via NCM S7, including CP operating status, general diagnostics and statistics functions, connection diagnostics, LAN controller statistics, as well as display of the diagnostics buffer. All MIB-2 objects can be read out over SNMP. The current status of the Ethernet interface can thus be called.

CP 343-1

The standard CP 343-1 permits connection of Simatic S7-300 to Industrial Ethernet. In addition to communication to other Ethernet partners, the CP as Profinet IO controller, and now also as an IO Device, also handles the connection of distributed input and output modules. As an IO controller, the CP in the machine also handles the control of distributed input and output modules. As a Profinet IO Device, the CP can exchange data like a field device with an IO controller.

The standard CP 343-1 provides powerful communication to the S5 and S7 and to OPC servers or the programming device, and thus offers the communications facilities of the S7-300 with:

- Programming devices, computers, HMI devices
- Other Simatic S7/C7 systems
- Simatic S5 PLCs
- Sinumerik 840D powerline
- Field devices (IO Devices)
- Third-party devices.

The CPþ343-1 can be used in the Sinumerik 840D powerline in order to connect the latter to Industrial Ethernet and to communicate with other automation systems, e.g. using open IE communication, S7 communication or Profinet communication.

The CPþ343-1 autonomously handles the data traffic over Industrial Ethernet. The module has its own processor. Multi-protocol mode of the TCP/IP, UDP and ISO transport protocols is possible. In order to check the connection (keep alive), an adjustable time can be configured for all TCP transport connections with active and passive partners. The CPU time can be set using NTP or Simatic procedures with an accuracy of approx. ±1þs. The module has a preset, unique Ethernet address, and can be started up directly over the network. The CP 343-1 operates in multi-protocol mode for the following communications services:

- Programming device/operator panel communication: see CP 343-1 Lean
- S7 routing: see CP 343-1 Lean
- Profinet communication:
  - Profinet IO controller: in order to link field devices over Industrial Ethernet, the CP 343-1 supports the functionality of a Profinet IO controller.
  - Profinet IO Device: in order to exchange data from the user program of the S7-300 station like a field device (input and output data in this case) with a Profinet IO controller, the CPþ343-1 can be operated as an IO Device.
  - Access using I/O data from the user program of the S7-300 station takes place using the PNIO_SEND and PNIO_RECV blocks.
- S7 communication: for linking the S7-300 (server and client) to S7-200/300/400 (server and client), HMI devices and PCs (Softnet-S7 or CPþ1613 A2 with S7-1613).

- Open IE-compatible and S5-compatible communication: see CP 343-1 Lean
- Diagnostics: see CP 343-1 Lean
- Security: a configurable IP access list can be used to specifically enable PCs and PLCs for IP-based access to the CP or controller.

CP 343-1 Advanced

The CPþ343-1 Advanced (Fig. 7.36) is the communications module for the SimaticþS7-300 for connection to Industrial Ethernet. The S7 Advanced communications modules use the advantages of Industrial Ethernet compared to the fieldbus. Since it is possible to communicate between the field level and the IT world without intermediate gateways, it is therefore also possible to implement a flat communications structure with small configuration requirements using the Advanced CPs. In many cases, communications gateways can be omitted between the field, MES and ERP levels. This reduces the configuration requirements and the possible sources of error. Like the CP 343-1, the CP 343-1 Advanced offers powerful communication with the S5 and S7 and with OPC servers or the programming device. Communication can also be programmed via TCP, and allows the integration of a wide variety of systems. The CPþ343-1 Advanced offers the communications facilities of the S7-300 with:

- Programming devices/PCs
- Host computers
- HMI devices
- Simatic S5/S7/C7 systems
- Profinet IO Devices
- Profinet CBA components

Fig. 7.36
CP 343-1 Advanced

As a Profinet controller, the CP in the machine also handles control of distributed input and output modules. The CP supports modular, object-oriented plant concepts via Profinet CBA. Important information concerning production data can be sent per e-mail. For example, the current data of individual machines can be imported via links in the Web browser to enable quality assurance analyses on Web sites. By means of the FTP protocol, the controller can fetch information directly from a mainframe or PC files via the CP for request processing. Despite IT communication, the CP 343-1 Advanced exhibits a high degree of resistance to attacks from the network. Continuous security updates are superfluous. An IP access list protects against access by non-authorized computers. Basic protection using passwords linked to persons and communications services protects against unauthorized access.

The CPþ343-1 Advanced autonomously handles the data traffic over Industrial Ethernet. The module has its own processor, and can be started up directly over the network using the preset, unique Ethernet address (MAC). Multi-protocol use of the TCP/IP and UDP transport protocols is possible. In order to check the connection (keep alive), an adjustable time can be configured for all TCP transport connections with active and passive partners. The CPU time can be set using NTP or Simatic procedures with an accuracy of approx.þ±1þs. The CPþ343-1 Advanced operates in multi-protocol mode for the following communications services:

- Programming device/operator panel communication: see CP 343-1 Lean
- S7 communication: see CP 343-1 Lean
- Open IE-compatible and S5-compatible communication: see CP 343-1 Lean
- IT functions: see CP 343-1 Lean
- Profinet communication:
  - Profinet IO controller: real-time communication (RT) with field devices on the Industrial Ethernet in line with the Profinet standard.
  - Profinet CBA: communication between technological modules (distributed intelligence); it is possible to select cyclic or acyclic communication.
- IT functions:
  - Web server; up to 30þMB freely-definable HTML pages can be called using standard browsers
  - Standard diagnostics sites for fast diagnostics on the plant for all modules inserted in the rack, without the necessity for supplementary tools
  - Sending of e-mails directly from the user program
  - Communication over FTP as an open protocol which is available on most operating system platforms
  - Intermediate storage of dynamic data using the 30þMB RAM file system
- Diagnostics: see CP 343-1 Lean. In addition: Web interface with basic diagnostics information and diagnostics buffers of the CP and CPU in plain text.
- Security: a configurable IP access list can be used to specifically enable PCs and PLCs for IP-based access to the CP or controller. Web sites can be protected using passwords.

CP 443-1 Advanced

Simatic Net-CP 443-1 Advanced (Fig. 7.37) can be used to integrate all PLCs of the Simatic S7-400 range into Profinet applications, Profinet IO and Profinet CBA. With a separate processor, it offloads the CPU from communications tasks, and permits additional connections. The module has its own powerful processor, and can be directly started up via the network with the preset, unambiguous Ethernet address (MAC address). To enable the design of small LANs or the connection of several Ethernet devices, a 4-port switch with autocrossover and autosensing has been integrated in the CP443-1 Advanced.

Fig. 7.37
CP 443-1 Advanced

CP 443-1 Advanced allows the Simatic S7-400 to communicate with:

- PG/PC
- Host computer
- HMI devices
- Simatic S5/S7/C7 systems
- Profinet CBA components
- Profinet IO Devices

CP 443-1 Advanced supports the following communications services, and offers further features:

- Profinet IO controller: direct access to IO Devices over Industrial Ethernet.
- Profinet CBA: use of a Simatic S7-400 for Component Based Automation.
- S7 communication: PG functions, HMI functions, data exchange via S7 connections.

- S5-compatible communication: SEND/RECEIVE interface via ISO transport connections or TCP connections, ISO-on-TCP and UDP connections; multicast via UDP connection, FETCH/WRITE services (server services; corresponding to S5 protocol) via ISO transport connections, ISO-on-TCP connections and TCP connections; LOCK/UNLOCK with FETCH/WRITE services.
- IT functions: send e-mail, monitor device and process data (HTML process control), FTP functions (File Transfer Protocol) for file management and access to data blocks in the CPU (client and server function).
- Time synchronization over Industrial Ethernet according to the following configured procedures: Simatic procedure: the CP receives MMS time messages, and synchronizes its local time. NTP procedure (Network Time Protocol): the CP sends time requests to an NTP server at regular intervals, and synchronizes its local time.
- Addressability using factory-set MAC address: the CP can be reached using the preset MAC address for assignment of the IP address; the CP supports the PST function (primary setup tool).
- SNMP agent: the CP supports data scanning using SNMP Version V1 (Simple Network Management Protocol) according to the MIB II standard.
- IP access protection (IP-ACL): using IP access protection it is possible to limit communication via the CP of the local S7 station to partners with specific IP addresses.
- IP configuration: it is possible to set the path or procedure with which the IP address, subnet mask and router address are assigned to the CP.
- Scan diagnostics buffer extract: the CP supports the possibility for scanning a diagnostics buffer extract of the last 10 diagnostics events of the CPUs and CP present in the same rack as the CP via Web browsers.
- S5/S7 addressing mode: the addressing mode can be configured for the FETCH/WRITE access as an S7 or S5 addressing mode.
- Recognize IP double addressing in the network: in order to avoid difficult searching for faults in the network, the CP recognizes double addressing.
- 4-port switch integrated: to enable the design of small LANs or the connection of several Ethernet devices, a 4-port switch has been integrated in the new CP 443-1 Advanced.

7.7.3 Further Profinet Products

Profinet's great breakthrough means that an increasing number of field devices with integral Ethernet interface is available in Simatic's range of modules. In addition, an increasing number of functions, tools and aids are being produced. Some of them are briefly presented here as examples.

SOFTNET PN IO

This software is used to connect PGs/PCs and notebooks to Profinet IO Devices over Industrial Ethernet. With SOFTNET PN IO, you are able to expand a network card by the required Simatic functionalities. Contrary to the procedure with a communications processor, SOFTNET executes the complete protocol stack in the PC. With this architecture, the performance depends on the design or loading of the PC used. Configuration is carried out using Step 7/NCM PC, V5.3 SP1 or later. SOFTNET PN IO is available for the following interfaces:

- CP 1612 (PCI)
- CP 1512 (PC-Card)
- Integral interfaces of Simatic PGs/PCs

If the appropriate hardware is available, the software provides the following functions:

- Profinet IO controller: interfacing of field devices with Profinet to Industrial Ethernet.
- OPC interface: the existing OPC server can be used as the standard programming interfaces for Profinet IO controllers in order to link applications from the automation engineering sector to OPC-compatible Windows applications (Office, HMI systems etc.).
- Programming interface via C library: The IO Base interface can be used for applications wishing to use the Profinet IO controller functionality directly via C/C++. The structure of this interface is based on the DP-Base interface of the Profibus CP 5613 and CP 5614 modules. Therefore portability of existing Profibus DP master applications to Profinet IO controller applications is simple.

The following compilers can be used together with SOFTNET PN IO: Microsoft Visual C/C++ V6.0, Microsoft Visual Basic V6.0, Microsoft Visual Basic V7.0.

PN-CBA-OPC server

The PN-CBA-OPC server (Profinet OPC server) is the PC application interface for communication with Profinet CBA components over Industrial Ethernet. OPC client applications communicate with the PN-CBA-OPC server over a standardized, open and therefore vendor-independent interface. The PN-CBA-OPC server offers:

- Standardized access for OPC-compatible applications and Windows applications (e.g. Microsoft Office) for synchronous and asynchronous reading and writing of variables made available through the component interface of the Profinet CBA components.
- User interface is uniform and easy to use.
- High-performance data access via the “custom interface” (C++, .NET).
- Easy to use via the “automation interface” (VB, .NET) and OCX data control for direct embedding in Windows applications supporting COM/DCOM.

- Internet communication via OPC XML-DA interface. This permits direct access to S7 CPUs over the Internet.

The PN-CBA-OPC server communicates with Profinet CBA components over Industrial Ethernet using the DCOM protocol. Open standardization of addresses is carried out using logical names for objects of an automation component or system.

IE/PB-Link PN IO

The IE/PB-Link PN IO, as an autonomous component, establishes the seamless transition between Industrial Ethernet and Profibus (Fig. 7.38). By using the IE/PB-Link PN IO as proxy, existing Profibus devices can be used further and integrated into a Profinet application.

The link operates as a compact router between Industrial Ethernet and Profibus:

- Connection to Industrial Ethernet at 10/100 Mb/s full/half duplex with autosensing for automatic switchover.
- Connection to Profibus at 9.6 Kb/s to 12 Mb/s including 45.45 Kb/s for Profibus PA.

The link also operates as a Profinet IO proxy for interfacing Profibus DP slaves to Profinet IO controllers using real-time communication (RT) according to the Profinet standard: from the viewpoint of the IO controller, all DP slaves are handled like IO Devices with Ethernet interface, i.e. the IE/PB-Link PN IO is their proxy.

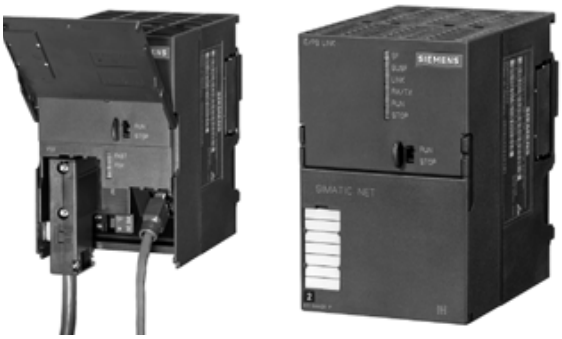


Fig. 7.38
IE/PB-Link PN IO

The link also provides the following functions:

- Cross-network PG/OP communication through S7 routing, i.e. all S7 stations can be remote-programmed by the PG on the Industrial Ethernet or Profibus. Cross-network access to data of S7 stations is carried out using S7 OPC servers and S7 routing. Access is possible from HMI stations on the Industrial Ethernet to visualization data of S7 stations on the Profibus.
- Data record routing (Profibus DP): By means of this option, the IE/PB-Link PN IO can be used as a router for records intended for field devices (DP slaves). One tool which generates such records for parameterization and diagnostics of field

devices is the Simatic PDM (Process Device Manager). It is then possible, for example, to carry out parameterization and diagnostics for a Profibus PA field device using Simatic PDM (on the PC) on the Industrial Ethernet via the IE/PB-Link PN IO and a DP/PA coupler.

- Using the IE/PB-Link PN IO, all data of S7 stations on the Profibus can be accessed by the PC on the Industrial Ethernet (e.g. for HMI applications with OPC client interface) using an S7 OPC server.
- Devices are replaced without a PG through use of the interchangeable medium C-Plug for saving the configuration data.
- Diagnostics: comprehensive diagnostics is made available using Step 7 or SNMP, including diagnostics of the assigned Profinet field devices; the connected DP slaves can be diagnosed like Profinet IO Devices (also in the user program of the Profinet IO controller) via the IE/PB-Link PN IO as proxy. The following are made available: general diagnostics and statistics functions, connection diagnostics, LAN controller statistics, diagnostics buffer, integration into network management systems through support of SNMP V1 MIB-II.

DP/AS-i LINK Advanced

The IE/AS-i LINK Advanced (Fig. 7.39) permits a Profinet IO Master to cyclically access the I/O data of all slaves of a subordinate AS-i segment. According to the enhanced AS-i specification (V3.0), a maximum of 62 slaves with four inputs and four outputs each as well as analog slaves can be connected per AS-i line.

Fig. 7.39
IE/AS-i LINK Advanced

The DP/AS-i LINK Advanced is thus ideally suitable for the distributed design and for linking a subordinate AS-i network. User-friendly diagnostics and commissioning can be carried out on site using a pixel graphics display and input keys or via the integral Web interface using a remote standard browser.

The device is available in two versions:

1. Single master: device with one AS-i line
   (maximum number of connectable AS-i slaves: 62)
2. Dual master: device with two AS-i lines
   (maximum number of connectable AS-i slaves: 124)

Profinet IO controllers can also trigger AS-i master calls using the acyclic Profinet services (e.g. write parameters, change addresses, read diagnostics values).

The subordinate AS-i line can be completely started up using an input display on the AS-i link. The IE/AS-i Link PN IO is equipped with two switched Ethernet ports which additionally permit use of the integral Web server and thus increase the operating convenience of the input display described above even further. Firmware updates are also possible. The optional C-Plug supports module replacement without the use of a programming device, thus reducing downtimes to a minimum.

CPU 31x-x PN/DP: The latest generation of these CPU modules for S7 controllers contains at least one integral Ethernet interface (Fig. 7.40). They are used in plants containing distributed automation structures in addition to the central I/O. They are used for example as the central controller in production lines or as a machine controller with high demands on the processing speed. Devices have a combined MPI/DP interface and at least one Ethernet interface. The latter is a Profinet interface based on Ethernet TCP/IP. The integral communications functions of the CPU mean that networked automation solutions are possible without additional components. The following properties are usually characteristic of the new generation of controllers:

- CPU with high command processing performance, large program memory and quantity framework for complex applications.
- Suitable for cross-industry automation tasks in series machine, special machine and plant construction.

Fig. 7.40
CPU module 319-3 PN/DP
with combined MPI/DP interface,
DP interface and Ethernet interface

- Use as central controller in production lines with central and distributed I/O on Profibus and Profinet.
- Distributed intelligence in Component Based Automation (CBA) on Profinet.
- Profinet proxy for intelligent devices on the Profibus DP in Component Based Automation (CBA).
- Isochronous mode on the Profibus.
- Provides optional support for use of Simatic engineering tools.
- The integral interface of the controllers is usually a Profinet interface based on Ethernet TCP/IP. It supports the following protocols:
  - S7 communication for data exchange between Simatic controllers.
  - Programming device/operator panel communication for programming, commissioning and diagnostics using Step 7.
  - Programming device/operator panel communication for linking to HMI and Scada (supervisory control and data acquisition).
  - Open TCP/IP, UDP and ISO-on-TCP (RFC1006) communication over Profinet.
- Simatic Net OPC server for communication with other controllers and I/O devices with their own CPU.
- The CPUs 315-2 PN/DP, 315F-2 PN/DP, 317F-2 PN/DP, 319-3 PN/DP can be referred to as examples with the functionalities described above. Details on the modules can be obtained from the relevant manual.

ET 200 X with PN interface module: The Simatic ET 200 is a distributed I/O device with Ethernet connection. It comprises:

- Interface module with Profinet interface
- Input/output modules (digital and analog sensors and actuators)

Fig. 7.41 ET 200S Profinet two-port interface modules IM 153-3, IM 151-3 PN FO for ET 200S, ET 200pro with Profinet connection

- Technology modules
- Frequency converters and motor starters for three-phase loads.

The comprehensive range of modules as well as uniform handling for configuration, assembly and programming allow the ET 200 to be used as a universal I/O system. A central controller can access the I/O modules of the ET 200 via Profinet just like central I/O modules. The interface module permits linking of the ET 200 to Profinet, and autonomously handles communication between the modules and the host Profinet I/O Controller.

Linking to Ethernet can be carried out optically or electrically in a number of different ways. Examples include the IM 151-3 PN (interface module for direct connection of the ET 200S as an IO Device, with integral two-port switch for line topology, also using fiber-optic cables) and IM 154-4 PN (interface module for direct connection of the ET 200pro as an IO Device with integral switch for line topology and high IP65/IP67 degree of protection) (Fig. 7.41). A number of versions are also available for a wide range of applications, such as ET200 S or ET200 Pro with Ethernet interface (Profinet).

PC-based Control with Profinet

WinAC software PLCs are particularly suitable for tasks requiring high flexibility and effective integration into the complete task. This includes close association with data processing or logistics systems, as well as linking to technological tasks, e.g. motion control or vision systems. The Windows Logic Controller (WinLC) handles the actual control task, and controls execution of the program. It coordinates the required input and output of process values via the subordinate Profibus fieldbus system, and provides the process values for visualization and data processing tasks.

Several processing levels are available for optimum control of processes, such as cyclic program execution, interrupt processing, and time/date-controlled processing.

By means of the WinAC-PN option, WinAC Basis can be used as the automation component – based on Profinet CBA – and therefore supports data exchange with other Profinet CBA-compatible devices over Industrial Ethernet. This results in the following additional applications for WinAC Basis:

- Coordination and linking of machines and plant sections which are to be connected together into a complex complete plant.
- Control of a machine or plant section which is to be integrated into a complete plant.
- PN proxy functionality for Profibus devices connected on the Profibus segment of WinAC Basis.

7.7.4 Fundamental Information on Hubs and Switches

Hub

A hub always copies the information received on the line to the respective other side, and amplifies it again to a normal output level. The term refers to almost all amplifier components which permit a star topology. A hub receives a data packet at one port, and directs it on to all occupied output ports (Fig. 7.42). Therefore all ports are occupied in the event of data traffic.

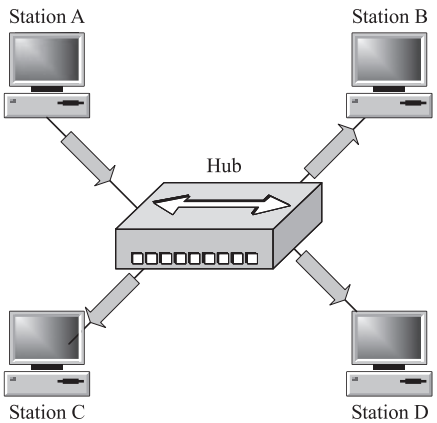


Fig. 7.42
A data package from station A is passed on to all connected stations B, C, D

A segment generated using hubs is called a “shared segment” since all stations of the hub share a segment of the LAN. Hubs currently contain at least one additional port for connecting a further network segment, e.g. an additional hub.

Never use hubs for Profinet networks, but exclusively switches. In contrast to a switch, a hub sets itself to the lowest speed at the ports, and passes on the signals to all connected devices. In addition, a hub cannot assign priorities to signals. This results in a very high communications load on the Industrial Ethernet. Data can only be transmitted collision-free when certain further conditions exist.

Switch

Profibus is a linear network. The communication stations are connected by a passive line, the bus. In contrast to this, Industrial Ethernet consists of point-to-point connections: each communication station is directly connected to exactly one other communication station. If one station is to be connected to several other stations, it is connected to the port of an active network component – the switch. Further communication stations (also switches) can then be connected to the other ports of the switch. The connection between a communication station and the switch still remains a point-to-point connection. A switch only passes on a record to the addressed station. Only connect a maximum of one Profinet device or one further switch to each port.

Switches have the following main functions:

- Connection of collision domains or subnets: since repeaters and star couplers (hubs) work in the physical layer, their application is limited to expansion of a collision domain. Switches connect collision domains. Their use is therefore not limited to the maximum expansion of a repeater network. On the contrary, very large networks with distances of 150 km can be produced with switches, and even up to 1300 km when using LD modules. Switches prevent the collision of data packets.
- Load decoupling: by filtering the data traffic using the Ethernet (MAC) addresses, it is ensured that local data traffic remains local (Fig. 7.43). In contrast to repeaters or hubs, which distribute data unfiltered to all ports/network stations, switches operate according to the direct switching procedure. Only data to stations of another subnet are transported further from the input port to the corresponding output port of the switch. For this purpose, the switch generates an assignment table of Ethernet (MAC) addresses to output ports in self-learning mode. Switches therefore use the Ethernet addresses to determine where the individual devices are connected, and use this knowledge to switch all subsequent data packets.

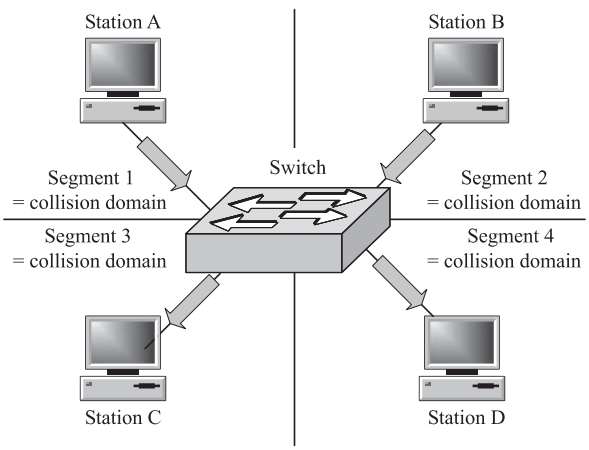


Fig. 7.43
A data packet from station A is only passed on to station D. At the same time, stations B and C communicate with one another

- Limitation of errors spreading to a subnet: by checking the validity of a data packet by means of the checksum present in each packet, the switch guarantees that faulty data packets are not transported further. In addition, collisions in a network segment are not passed on to other segments.
- Conversion of different connection speeds: data terminals with 10-Mb Ethernet and 100-Mb Fast Ethernet can communicate with each other in one LAN. On the other hand, only devices with the same speed can be connected to a hub. A switch has a specific number of ports.

Profinet only uses devices with a switch functionality as signal distributors. To permit use in the Profinet network, a switch must at least have the following functionalities:

- Support of Ethernet according to ISO/IEC 8802-3 (10/100 Mb/s)
- Support of Ethernet according to IEEE 802.1D and IEEE 802.1Q
- Support of standardized diagnostics paths
- Full duplex mode
- Support of autocrossover function.

7.7.5 Switches for Industrial Use: Scalance X

Scalance X is the new product range of Simatic Net industrial switches for Industrial Ethernet. Switches are active network components which specifically distribute data to the corresponding addresses.

Industrial networks place high demands on the switches used. Standard devices from the office sector cannot provide the required functions. For example, fast in-

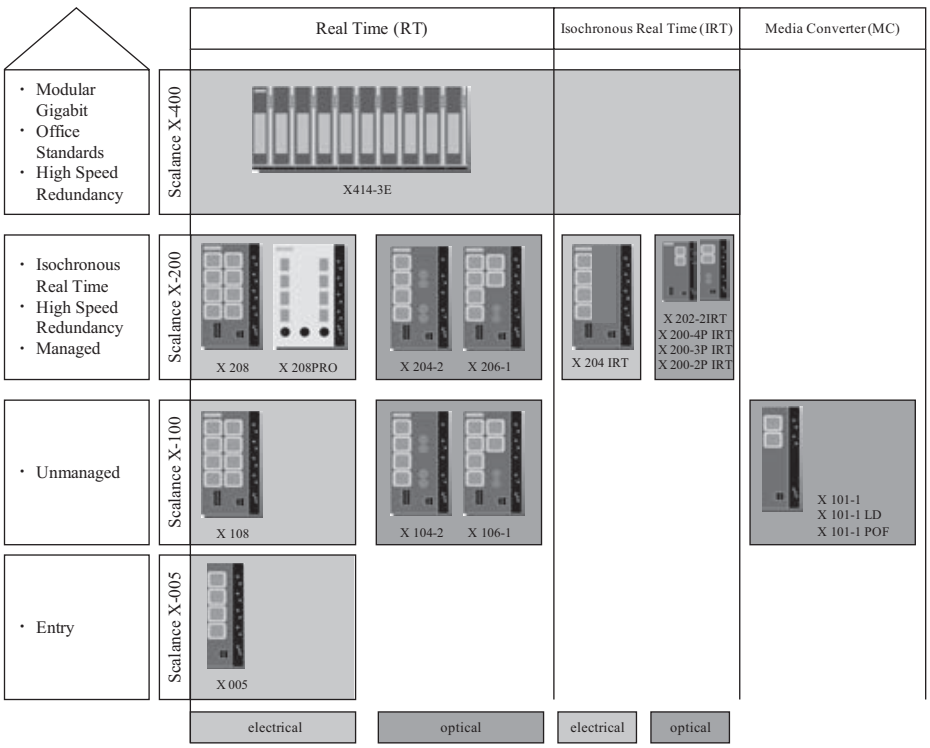


Fig. 7.44
The Scalance X range sorted according to optical and electrical interfaces as well as performance classes and RT/IRT functionality

dustrial applications require an extremely reliable and fast redundancy mechanism should a network component fail. Redundant networks increase the total security, and minimize plant downtimes. The Scalance X range offers high-speed redundancy for activation of replacement links in less than 0.3 seconds. This makes a major contribution to the failsafety of the network. Industrial switches permit the design of large networks with many stations, increase the data throughput, and simplify expansion of the network.

In addition to fast redundancy, network management and diagnostics are also of decisive importance. Scalance X offers the facility for permanent monitoring of network components using signaling contact, Profinet diagnostics or network management. Any problems occurring can be rapidly detected and eliminated by both the network administrator and the automation system. Generation and operation of networks are simple through integration into the existing Simatic engineering. Operators are provided online with important details which permit preventive maintenance of their network.

In order to handle high data quantities, it is necessary for the devices to process increasingly high data rates. The performance of networks for Industrial Ethernet can be matched to the respective requirements. As a result of the uniform compatibility – which safeguards investments when introducing new technologies – as well as the scalability of a matched product range, the devices always provide an adequate performance and configuration for many different tasks.

The range of Simatic Net Scalance X industrial switches currently consists of three matched families which are tailored to the respective automation task (Fig. 7.44).

Fig. 7.45
Overview of the Scalance X range

- **Scalance X005 entry level:** unmanaged switch with five RJ45 ports for use in machine and plant islands.
- **Scalance X100 unmanaged:** switches with up to eight ports and local diagnostics for use in applications at machine level.
- **Scalance X200 managed:** for universal use, from applications at machine level up to networked plant sections. Configuration and remote diagnostics are integrated in the Simatic Step 7 engineering tool. This increases plant availability. Devices with a high degree of protection need not be installed inside cabinets.
- **Scalance X200 IRT managed:** for use in plant section networks with strict real-time requirements (isochronous real-time) and maximum availability. Data transfer without real-time requirements can take place on the same network, making duplicate network structures unnecessary.
- **Scalance X400 modular:** for use in high-performance plant networks which also have to satisfy future requirements (e.g. high-speed redundancy). The modular design of the switches means they can be adapted to the respective task. Supporting of Office standards means that seamless integration of automation networks is possible into existing office networks.

Scalance X005

The Scalance X005 Industrial Ethernet entry level switch (Fig. 7.46) is suitable for the low-cost design of small Industrial Ethernet networks with 10/100 Mb/s and a line or star topology. The Scalance X005 is an unmanaged switch. It possesses the autosensing function for detection of the data transfer rate, and has five electrical RJ45 ports with 10/100 Mb/s and securing collar. These are designed for rugged, industry-compatible connection of stations with the matching Industrial Ethernet FastConnect RJ45 Plug 180 with strain and bending relief, and are thus suitable for the electric connection of stations or networks. It provides additional diagnostics on the device by means of LEDs (power, link status, data traffic). The use of un-

Fig. 7.46
Scalance X005

crossed cables is possible by means of the integral autocrossover function for automatic detection of the data transfer rate (10 or 100 Mb/s).

The Scalance Industrial Ethernet switches with rugged metal enclosure (IP30) have been optimized for assembly on standard and S7-300 rails. Direct wall assembly is also possible in various positions. The enclosure dimensions correspond to those of the Simatic S7-300, making the devices optimally suitable for integration in an automation solution with S7-300 components.

The Scalance X005 switch features the following:

- Power supply (1 × 24 V DC)
- LED row for display of status information (power, link status, data traffic)
- 10/100Base-TX, RJ45 connection
- RJ45 socket, automatic detection of data transfer rate (10 or 100 Mb/s), with autosensing and autocrossover functions for connection of IE FC cables via IE FC RJ45 Plug 180 for distances up to 100þm.

Scalance X100

Scalance X100 provides economy in applications at machine level. The switches specially designed for application in harsh industrial environments have up to eight ports and local diagnostics. The compact design and assembly on standard and S7-300 rails permit space-saving assembly in the control cabinet. The device plugs have the collar securing concept conforming with Profinet. Examples of possible configurations of the Scalance X100 range (Fig. 7.47):

- Industrial Ethernet Scalance X108: switch with eight 10/100-Mb/s RJ45 ports for design of star topologies
- Industrial Ethernet Scalance X104-2: switch with four 10/100-Mb/s RJ45 ports and two fiber-optic ports for design of star topologies
- Industrial Ethernet Scalance X106-1: switch with six 10/100-Mb/s RJ45 ports and one fiber-optic port for design of star topologies.

Fig. 7.47
Scalance X104-2, X106-1, X108

Scalance X100 is a plug-and-play device which does not require any settings for commissioning. The Scalance X100 and X200 all support the MDI/MDIX autocrossover and autonegotiation functions.

It is possible to connect TP Cords or TP-XP Cords with a maximum length of 10 m to the TP port of the RJ45 version of the Scalance X100 and X200 ranges. In conjunction with the IE FC Outlet RJ45, a total line length of 100 m is permissible. In conjunction with the IE FC Standard Cable and IE FC RJ45 Plug 180, a total line length of 100 m is possible between two devices.

Permissible line lengths for connections using Industrial Ethernet FC-TP cables:

- 0-100 m: Industrial Ethernet FC-TP Standard Cable with IE FC RJ45 Plug 180 or via Industrial Ethernet FC Outlet RJ45 with 0-90 m Industrial Ethernet FC-TP Standard Cable + 10 m TP Cord.
- 0-85 m: Industrial Ethernet FC-TP Marine/Trailing Cable with IE FC RJ45 Plug 180 or 0-75 m Industrial Ethernet FC-TP Marine/Trailing Cable +10 m TP Cord.

The number of Industrial Ethernet Scalance X switches connected influences the throughput time of a frame. When a frame passes through the Scalance X100 and/or Scalance X200, it is delayed by the store-and-forward function of the switch – by approx. 10 µs with a frame length of 64 bytes (at 100 Mb/s), and by approx. 130 µs with a frame length of 1500 bytes (at 100 Mb/s). This means that the throughput time of a frame increases as it passes through more and more Scalance X100 and/or Scalance X200 switches.

The Scalance Industrial Ethernet switches with rugged metal enclosure have been optimized for assembly on standard and S7-300 rails. Direct wall assembly is also possible in various positions. The enclosure dimensions correspond to those of the Simatic S7-300, making the devices optimally suitable for integration in an automation solution with S7-300 components. The Scalance X100 switches feature the following:

- 4-pin terminal block for connection of the redundant power supply (2×4 V DC)
- LED row for display of status information (power, link status, data traffic, signaling contact)
- 2-pin terminal block for connection of the floating signaling contact
- SET key for on-site configuration of the signaling contact.

The following types of ports are available:

- 10/100Base-TX, RJ45 connection: RJ45 socket, automatic detection of data transfer rate (10 or 100 Mb/s), with autosensing and autocrossover functions for connection of IE FC cables via IE FC RJ45 Plug 180 at distances up to 100þm
- 100BaseFX, BFOC connection system: BFOC sockets for direct connection to Industrial Ethernet glass fiber-optic cables at distances up to 3,000þm for designing line and star topologies.

Scalance X200

These devices are suitable for applications at machine level and also for networked plant sections. Assembly is either on standard or S7-300 rails. Devices with a high degree of protection also permit installation outside the control cabinet. The collar securing concept conforming with Profinet also secures the connectors in this case. Scalance X200 is available in versions with electrical and/or optical ports. Integration of configuration and remote diagnostics into the Simatic Step 7 engineering tool results in significant advantages from planning right up to operation.

Standard remote diagnostics functions such as SNMP and Web server have been incorporated. This range of devices permits applications with strict real-time requirements and maximum availability. Some of the switches from the Scalance X200 range can be configured, diagnosed and addressed as Profinet IO Devices if the switch has been incorporated into Step 7 by means of a GSD file. To assign the IP address, the primary setup tool (PST) can be used as an alternative to Step 7 for the switches. The devices offer integral Profinet diagnostics. Examples of possible configurations of the Scalance X200 range (Fig. 7.48):

- Industrial Ethernet Scalance X208: switch with eight 10/100-Mb/s RJ45 ports for design of star topologies with integral SNMP access, Web diagnostics, copper cable diagnostics and Profinet diagnostics
- Industrial Ethernet Scalance X206-1: switch with six 10/100-Mb/s RJ45 ports and one fiber-optic port for design of star topologies with integral SNMP access, Web diagnostics, copper cable diagnostics and Profinet diagnostics
- Industrial Ethernet Scalance X204-2: switch with four 10/100-Mb/s RJ45 ports and two fiber-optic ports for design of star topologies with integral SNMP access, Web diagnostics, copper cable diagnostics and Profinet diagnostics
- Industrial Ethernet Scalance X208PRO: switch with eight 10/100-Mb/s RJ45 ports for design of star topologies with integral SNMP access, Web diagnostics, copper cable diagnostics and Profinet diagnostics.
- Industrial Ethernet Scalance X204-2 LD and X206-1 LD switches: these devices possess the known functions and interfaces of the X200 range, and are especially designed for transmission links up to 26þkm (long distance) with singlemode fiber-optic cables.

The C-Plug is used with these devices. It functions as an interchangeable medium for saving the configuration and programming data of the basic device. The configuration data is then still available when the basic device is replaced. On an unwritten C-Plug (factory state), all configuration data of the Scalance X200 are automatically saved during the device startup. In addition, changes in the configuration during runtime are saved on the C-Plug without an operator intervention. A basic device with an inserted C-Plug automatically uses the configuration data of the C-Plug during startup. A prerequisite is that the data have been written by a compatible type of device. This permits fast and simple replacement of the basic device in the event of a fault. When replacement is necessary, the C-Plug is simply

Fig. 7.48
Scalance X204-2, X206-1, X208, X208PRO

removed from the faulty device and inserted into the replacement device. Following the initial startup, the replacement device automatically has the same configuration as the failed device, apart from the specific MAC address specified by the vendor.

In the case of the devices with optical ports, the transmission rate is 100 Mb/s. Since the full duplex procedure and the transmission rate cannot be changed in the case of optical transmission, autonegotiation cannot be selected. Data transmission is on multimode FOCs. The wavelength is 1310 nm. Multimode FOCs are used with a core diameter of 50 or 62.5 µm, the light source is an LED. Many modes (light beams) are used for the signal transmission. The outer diameter of the FOC is 125 µm. The maximum transmission range (segment length) is 3 km. The BFOC sockets are used for the connection.

By means of Web-based management, the Industrial Ethernet switches of the Scalance X200 range offer various diagnostics functions which can be accessed using an Internet browser (e.g. Microsoft Internet Explorer or Netscape). Operation is carried out using a Java script which is saved in the Industrial Ethernet switches of the Scalance X200 range and downloaded by the browser.

Profinet IO diagnostics: one possibility for diagnostics, parameterization and generation of interrupts for the connected Scalance X200 devices is use of Profinet IO. In order to integrate the individual switches as PN IO Devices, it is necessary for the devices of the Scalance X200 range to be present in the module catalog under Profinet IO. In order to incorporate the devices of the Scalance X200 range for the first time, you must install the GSD files according to the manual of the Scalance range. You can then carry out all settings and diagnostics for the devices in Step 7.

Scalance X200 IRT

These devices are suitable for use in plant section networks with strict real-time requirements (isochronous real-time) and maximum availability. Data transfer without real-time requirements can take place on the same network, making duplicate network structures unnecessary. Based on Profinet, the Scalance X200 IRT switches fulfill the real-time requirements of the field level up to high-performance motion control applications such as:

- Linking of Profinet IO Devices to the Profinet IO controller by means of high-performance, deterministic data transmission.
- Isochronous real-time communication based on the IEEE 802 transmission procedure, through combination of the switching mechanisms “Cut through” and “Store and forward”. Profinet with isochronous real-time is the most powerful system worldwide with respect to deterministics and isochronous mode for drive controls. With a cycle time of 1 ms and a jitter < 1 µs, it is possible, for example, to control 150 axes in isochronous mode, while 50% of the bandwidth is still available for IT communication without limitations at the same time.
- Coexistence of strict real-time and IT openness: increased availability through redundant transmission with bumpless switchover for real-time data.

The Scalance X200 IRT modules are available with the following types of port:

- 10/100Base-TX, RJ45 connection: RJ45 socket, automatic detection of data transfer rate (10 or 100 Mb/s), with autosensing and autocrossover functions for connection of IE FC cables via IE FC RJ45 Plug 180 at distances up to 100 m.
- 100BaseFX, BFOC connection system: BFOC sockets for direct connection to Industrial Ethernet glass fiber-optic cables at distances up to 3,000þm for designing line and star topologies.
- 100BaseFX, SC RJ connection system: SC RJ sockets for connection to the Industrial Ethernet POF cables (50þm) and PCF fiber-optic cables (100þm) via SC RJ plug connectors.

The Scalance X200 IRT devices satisfy the special automation requirements with regards to line topology, strict real-time and IT openness within one technology based on the Profinet standard. The following product versions are available:

Scalance X204 IRT (Fig. 7.49): for design of electrical Industrial Ethernet line, star or ring topologies with four electrical ports. Length of TP cable between two Scalance X switches: max. 100þm with IE FC cable and IE FC RJ45 Plug 180, and max. 10þm with TP cord.

Scalance X202-2 IRT: for design of optical Industrial Ethernet line, star or ring topologies with two optical ports and two electrical ports. Length of optical cables: max. 3,000þm with Industrial Ethernet glass fiber-optic cables.

Scalance X202-2P IRT: for design of optical or electrical Industrial Ethernet line, star or ring topologies with two optical POF fiber-optic ports and two electrical ports. Length of optical POF fiber-optic cables: max. 50þm.

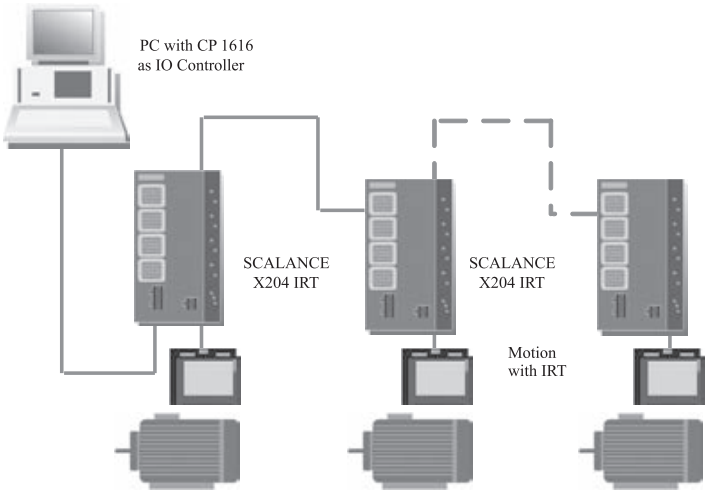


Fig. 7.49 Example configuration with Scalance X204 IRT

Scalance X201-3P IRT: for design of optical Industrial Ethernet line, star or ring topologies with three optical POF fiber-optic cable ports and one electrical port.

Scalance X200-4P IRT: for design of optical Industrial Ethernet line, star or ring topologies with four optical POF fiber-optic ports.

Additional key data of the Scalance X200 IRT devices compared to the Scalance X200 series:

- Designed especially for real-time (RT) and isochronous real-time (IRT) Industrial Ethernet networks with line, star or ring topologies with 10/100 Mb/s (RM integrated); redundant ring connections can be provided.
- Combination of the switching mechanisms “Cut through” and “Store and forward” for optimum performance.

Scalance X400 – the modular high-performance switches

Scalance X400 devices are dimensioned for use in high-performance plant networks including Gigabit Ethernet which must already be equipped today for high future requirements. Through the modular design, the switches can be exactly matched to the respective task.

The basic device consists of a frame, power supply, digital inputs and a switch CPU. The Scalance X400 range consists of modular Industrial Ethernet switches, medium modules and extenders. The system offers a modular design for the required ports. This modularity facilitates the design and subsequent expansion of complex network topologies using expansions specific to requirements. 100-Mb and 1000-Mb technologies are supported for various transmission media (twisted-pair, fiber-optic) and increased port requirements. Scalance X400 provides electrical

ports which can be used as Gigabit and ring ports. Expansion by media modules provides additional optical ports. Assembly is on standard and S7-300 rails. Supporting of Office standards means that seamless integration of automation networks is possible into existing office networks. The devices offer integral Profinet diagnostics.

Scalance X414-3E: The Industrial Ethernet Scalance X414-3E switch is the core of the Scalance X400 range. It contains the switching functionality, and is responsible for diagnostics.

In addition to two integral Gigabit Ethernet twisted-pair ports (10/100/1000 Mb/s, RJ45 sockets) for interconnection of the Scalance X400 switches and twelve integral Fast Ethernet twisted-pair ports (10/100Mb/s, RJ45 sockets with securing collar), the Scalance X414-3E has one slot for optical Gigabit Ethernet media modules with two ports, as well as two slots for optical Fast Ethernet media modules with two ports.

By means of an extender interface, the Scalance X414-3E can be expanded by a further eight Fast Ethernet ports (twisted-pair or fiber-optic depending on the extender version). This permits a maximum configuration with two Gigabit Ethernet ports (electrical or optical) and up to 24 Fast Ethernet ports (of which 4 to 12 are optical ports). The maximum mounting width together with the extender is 19 inches.

In the respective slots, the modules of the motherboard have the following functions (Fig. 7.50; slot 1 is reserved for a power supply unit):

- Slot 2: power module – the input voltage of 24 V DC is transformed into the internal supply voltage. The module has two 4-pin sockets for connecting a redundant power supply as well as the signaling contact and protective earth. The 110/220þV AC supply can be converted by appropriate S7-300 power supply units to 24þV DC.

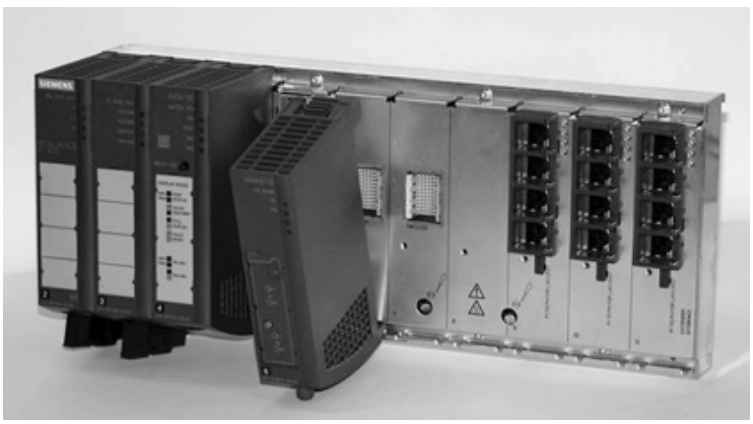


Fig. 7.50 Basic device without media modules, caps and covers

- Slot 3: digital input module – the input module has two 5-pins sockets for connecting eight digital inputs which permit various signaling modes. The floating inputs are used to record digital status information such as signaling contacts from Profibus OLM or door contacts, and passing on via Scalance X400 diagnostics routes (LED display, log table, trap or e-mail).
- Slot 4: CPU module – contains the processor which provides the management functionality.
  - C-Plug for saving the parameter settings and for simple device replacement (included in scope of delivery).
  - DIP switches for redundancy manager function and for defining the ring ports.
  - SELECT/SET keys for switching over the display modes, for resetting to the default settings, and for definition of the signaling window.
  - Comprehensive mode and status information is displayed on LEDs and selection keys.
  - Console port (serial interface) and out-band Ethernet port for on-site parameterization/diagnostics and for firmware update.
  - Floating signaling output for simple display of faults.
- Slot 5: contains two RJ45 sockets which permit electrical (twisted-pair) connections (10, 100, 1000 Mb/s). As an option, slot 5 allows the use of an optical Gigabit module with two ports (1000Base-SX or 1000Base-LX).
- Slots 6 and 7: optional use of two optical Fast Ethernet modules (100 Mb/s) with two ports each (100Base-FX).
- Slot 8: Due to system, no function.
- Slots 9 to 11: each contain four RJ45 sockets which provide a total of 12 electrical (twisted-pair) connections (10, 100 Mb/s). Occupation by media modules is not possible.

Scalance X400 media modules (MM): Using media modules, the Industrial Ethernet ScalanceþX414-3E switch can be equipped with fiber-optic cables. Media modules are available for both multimode and single mode fiber-optic cables. They can be added or replaced during operation. The Scalance X414-3E basic device supports two optical Gigabit Ethernet ports plus up to four optical Fast Ethernet ports. The following media modules are available:

- MM491-2: two fiber-optic ports (BFOC sockets) 100 Mb/s for distances up to 3þkm with multimode FOC
- MM491-2LD: two fiber-optic ports (BFOC sockets) 100 Mb/s for distances up to 26þkm with single mode FOC
- MM492-2: two fiber-optic ports (SC sockets) 1 Gb/s for distances up to 750þm with multimode FOC (when using Simatic NET FO Cable 50/125þµm)
- MM492-2LD: two fiber-optic ports (SC sockets) 1 Gb/s for distances up to 10þkm with singlemode FOC.

An inserted media module for Gigabit Ethernet converts the two Gigabit Ethernet twisted-pair ports present in the switch to optical. The two Gigabit ports can then be optionally used as twisted-pair or fiber-optic ports. Optical media modules for Fast Ethernet each generate two additional ports per slot.

Scalance X400 extender modules (EM): an optional extender module with up to eight further Fast Ethernet ports can be mounted next to the expansion interface of the Scalance X414-3E. The following versions are available:

- EM495-8 with eight twisted-pair ports (RJ45 sockets with securing collar) 10/100 Mb/s. The twelve onboard Fast Ethernet twisted-pair ports of the Scalance X414-3E can then be expanded to a total of 20 ports.
- EM496-4 with four additional media module slots for Fast Ethernet media modules for up to eight optical Fast Ethernet ports (Fig. 7.51).

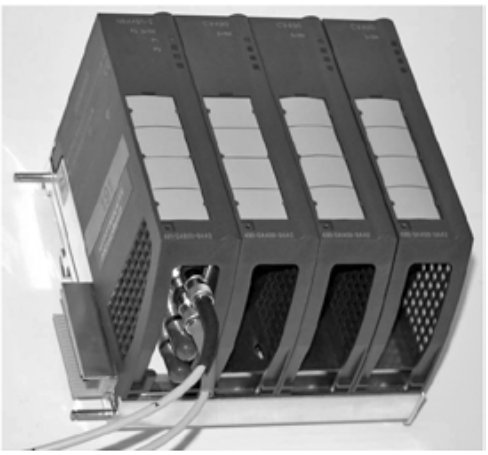


Fig. 7.51
EM496-4 extender module with MM491-2 media module

The design of the Scalance X400 range offers the following advantages:

- Simple connection of stations using twisted-pair cables
- Gigabit Ethernet transmission rate between Scalance X400 switches
- FOC connection using fiber-optic media modules
- Reduced costs for the stocking of spare parts; electrical and optical versions are covered by one basic device and FOC media modules.

Functions and characteristics of the Scalance X400 range:

- The Scalance X400 range comprises modular Industrial Ethernet switches which can be expanded by various media modules and extenders. 10/100/1000 Mb technologies are supported for various transmission media (twisted-pair, fiber-optic) and increased port requirements. The main application range is for high-performance plant networks (control level). Through the modular design,

the X400 range can also be designed for future requirements and can be matched to the respective task.

- The X414-3E switch (Fig. 7.52) has two integral Gigabit Ethernet twisted-pair interfaces (10/100/1000 Mb/s) for interconnecting several switches. Stations are connected using twelve Fast Ethernet ports (10/100 Mb/s) integrated in the switch.
- A further eight stations can be connected via an 8-port Fast Ethernet twisted-pair extender which is docked on the right of the switch.
- The integral redundancy manager also permits fast media redundancy for large networks, both for Gigabit Ethernet (Scalance X400 switches in the ring) and Fast Ethernet (Scalance X400 switches in the ring in combination with Scalance X200 switches or OSM/ESM).
- To produce optical Gigabit Ethernet rings, the two integral Gigabit Ethernet ports can be converted to fiber-optic via a 2-port Gigabit Ethernet media module. Module versions are available for multimode (up to 750þm FOC length) and single mode (up to 10þkm).
- By means of a plug-in 2-port Fast Ethernet media module for multimode or alternatively single mode FOC, Scalance X400 switches can also be integrated in 100-Mb/s rings e.g. with Scalance X204-2 or OSM.
- A second plug-in 2-port Fast Ethernet FOC media module permits optical linking of remote stations.
- Remote diagnostics is possible using Profinet diagnostics (available soon), Web browsers or SNMP.
- Switches from the Scalance X400 range support IT standards, and thus permit seamless integration of automation networks into existing corporate networks. Virtual networks (VLANs) can be established.
- Supporting of standardized redundancy procedures (Rapid Spanning Tree Protocol) permits redundant integration into host enterprise networks.

Fig. 7.52 Scalance X414-3E

- By learning of the multicast sources and destinations (IGMP, Internet Group Management Protocol, snooping), X400 switches can also filter multicast data traffic and thus limit the load on the network.
- Layer-3 routing (static, RIP v1/2, OSPF) permits communication between different IP subnets.
- The basic device consists of a rack, a power supply, digital inputs and a switch CPU.
- Scalance X400 offers a modular design for the required ports. This modularity facilitates the design and subsequent expansion of complex network topologies by means of expansions in line with requirements.
- Gigabit technology: the basic device offers connections with a transmission rate of 1 Gb/s for electric cables (twisted-pair) or, when expanded by a Gigabit media module, for fiber-optic cables.
- Splitting: splitting of the ring port between two different slots is possible for Scalance X400, and operation as a line topology can be retained should a media module fail.
- Online module replacement: a faulty module can be replaced during operation.
- Diagnostics: remote diagnostics is possible via Web-based Management, TELNET or SNMP. The basic device provides a signaling contact and local operation. An Ethernet interface is available for diagnostics and for management purposes.
- C-Plug: easy importing of configuration data is possible through further use of the C-Plug following replacement of the basic device.
- VLAN: the devices provide port-based support for VLANs. A physically existing network can be divided into several virtual networks. This results in a lower network load compared to other defined VLANs.
- Spanning Tree/Rapid Spanning Tree: Scalance X400 can process both the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP). Circling frames are thus prevented, and an alternative path is rapidly provided in the event of a fault. The reconfiguration time is 20-30 seconds with spanning tree, and one second with rapid spanning tree.

Scalance X100 unmanaged media converter

Media converters are devices used in networks to combine segments comprising different media (copper, fiber-optic), and thus physically convert the transmitted data from one medium to the other (see Table 7.5). Enormous improvements in the size of the network can then be achieved. Media converters usually work at the first layer of the OSI model.

The media converters from the Scalance X100 range permit conversion of various transmission media in the industrial environment. They are used to convert electrical signals into optical signals within Industrial Ethernet line, star and ring to-

Table 7.5 Summary of available media converters with associated interfaces

Cable type/transceiver wavelength	Device type, interface				
	X101-1	X101-1FL	X101-1LD	X101-1POF	X101-1AUI
TP(RJ45)	X	X	X	X	X
Multimode fiber (BFOC)/1300þnm	X				
Multimode fiber (BFOC)/820þnm		X			
Long Distance single mode fiber (BFOC)/1310þnm			X		
Plastic optical fiber (SC-RJ)/650þnm				X	
AUI interface					X

pologies. They are designed for use in a control cabinet. Individual, remote terminal equipment or network segments can be connected via the optical path of the Scalance X100 media converters. Integration of an optical path into a redundant ring is also possible, as well as integration of the Scalance X100 media converters into a standby link.

The Industrial Ethernet Scalance X101-1 and Scalance X101-1LD media converters possess:

- An electrical 10/100þMb/s RJ45 port. The electrical RJ45 socket is of industry design with an additional securing collar. It is used to connect the IE FC RJ45 plugs. Detection of the data transfer rate (10 or 100 Mb/s) is carried out automatically by means of autosensing and autocrossover functions for the connection of IE FC cables via IE FC RJ45 plugs. TP cords or TP-XP cords with a maximum length of 10þm can be connected to the TP port of RJ45 design. Depending on the type of cable, a total length of up to 100 meters is possible between two devices using the IE FC cables and IE FC RJ45 plug 180.

Fig. 7.53
Scalance X101-1 and X101-1POF media converters

- Scalance X101-1: one 100 Mb/s multimode interface with BFOC connection system. The BFOC sockets are used for direct connection to the Industrial Ethernet glass FOCs at distances up to 3,000þm for designing line, star or ring topologies.
- Scalance X101-1LD: one 100 Mb/s single mode interface with BFOC connection system, suitable for cable lengths up to 26,000þm.
- Scalance X101-1POF: one 100 Mb/s plastic optical fiber (POF) interface with SC-RJ connection system, suitable for cable lengths up to 50þm.
- Scalance X101-1FL: one 10 Mb/s multimode interface with BFOC connection system, suitable for cable lengths up to 3,000þm.
- Scalance X101-1AUI: one 10 Mb/s AUI interface with SUB-D connection system, suitable for cable lengths up to 50þm.

The Scalance X100 media converters (Fig. 7.53) possess:

- 4-pin terminal block for connection of the redundant power supply (2×4 V DC)
- LED row for display of status information (power, link status, data traffic, signaling contact)
- 2-pin terminal block for connection of the floating signaling contact
- SET key for on-site configuration of the signaling contact and of the cascading mode.

7.7.6 Routers

Large networks consist of many smaller subnets which are connected together. The various networks are connected together using special devices, so-called routers. These routers are responsible for passing on data between computers in different networks on the most favorable paths. Criteria for the optimum path could, for example, be the length or the shortest transmission delay.

Before the router passes on a packet to a connected LAN or WAN, it examines the address data of the data packet, e.g. the IP address, and passes on the data according to its internal routing table. A table with all accessible stations could hardly be implemented. The routing table therefore does not contain the complete path to a computer with a specific IP address, but only the next intermediate station on the path to the destination. The data packets then proceed from router to router up to the destination.

The real strength of routers is their capability to select the route from the table which is usually best for a data package by application of algorithms (e.g. the load balancing algorithm). Further features of routers are their network management and filter functions. Using appropriately selected routers settings, it is possible to improve the network performance according to the requirements. However, routers provide a generally higher isolation since, for example, they do not usually pass on broadcasts. In addition, routers can additionally function as firewalls in that, for example, they prevent access of certain IP addresses to defined sections of the network.

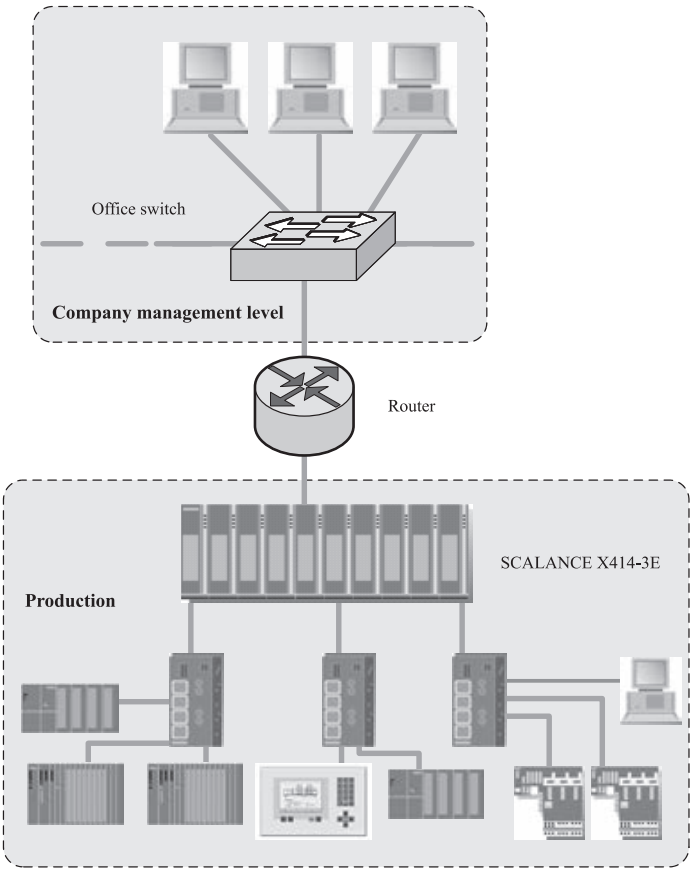


Fig. 7.54 Isolation of office and production communication

A router operates similar to a switch. It is additionally possible to define for a router which communication stations may communicate via the router and which may not. Communication stations on different sides of a router can only communicate with one another if the communication between these stations has been specifically enabled by the router. The high communication load on the office Ethernet could restrict the communication on the Industrial Ethernet. The router prevents this, and limits the network load. For example, if you wish to directly access the production data from SAP, connect your Industrial Ethernet in the production plant with the Ethernet in your office sector using a router. A router therefore limits a subnet (Fig. 7.54).

Please note: real-time communication with Profinet is not possible beyond the limits of a network. It only functions within a network. Therefore routers cannot be used for real-time communication with Profinet. In Profinet networks, routers can only be used for WAN interfacing.

7.8 Topologies for Profinet Networks

A network topology is understood to be the spatial structure of the transmission media. The topology of a network has effects on its capabilities. All network drafts are based on three basic topologies: linear, star and ring. In practice, a system usually consists of a mixture of these topologies.

Network topologies must be oriented according to the requirements of the equipment to be networked. In the office sector, the star and tree topologies defined in IEC 11801 have been proven and are largely accepted. The conditions for networking in an automation environment are greatly different from those in the office sector. This particularly applies to:

- Number of data terminals in the network
- Data terminal density, or distribution of data terminals
- Distances between the data terminals
- Arrangement of the data terminals (e.g. linear arrangement in a transfer line in contrast to a cluster arrangement in an office)
- Availability demands.

Ethernet-based networking in the automation sector necessitates correspondingly optimized network infrastructures which consider the above-mentioned conditions. The chapter on network topologies describes structures for communication cabling which are commonly encountered in industry. To clarify their structural principle, the star, linear, tree and ring structures are explained in their pure form. All topologies presented can be implemented with both symmetrical copper cables and fiber-optic cables. The topology selected depends on the type (cable types, station arrangement) and capability of the equipment, the growth of the network, and the type of network management (network operating system).

It is recommendable to keep switch ports vacant on all signal distributors for subsequent expansion of the plant or for temporary connection of servicing equipment for diagnostics on site.

A summary of various possibilities for designing a Profinet network is provided below.

7.8.1 Star

The star topology is a star-shaped arrangement with individual connections (TP or FOC) from the stations to a central distributor (switch). Data are always exchanged via a detour through the central switch (Fig. 7.55).

A star-shaped network topology automatically results by connecting the stations to a switch. If a single Profinet device fails, this structure does not automatically result in failure of the complete network, in contrast to other structures. Only the failure of a switch results in failure of part of the communication network. The cascading depth and the total expansion of the network are only limited by the signal propagation times of the communication links.

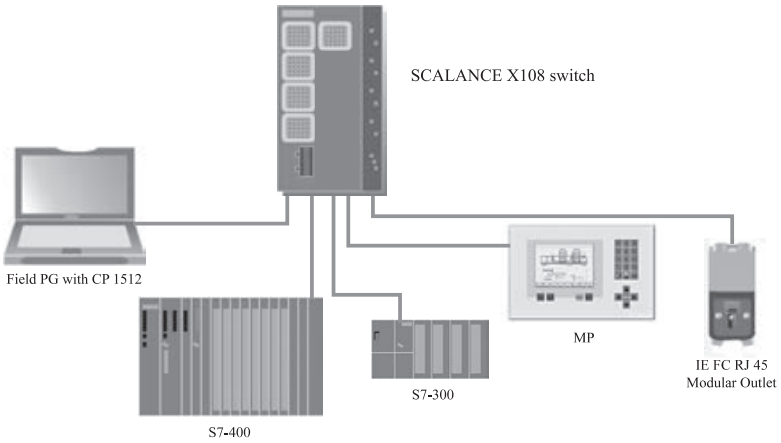


Fig. 7.55 Scalance star topology (electrical)

Examples of applications for star topologies include areas with a high device density and small spatial expansions:

- Small production cells
- Individual production machines
- Control room area of a large plant.

User benefits of the star topology:

- Favorable network component costs per port (network connection) through high port density
- Flexible addition/removal of stations
- Simple administration, monitoring and diagnostics of the network
- Active network components are combined in one location; thus simpler to protect against environmental conditions such as temperature, contamination etc.

The following aspects must be considered:

- High cabling costs and complexity with widely distributed plants
- Reduced availability as a result of central nodes.

7.8.2 Tree

The tree topology results from the connection of several stars into a network, possibly with mixing of fiber-optic and symmetrical copper cables (Fig. 7.56). Plant sections with related functions are combined into star points. These are networked together using adjacent switches. A switch handles the signal distribution function in the start point. Since the switch passes on messages on an address-oriented basis, only messages reach adjacent distributors which are required outside the star point. The higher-level structure is not loaded by pure local data transfer.

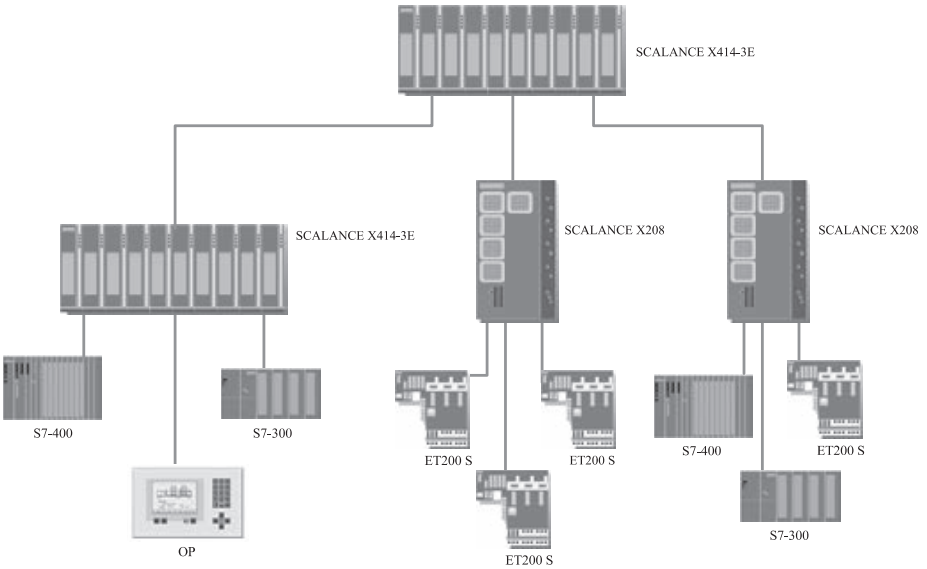


Fig. 7.56 Scalance star topologies as tree (electrical)

The tree topology is used to divide complex plants into autonomous plant sections.

The tree topology offers the following benefits:

- High clarity through division and adaptation of the communications structure according to plant structure
- High transmission capacity of the complete network since local data traffic is limited to the star
- High data security since local data traffic is limited to the star
- Increased availability of independent plant sections
- The transmission medium for interconnection of the stars can be changed if necessary, e.g. to achieve greater path lengths.

If several star topologies are connected together, the result is a tree topology.

7.8.3 Line

Very many applications in the cell and field areas are currently implemented with Profibus in a linear topology. This plant-based networking topology is also available with Profinet. All communication stations are connected in series. The linear topology with Profinet is implemented using switches which are already installed in Profinet devices (Fig. 7.57). Therefore the linear topology with Profinet is merely a special form of the tree/star topology. The cabling requirements are lowest of all with a linear topology. The cascading depth and the total expansion of the network are only limited by the signal propagation times of the connections.

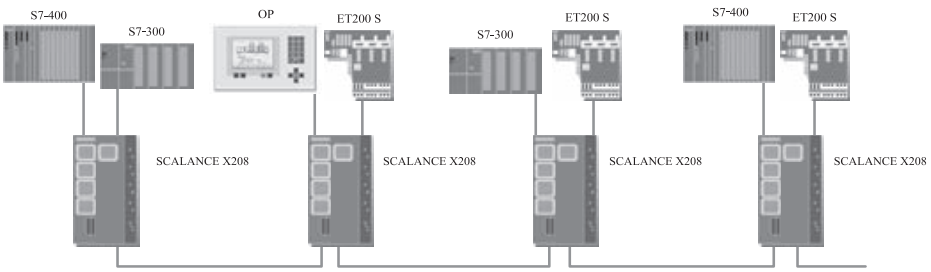


Fig. 7.57
Scalance line topology with Simatic S7-300/400 and operator panel as data terminals

The linear topology is preferably used:

- In plants with an extensive structure, e.g. conveyor systems, assembly lines or
- for connecting production cells.

The linear topology provides the following user benefits:

- Cost-optimized cabling is possible for extensive plants
- The structure corresponds to the well-known fieldbus structure
- Active network components and automation electronics are present in the same control cabinet; this simplifies the power supply and protection against environmental influences
- Cabling is usually close to the machine and time/cost-effective
- Device replacement for servicing or repair is very simple.

The following aspects must be considered:

- Only network components with throughput times as low as possible should be used. The delay time of a message accumulates when passing through each switch in a line
- An interruption in the line results in division into two functioning segments
- Linear topologies can be produced very easily with switches which are integrated in a field device (e.g. CP 443-1 Advanced with 4-way switch).

7.8.4 Ring

If increased availability is required, it is recommendable to use a ring topology. With this structure, all stations are connected together by a ring cable, so that each station has access to its predecessor and successor. The information to be transmitted is passed on from node to node in a fixed direction, during which the signals are tested and amplified before being passed on. The ring structure is generated by an additional connection between the ends of a line (Fig. 7.58). A special mechanism must of course make sure in at least one network component in the ring that the ring logically remains a line.

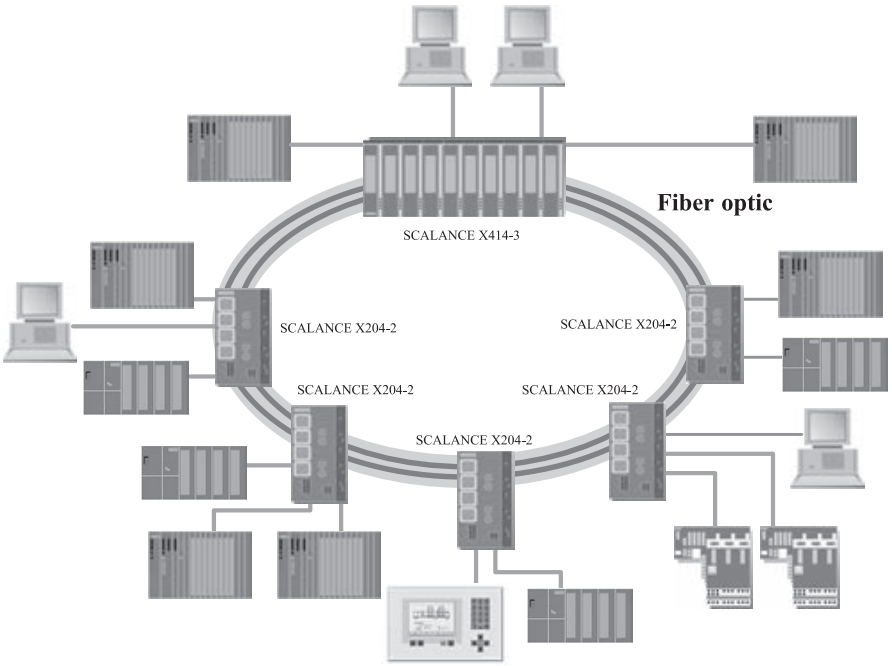


Fig. 7.58 Scalance ring structure with FO cable and redundancy manager

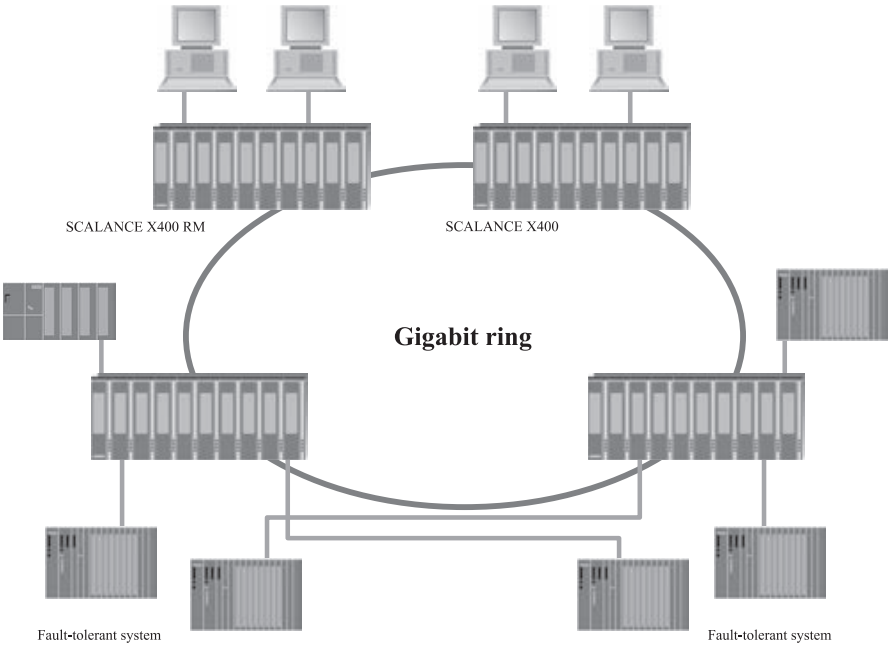


Fig. 7.59 Scalance Gigabit ring with redundancy manager (RM)

This mechanism is controlled by a redundancy manager (Fig. 7.59). The defined point of interruption may only be closed if the ring is interrupted at another point, e.g. by an open-circuit. With a line interruption, the redundancy manager requires up to 300 ms in order to configure the network such that the data can be diverted. The IO controller cannot access the IO Devices in the associated network during this period. Ring topologies are used in plants with increased availability demands.

The user benefits of a ring topology are:

- Increase in plant availability through protection against open-circuits or failure of a network component.

The following aspects must be considered:

- It is necessary to route the return path for closing the ring on a separate return route
- The network components must be provided with a special mechanism so that the ring logically remains a line.

7.9 Installation Guidelines for Optimization of Profinet

The following installation guidelines provide an overview for installation of a Profinet network. More detailed information can be found in the Simatic Net manual “Twisted-pair and fiber-optic networks”. Also refer to the document “Profinet installation guidelines from Profibus International”. Basic information can be found in the manual “Communication with Simatic”.

The vendor-specific installation guidelines of the devices or system manufacturers as well as the applicable safety directives must be considered in addition. The installation guidelines presented here do not claim to be complete.

7.9.1 Electromagnetic Compatibility

The electromagnetic compatibility (EMC) is the ability of electrical equipment to function satisfactorily within its electromagnetic environment without influencing this environment, to which other equipment also belongs, by an unacceptable amount (according to DIN VDE 0870). The mutual influencing can be the result of electric, magnetic or electromagnetic effects. These can be conducted over lines (e.g. common power supply) or also propagated on a line-independent basis through a radiation or emission. To avoid interferences in electrical equipment, these effects must be limited to a certain value. Limiting measures primarily include the electromagnetically compatible arrangement and wiring of all conducting plant components. In addition to the electrical supply network and the signal/data cables, this also includes all conducting structures (pipelines, steel girders etc.). If sufficient attention is already paid to EMC during the planning of automation plants including the associated building, measures appropriate to EMC can be implemented at minimum cost. On the other hand, modifications which become subsequently necessary are usually very costly.

The following points should be observed in the planning phase:

- An equipotential bonding system should be provided at the plant location which includes all inactive metal components of the plant and building, the electrical installation and the shields of the data cables. As a result of the high operating frequencies, it is recommendable to ground the cable screens at both ends. Keep an eye on the resulting shield currents. If these become impermissibly high, equipotential bonding conductors must be routed parallel to the data line, or use of optical transmission over FOCs should be considered.
- As a result of the optical transmission principle, fiber-optic cables are insensitive to electromagnetic influences. The use of FOCs is recommended for bus connections in critical EMC areas as well as between buildings and/or external equipment!
- Plants and buildings should be provided with power from a distribution system with zero current protective earth conductor (e.g. according to the TN-S system).
- The Profinet bus system must only contain components and data cables which support a shielding concept without interruptions.
- Coupled-in noise should be kept to a minimum in the spatial arrangement of devices and cables.
- The installation guidelines of the component manufacturers must be observed. All limits specified by the manufacturers for electromagnetic radiation or emission are only valid if the specified installation rules are observed.
- Extreme sources of interference must be suppressed by special measures.
- In case of doubt, the requirements resulting from electrical safety directives have priority over EMC rules.

7.9.2 Installation Guidelines for Electrical and Optical Data Cables

Remember when routing the data cables that only a limited mechanical load is permissible. In particular, the cables can be damaged or destroyed by excessive tension, pressure, twisting or bending. Cables which have been excessively stressed by one or more of these causes must always be replaced. The following information should help you avoid damage when routing data cables:

- **Route data cables separately:** in conjunction with measures for improving the EMC characteristics, it is recommendable to route the data cables in a separate cable duct. If only one common cable duct is available, the data cables should at least be combined in separate bundles. Separation provides several advantages:
  - Improvement in EMC
  - Improved protection against direct damage, e.g. during subsequent pulling through of hard power cables in the same duct
  - Simpler locating if troubleshooting is necessary.
- **Protect data cables exposed to mechanical danger:** in parts of buildings and machines which are stepped upon and in the vicinity of transport paths and

bushings, it is recommendable to route the data cables in a completely closed aluminium or steel conduit or in a steel cable tunnel.

- **Use separate routes for redundant data cables:** redundant cables should always be routed on separate paths in order to exclude simultaneous damage by the same event.
- **Storage and transport:** during storage, transport and routing, the non-assembled data cable must be kept closed at both ends by a shrink cap to prevent oxidation of the individual conductors and shield as well as accumulation of moisture in the cable.
- **Temperatures:** the minimum and maximum temperatures defined for the cable for transport, handling and operation must not be violated. Otherwise the electrical and mechanical properties of the cables may be negatively influenced. You can find the permissible temperature ranges of the cables in the technical data sheets of the manufacturer.
- **Tensile strengths**: tensile forces acting on the cables must not exceed the maximum permissible tensile strengths neither when handling (e.g. removing from drums) nor in the installed state. You can find the permissible tensile forces on the cables in the technical data sheets of the manufacturer.
- **Provide strain relief:** provide strain relief for all cables subject to strains at approx. 1 m from the connection point. Shield connections are insufficient for strain relief!
- **Pressure loads**: avoid excess stress on the data cables through pressure, e.g. from squeezing through incorrect mounting.
- **Torsion:** torsional forces may result in shifting of the individual cable attachments, and thus to negative influencing of the electrical properties of the cables. Data cables must not be twisted for this reason, unless cables specially designed for twisting are used (e.g. robot applications).
- **Bending radii:** The minimum bending radii of data cables must not be violated at any time. Damage or impermissible impairing of the specified transmission properties may otherwise occur. Note that the permissible bending radii when pulling in under tension are greater than in the stationary installed condition, and that with flat cables the data only apply to bending over the flat side! Bending over the higher side requires significantly greater radii. You can find the permissible bending radii of the cables in the technical data sheets of the cable.
- **Avoid the production of loops:** unroll the data cable tangentially from the drum or use appropriate rotary tables. You then avoid the production of loops with the resulting kinks and twists. The cables must be installed free of torsion.
- **Subsequent installation:** when routing data cables it should also be observed that they are not impermissibly stressed when already positioned. This is possible, for example, if the cables have been routed with other cables on a common cable rack or path (providing the electrical safety permits this) and new cables are subsequently routed (with repairs, expansions).

The following additional information must be observed when routing fiber-optic cables:

- **Danger when using fiber-optic cables:** installation waste must be handled carefully, collected in appropriate containers (not by hand) and disposed of by an approved service facility. Freely-accessible ends of fibers must be kept away from your skin and eyes. If you are unsure that the power output by the optical fiber corresponds to EN 60825, do not look directly into the open ends of fibers. Racks containing connection points for fiber-optic cables must be identified by appropriate warning labels or texts.
- **Protect connectors from contamination:** fiber-optic connectors are sensitive to contamination. Plugs or sockets which have not yet been connected must always be protected by the supplied caps.
- **Change in attenuation under load:** when routing, the fiber-optic cables must not be twisted, stretched or pressed. The specified limits for tension, bending radii and temperature ranges must therefore be observed. The attenuation values may change slightly during the routing, but these deviations are reversible as long as the loading limits have not been exceeded.
- **Provide strain relief**: even if the connectors of the fiber-optic conductors have strain relief and kink protection, it is recommendable to secure the cable against mechanical stress using additional strain relief as close as possible to the connected device.
- **Plan attenuation reserves**: when routing the cables over greater lengths, it is recommendable to plan one or more repair splice connections in the attenuation balance.
- **EMC stability:** fiber-optic cables are insensitive to electromagnetic influences. The cables can therefore be routed together with other cables (e.g. 230 V/400 V power supply cables) in the same cable duct without problem. However, when routing in cable ducts it should be ensured that the permissible loads on the fiber-optic cables are not exceeded when pulling other cables through.
- **Fiber-optic plug connectors:** plug connectors for glass FOCs should only be assembled by trained personnel using special tools. Correct assembly results in a very small insertion loss and high repeatability of the value even after plugging/removing several times.

7.10 Configuration of Scalance X Devices

Certain rules and restrictions apply to the configuration of Profinet networks using Scalance X in order to guarantee trouble-free and secure operation of an automation network.

7.10.1 Scalance X005

The Scalance X005 can be used in small electrical star (Fig. 7.54) and line (Fig. 7.57) topologies. Configuration and expansion of networks are simple to carry out, and there are no limitations to the cascading of the Scalance X005.

The following conditions must be observed when configuring the network:

- Length of TP cable between two Scalance X switches:
  - TP cords or TP-XP Cords with a maximum length of 10þm can be connected to the TP port of RJ45 design.
  - Depending on the type of cable, a total cable length of up to 100þm between two devices is permissible with the IE FC Cables and IE FC RJ45 Plug 180.
    - Cable length 0-100þm: Industrial Ethernet FC TP Standard Cable with IE FC RJ45 Plug 180 or via Industrial Ethernet FC outlet RJ45 with 0-90 m Industrial Ethernet FC TP Standard Cable + 10þm TP Cord
    - Cable length 0-85þm: Industrial Ethernet FC TP Marine/Trailing Cable with IE FC RJ45 Plug 180 or 0-75þm Industrial Ethernet FC TP Marine/Trailing Cable + 10þm TP Cord.

7.10.2 Scalance X100

The Scalance X100 permits electrical and optical mixing in star and line topologies (Figs. 7.55 and 7.57).

The following conditions must be observed when configuring the network:

- Length of the TP cable between two Scalance X switches:
  - TP Cords or TP-XP Cords with a maximum length of 10þm can be connected to the TP port of RJ45 design.
  - Depending on the type of cable, a total cable length of up to 100 m between two devices is permissible with the IE FC Cables and the IE FC RJ45 Plug 180.
    - Cable length 0-100þm: IE FC TP standard Cable with IE FC RJ45 Plug 180 or IE FC Outlet RJ45 with IE FC TP Standard Cable (0-90þm) + 10þm TP Cord.
    - Cable length 0-85þþm: IE FC TP Marine/Trailing/Flexible Cable with IE FC RJ45 Plug 180 or IE FC TP Marine/Trailing/FlexibleCable (0-75þm) + 10þm TP Cord.
- Length of fiber-optic cables:
  - With Scalance X104-2 and X106-1: cable length 0-3000þm with Industrial Ethernet glass FOC: glass FOC 62.5/125þµm or 50/125þµm glass fiber; ð 1 dB/km at 1300þnm; 600 MHz × km at 1300þnm; 6þdB max. permissible FOC loss per section with 3þdB system reserve.

7.10.3 Scalance X100 Media Converters

Media converters can be used in line, star and ring topologies. They convert the signals from electrical to optical, and vice versa.

The following conditions must be observed when configuring the network:

- Length of TP cable between two Scalance X switches:
  - TP cords or TP-XP cords with a maximum length of 10þm can be connected to the TP port of RJ45 design.
  - Depending on the type of cable, a total cable length of up to 100 m between two devices is permissible with the IE FC Cables and IE FC RJ45 Plug 180.

  - Cable length 0-100þm: IE FC TP Standard Cable with IE FC RJ45 Plug 180 or IE FC Outlet RJ45 with IE FC TP Standard Cable (0-90þm) + 10þm TP Cord.
  - Cable length 0-85þm: IE FC TP Marine/Trailing/Flexible with IE FC RJ45 Plug 180 or IE FC TP Marine/Trailing/Flexible (0-75þm) + 10 m TP Cord via IE FC Outlet RJ45.
- Length of fiber-optic cables:
  - With Scalance X101-1: cable length 0-3000þm with Industrial Ethernet glass FOC: glass FOC 62.5/125þµm or 50/125þµm glass fiber; ð 1þdB/km at 1300þnm; 1200 MHz x km at 1300þnm; 6þdB max. permissible FOC loss per section with 3þdB system reserve.
  - With Scalance X101-1LD: cable length 0-26000þm with Industrial Ethernet glass FOC 10/125þµm singlemode fiber; ð 0.5þdB/km at 1300þnm; 13þdB max. permissible FOC loss per section with 2þdB system reserve.
  - With Scalance X101-1POF: cable length 0-60þm plastic FOC 980/1000þµm POF; ð 230þdB/km at 660þnm; 11.5þdB max. permissible FOC loss per section with 3þdB system reserve.
  - Bending radius, once without tension: 100þmm; bending radius, repeated, with tension: 150þmm.
- Cascading (series connection) of two media converters: if you connect two media converters in series, i.e. via the FO port, it is essential to first switch on this mode using the key on the device. Hold the key pressed for 1-2 seconds. When released, activation of this mode is indicated by lighting up of the LED “TL” (Transparent Link). You can leave this mode by pressing the key again for 1-2 seconds, the LED “TL” goes off.
- Important notes:
  - A maximum of two media converters can be connected in series.
  - Mixed cascading with Scalance X100 and OMC media converters is not possible.
  - The series connection is only permissible via connection of the FO ports.

7.10.4 Scalance X200

The Industrial Ethernet Scalance X200 switches with IP30 protection are usually accommodated together with the connected stations in a control cabinet. Electrical and optical mixing is permissible in star, line and ring line topologies. The Scalance X208 PRO is designed for mounting outside cabinets.

The following conditions must be observed when configuring the network:

- Length of TP cable between two Scalance X switches:
  - TP Cords or TP-XP Cords with a maximum length of 10þm can be connected to the TP port of RJ45 design.
  - Depending on the type of cable, a total cable length of up to 100 m between two devices is permissible with the IE FC Cables and IE FC RJ45 Plug 180.
    - Cable length 0-100þm: IE FC TP Standard Cable with IE FC RJ45 Plug 180 or IE FC Outlet RJ45 with IE FC TP Standard Cable (0-90þm) + 10þm TP Cord.

  - Cable length 0-85þm: IE FC TP Marine/Trailing/Flexible with IE FC RJ45 Plug 180 or IE FC TP Marine/Trailing/Flexible (0-75þm) + 10þm TP Cord.
- Scalance X208 PRO:
  - Cable length 0-100þm: IE FC TP Standard Cable with IE M12 Plug PRO.
  - Cable length 0-85þm: TP-cable length 0-8þm IE FC TP Marine/Trailing/Flexible Cable with IE M12 Plug PRO.

- Length of fiber-optic cables:
  - With Scalance X204-2 and X206-1: cable length 0-3000þm with Industrial Ethernet glass FOC: glass FOC 62.5/125þµm or 50/125þµm glass fiber; ð 1þdB/km at 1300þnm; 600 MHz × km at 1300þnm; 6þdB max. permissible FOC loss per section with 3þdB system reserve.
  - With Scalance X204-2LD and X206-1LD: cable length 0-26000þm mit Industrial Ethernet glass FOC 10/125þµm singlemode fiber; ð 0.5 dB/km at 1300þnm; 13þdB max. permissible FOC loss per section with 2þdB system reserve.

7.10.5 Scalance X200 IRT

The Industrial Ethernet Scalance X200 IRT switches are usually accommodated together with the connected stations with real-time capability (see Fig. 7.60) in a control cabinet. The following conditions must be observed when configuring the network:

- Length of the TP cable between two Scalance X switches:
  - TP cords or TP-XP cords with a maximum length of 10þm can be connected to the TP port of RJ45 design.

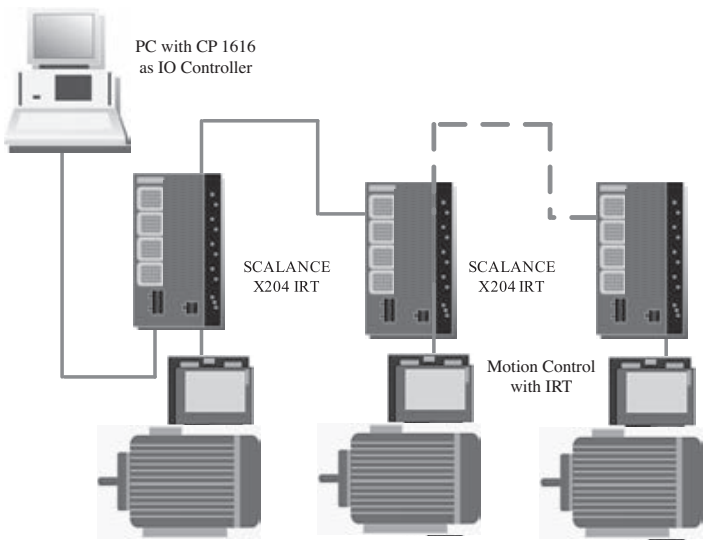


Fig. 7.60
Example configuration with Scalance X204 IRT for Profinet with real-time capability

  - Depending on the type of cable, a total cable length of up to 100 m between two devices is permissible with the IE FC Cables and IE FC RJ45 Plug 180.
    - Cable length 0-100 m: IE FC TP Standard Cable with IE FC RJ45 Plug 180 or IE FC Outlet RJ45 with IE FC TP Standard Cable (0-90 m) + 10 m TP Cord
    - Cable length 0-85 m: IE FC TP Marine/Trailing/Flexible with IE FC RJ45 Plug 180 or IE FC TP Marine/Trailing/Flexible (0-75 m) + 10 m TP Cord

- Length of fiber-optic cables:
  - With Scalance X202-2IRT and X206-1: cable length 0-3000þm with Industrial Ethernet glass FOC: glass FOC 62.5/125þµm or 50/125þµm glass fiber; ð 1þdB/km at 1300þnm; 600 MHz × km at 1300þnm; 6þdB max. permissible FOC loss per section with 3þdB system reserve.
  - Max. 100þm with Industrial Ethernet PCF cable
  - Max. 50þm with Industrial Ethernet POF cable

7.10.6 Scalance X400

It is simple to adapt the network topology to the plant structure using Industrial Ethernet Scalance X400 switches. Scalance X400 provides electrical ports which can be used as Gigabit and ring ports. The expansion by media modules provides additional optical ports. By using an extender module, the number of ports can be increased by a maximum of eight.

The following network structures and combinations can then be implemented:

- Fast Ethernet and Gigabit rings with fast media redundancy: for protection against failure of a transmission link or switch, up to 50 X400 switches in a linear cascade can be connected together in a ring with a range of up to 150þkm using multimode or 1300þkm using singlemode. On failure of a transmission link or Scalance X400 switch in the ring, the transmission path is reconfigured within 0.3 seconds.
- Redundant connection of several rings is possible using the standby function (Fig. 7.59). Mixing is possible with other Scalance modules with redundancy function (Fig. 7.58).
- At the same time, Scalance X400 permits redundant connection of the ring structure to the company network using rapid spanning tree.
- Star structure with Scalance X400 switches: each Scalance X400 switch represents a star point which can connect up to 26 stations or subnets together electrically or optically (Fig. 7.56).

The following conditions must be observed when configuring the network:

Data transmission is carried out using multimode or singlemode fiber-optic cables (FOC). The wavelength is 1310þnm. Two types of FOC can be used:

- Multimode FOC: data transmission is carried out using multimode FOCs. The wavelength is 850þnm. The core diameter of the multimode FOC is 50þm, the light source is an LED. Many modes (light rays) are used for the signal transmis-

sion. The differences in the propagation times of the light pulses (dispersion) result in quite a limitation in the maximum range.

- Singlemode FOC: data transmission is carried out using singlemode FOCs. The wavelength is 1310þnm. The core diameter of the singlemode FOC is 9 or 10þm, the light source is a laser diode. Only one mode (light ray) is used for the signal transmission, resulting in a significantly smaller dispersion. Therefore the maximum range with singlemode FOCs is greater than with multimode FOCs.

The outer diameter of the FOC is 125þm independent of the type used. The maximum transmission range (segment length) depends on selection of the module and the corresponding FOC. Ranges:

- For 100Base-FX module and multimode FOC with BFOC sockets: 3þkm
- For 100Base-FX-LD module and singlemode FOC with BFOC sockets: 26þkm
- For 1000Base-SX module and multimode FOC with SC duplex plugs: 750þm.
- For 1000Base-LX module and singlemode FOC with SC duplex sockets: 10þkm.

Maximum cable length with twisted-pair:

- The maximum transmission range (segment length) is 100þm.
- Data transmission is carried out at both 10 Mb/s and 100 Mb/s on two pairs of conductors (pins 1, 2, 3, 6) of the twisted-pair cable. At 10þMb/s, at least one cable of Category 3 is required, at 100þMb/s at least one four-core cable (22).
- For data transmission at 1 Gb/s at least one Category 5e twisted-pair cable with 4×2 cores is required. With a four-core cable (22), a maximum data transfer rate of 100þMb/s is possible.

7.10.7 General Rules for Design of Profinet Networks

Profinet permits high-performance and uniform communication. The performance can be increased even further by observing the following design guidelines.

1. Connect a router or a Scalance S between the office network and the Profinet system. By means of the router you can exactly define who may access your Profinet system.
2. Never use hubs or bridges for Profinet. Only select switches which offer the unlimited Profinet functionality.
3. Only use lines with twisted copper cables (100Base-TX) with a transmission rate of 100 Mb/s (Fast Ethernet). The transmission properties of this cable must comply with the requirements of CAT 5 according to ISO/IEC 11801 at 100 Mb/s.
4. Where it appears meaningful, provide your Profinet system with a star topology (e.g. in the control cabinet).
5. Only use a small concatenation depth for the switches. This additionally increases the clarity of your Profinet system.

6. Connect your programming device (PG) in the vicinity of the communications partner (e.g. PG and communications partner on same switch).
7. Only use products as plant components which have been certified by the PNO. The certificate provided by the PNO confirms that the response within a plant conforms to the standard. This certificate also confirms observation of the EMC guidelines.
8. Be extremely careful during configuration, planning and commissioning! Optimization can be carried out at an early point in time, reducing or eliminating possible sources of error.
9. Train your personnel and provide ongoing training: planning, commissioning and servicing engineers should always be aware of the latest developments and technologies associated with Profinet.
10. Always observe the vendor-specific operating instructions and installation guidelines for the devices. The applicable safety directives must also be considered in addition.

7.10.8 Summary of Fundamental Standards and Directives Applicable to Profinet Networking

The Profinet transmission system is based on the following international standards:

- ISO/IEC 8802-3:2000: Information technology – Telecommunications and Information Exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
- ISO/IEC 9314-3:1990: Information processing systems – Fiber Distributed Data Interface (FDDI) – Part 3: Physical Layer Medium Dependent (PMD).
- ISO/IEC 9314-4:1999: Information technology – Fiber distributed data interface (FDDI) – Part 4: Single-mode fibre physical layer medium dependent (SMF-PMD).

The Profinet cabling structure is based on the following standards: ISO/IEC 11801: Edition 2.0, Information technology – Cabling systems for customer premises.

The components of the symmetrical copper cabling are based on:

- IEC 61156-2 Edition 2.0: Multicore and symmetrical pair/quad cables for digital communications – Part 2: Horizontal floor wiring – Sectional specification.
- IEC 61156-3 Edition 2.0: Multicore and symmetrical pair/quad cables for digital communications – Part 3: Work area wiring; Sectional specification.

The components of the fiber-optic cabling are based on:

- IEC 60793 series: Optical fibres
- IEC 60794 series: Optical fibre cables

- IEC 60874-14:1993, Connectors for optical fibres and cables – Part 14: Sectional specification for fibre optic connector – Type SC
- IEC 60874-10:1992: Connectors for optical fibres and cables – Part 10: Sectional specification for fibre optic connector – Type BFOC/2,5

Planning and installation of the Profinet cabling is oriented on the European standards of the EN 50174 series:

- EN 50174–1, Informationstechnik – Installation von Kommunikationsverkabelung Teil 1: Spezifikation und Qualitätssicherung
- EN 50174–2 Informationstechnik – Installation von Kommunikationsverkabelung Teil 2: Installationsplanung und Installationspraktiken in Gebäuden
- EN 50174–3 Informationstechnik – Installation von Kommunikationsverkabelung Teil 3: Installationsplanung und – praktiken im Freien

When integrating the shielded, symmetrical copper cables into the Profinet cabling in a total concept for grounding and equipotential bonding in buildings, the following standard must be applied:

- EN 50310, Anwendung von Maßnahmen für Erdung und Potenzialausgleich in Gebäuden mit Einrichtungen der Informationstechnik

Where applicable, international standards concerning electromagnetic radiation and shielding as well as local regulations should also be considered, e.g.:

- IEC 61000-6-2:1999, Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen – Störfestigkeit für Industriebereich
- IEC 61000-6-4:1997: Elektromagnetische Verträglichkeit (EMV) – Teil 6-4: Fachgrundnormen – Störaussendung für Industriebereich
- IEC 61131-2: Speicherprogrammierbare Steuerungen – Teil 2: Betriebsmittelanforderungen und Prüfungen

8 Profinet Security

Modern automation technology is based on communication and the increasing networking of individual production islands. Industrial applications are currently handled using standard fieldbus systems which are designed in line with the special requirements. However, the tendency is toward even higher integration of all production components with uniform networking to the office network or company intranet. Remote access facilities for servicing purposes, increasing application of IT mechanisms such as Web servers and e-mail for PLCs, as well as the use of wireless LAN are further trends being incorporated into the world of industrial communication at unbelievable speed. Lower prices, higher performance and components "hardened" in line with industrial requirements are increasingly turning the Ethernet into a universal, open fieldbus for the industrial sector.

Industrial communication is becoming part of the IT world, and is suddenly exposed to the same dangers known from the office and IT environments such as hackers or malicious software which destroy or spy on data or prevent communication through the generation of extreme network loads. In addition, new potential dangers result from the application of open standards which are easier to attack since the protocols are open and weak points are easier to find.

Uniform networking provides many advantages permitting, for example, data and devices to be accessed from a workstation or central control room. However, this also increases the possibility of mistakes since the devices are almost exclusively identified only by their IP addresses without any visual contact being made with them. Even a careless typing error could therefore result in unacceptable problems if no appropriate security measures are present.

The possible effects of security weak points are assessed as being far more serious for automation networks than for office networks since even brief network faults can result in production failures or could produce extreme damage. Therefore appropriate security measures are essential. However, existing security concepts are tailored to the office sector, and do not satisfy the special requirements of automation systems, or there are acceptance problems, because:

- Continuous updating and special expert knowledge is required.
- Integrating into existing networks is not without feedback, i.e. network topologies must be changed and stations reconfigured.
- The special protocol structure of automation systems is not considered, in particular the layer 2 protocols.

Security refers to a state in which the risks existing when using information technology can be limited to an acceptable level using appropriate measures. IT secu-

rity is therefore the state in which the confidentiality, availability and integrity of information and information technology are protected by appropriate measures. The three fundamental values of IT security are therefore:

- Confidentiality: information must be protected against unauthorized access by third parties.
- Availability: access to information and to the system must be guaranteed at all times.
- Integrity: it must be possible to recognize non-authorized modification or manipulation of information content with a defined degree of reliability.

Each user can of course also consider further fundamental values when defining the protection requirements should these be helpful in the particular application. Examples of further generic terms for IT security include:

- Authenticity
- Liability
- Reliability

A security concept is therefore required which can reliably protect industrial communication on the one hand, but also considers the special requirements of automation systems on the other.

8.1 Scalance S

Siemens has therefore developed a security concept which applies security modules to satisfy these requirements and which simultaneously takes into account the increasing network security requirements. Security modules from the Scalance S range have been especially designed for use in automation systems, but are nevertheless linked seamlessly to the security structures of the office and IT environments. They provide security but also satisfy the special requirements of automation systems such as easy upgrading of existing plants, simple installation, or minimum downtimes in the event of faults. Through combination of different security measures such as firewall and VPN (virtual private network) by means of IPsec tunnel, Scalance S protects individual devices or even complete automation cells against:

- Data espionage
- Data manipulation
- Unauthorized access
- Automated penetration attempts.

Scalance S achieves this protection flexibly, without feedback, independent of the protocol (layer 2 and above according to IEEE 802.3) and without complicated handling. It is then possible to secure all existing networks without having to recon-

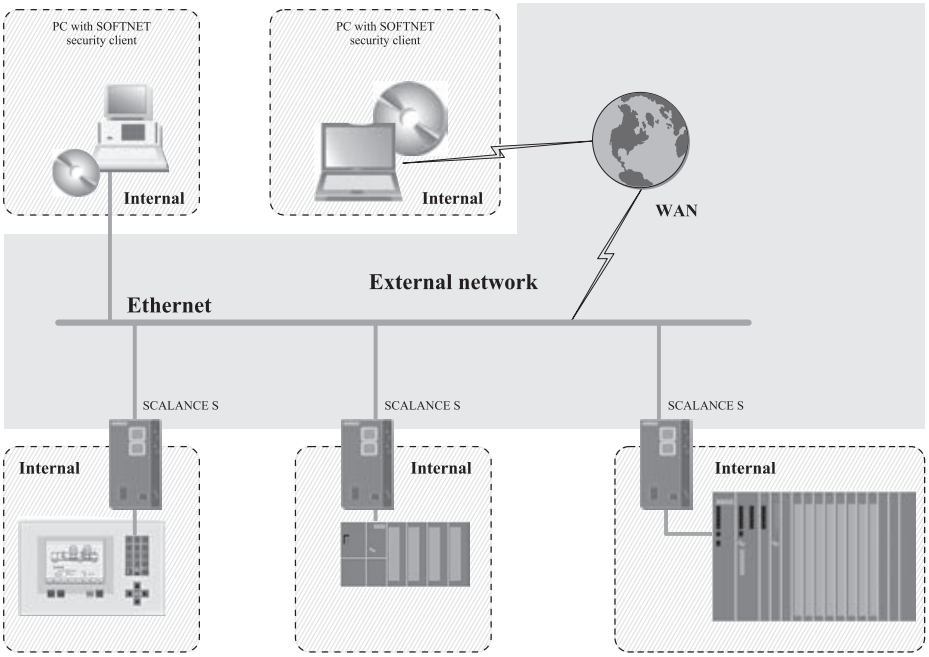


Fig. 8.1 Scalance S divides networks into internal and external areas

figure existing stations or change the network topology. Scalance S divides networks into two areas (Fig. 8.1):

- Protected areas with “internal nodes”: internal nodes are all those which are protected by a Scalance S.
- Unprotected areas with “external nodes”: external nodes are all those which are located outside the protected area.

The internal networks are considered as being secure (trustworthy). Internal areas can communicate with other, trustworthy internal areas. You must only connect an internal network segment to the external network segments using Scalance S. Other non-secure paths between the internal and external networks must not be present!

Scalance S security modules are available as network components with a rugged, industry-compatible design and also as software. The modules can simply be connected in series since they do not require different IP networks like routers but work as transparent proxies. This concept offers the following advantages:

- Nodes without their own security functionality can be protected. This is of increasing importance since many automation devices are not equipped with this – or cannot be retrofitted – for technical or economical reasons. The existing infrastructure can therefore be protected without changes.

- Protection against maloperation, data espionage, data manipulation, overloading of communications system, mutual influencing, unauthorized access, automated penetration attempts and faulty addressing in the monitored network.
- User-friendly and simple configuration and administration using IT security without special knowledge. Scalance S is configured using the security configuration tool. This permits simple handling with minimum configuration without special knowledge of IT security. It is only necessary to create and configure the security modules which are to communicate securely with one another.

No changes or adaptations are required in the existing network structure, applications or nodes – the system is therefore flexible, without feedback and independent of the protocol.

Special consideration was applied to configuration of the modules. Associated office security solutions are mainly expert systems. In automation systems, however, it cannot always be assumed that a high degree of security know-how is present and available 24 hours a day. Therefore particular attention was applied during the development of the configuration tools of the security modules that no special knowledge of the security mechanisms is required for commissioning and servicing.

During configuration, the security modules present in a network are assigned to certain groups. Only security modules in the same group or in the devices protected by them can communicate with one another. Security modules can of course also be assigned to several groups. Corresponding configuration files are then generated which are uploaded by the configuration engineer to the security modules via a secure channel. In addition to this minimum configuration, there are also enhanced adjustment facilities which can be applied as necessary, e.g. the firewall configuration. It is then possible to differentiate the access privileges and possibilities even further in that certain services can be specifically disabled or enabled. It would be possible here to enable users to access Web servers with HTTP but not to transfer or even delete files by FTP. It is additionally possible with the firewall to check the data transfer from the internal to external network, and to limit it as required.

In addition, the security modules support a learning process. They then automatically recognize every station on the internal network, making it unnecessary to configure the stations. In addition, security modules also recognize other security modules in the network, i.e. it is not necessary to reconfigure the existing security modules when the system is expanded.

Various security functions can be combined together depending on the respective security requirements in order to protect individual devices or also complete automation cells:

- Firewall: IP firewall with stateful packet inspection as well as firewall also for Ethernet “Non-IP” frames according to IEEE 802.3 (layer 2 frames). All network nodes located in the internal network segment of a Scalance S are protected by this firewall.

- Secure communication through IPsec tunnel (VPN, virtual private network): Scalance S modules can be combined into groups through configuration. IPsec tunnels are established between all Scalance S modules of a group. All internal nodes of these Scalance S modules can communicate securely with one another by means of this tunnel. Tunneling also comprises Ethernet frames according to IEEE 802.3 (layer 2 frames). Both IP frames and non-IP frames can then be transmitted. Protection of communication is independent of the protocol (Profinet, Ethernet/IP, MODBUS TCP etc.).
- Protection for devices and network segments: firewall and VPN can cover the operation of individual devices, several devices or also complete network segments.

The application of standard security mechanisms is always associated with a certain loss of performance since frames have to be checked using filter tables or encrypted/decrypted. This is not compatible with certain real-time applications. However, it is possible by segmenting into secure and non-secure areas to keep real-time applications in the internal network independent of a security module, since security of the internal data traffic is not influenced. Even if the external network should crash, the data traffic in the internal network, e.g. an automation cell, is not affected.

Several versions of security software are available supplementary to the security modules. One version is a software client module which permits stationary or mobile PCs or programming devices to access devices protected by security modules. This software can be considered as a key to a lock. Another version protects industrial PCs or servers, and contains the same security functionality as the security modules. Automation computers which generate a transition between different networks can then separate the two networks with respect to security functions.

8.2 Protection Functions of the Security Modules

The protection functions of the security modules are mainly based on two mechanisms: establishment of virtual private networks (VPN) and a packet filter firewall as well as the IPSec protocol (IP security) and Network Address Translation (NAT). The two mechanisms will be briefly described here to enable better understanding.

8.2.1 The Firewall Functionality

The task of the Scalance S firewall functionality is to protect the internal network against influences or interferences from the external network. This means that only specific, previously-defined communications relations are permissible between nodes from the internal network and nodes from the external network. A firewall is a system which protects individual stations or complete computer networks against attacks from a coupled network. It limits access between the network to be protected and the coupled network.

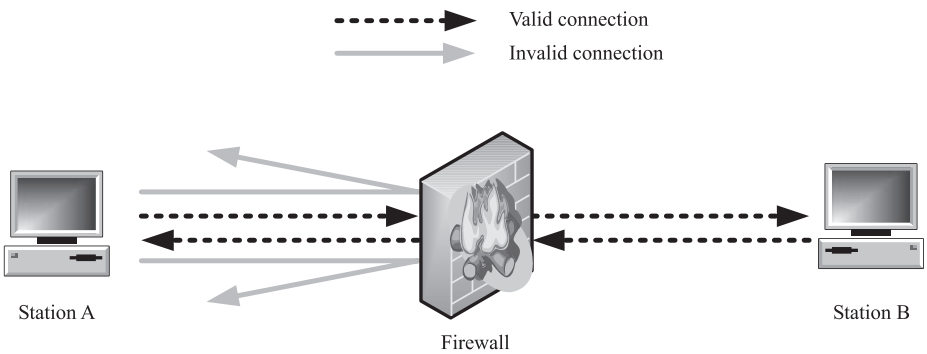


Fig. 8.2 Invalid data streams are blocked by the firewall, valid data streams approved by the firewall rules are permitted to pass

In order to clarify this functionality, one can imagine a firewall as being a moat around a castle (in this case: network or station, PLC). In order to reach the castle, it is necessary to either get over the moat and the walls or to access the fortress over the drawbridge. A firewall has several functions:

- Persons only have access to the "castle" via a strictly controlled point (drawbridge with one or two checkpoints outside in front of the moat and inside at the gate to the castle).
- Attackers are prevented from coming too close to a safeguard (in this case: the castle wall).
- It is also ensured that the castle can only be left through one exit.

Firewalls or packet filters are able to block undesired communication in that IP packets are filtered according to rules defined by the user. Both incoming and outgoing communication can be blocked (Fig. 8.2). A firewall can be used for encrypted (IPsec tunnel) and non-encrypted data traffic.

8.2.2 Packet Filters

Packet filter firewalls are a historical extension of network routers. Each router usually has two or more interfaces to connected networks, and produces tables on which networks are connected to which interfaces or are accessible via it (routing tables). It is quite simple to extend sets of rules in a similar manner which define whether the existing routes can be used by different IP packets or not. The filter criteria can be IP addresses (source and destination addresses), port numbers or certain protocols which can be either stopped or enabled. To achieve this, a firewall compares for example, the IP address of the computer from which a received data packet originates with a list of permissible senders – and only their data are permitted to pass through.

Routers make their decisions exclusively at the connection layer of the OSI protocol (layer 3). It is only necessary to analyze the IP header of the packets for this

purpose, meaning that routers with even a minimum hardware configuration can achieve sufficiently high data throughputs. In a comparable manner, the filter mechanisms of a classic packet filter are kept simple to again guarantee appropriate data throughputs. These packet filters therefore only consider information present in the headers of the data packets, and do not consider the data contents of the IP packets in higher protocol layers. A well-equipped packet filter in the TCP/IP environment therefore makes its decisions on the basis of the following parameters:

- IP addresses of sender and receiver
- IP protocol used
- TCP or UDP ports if the IP packet transports one of these protocols
- IP and TCP flags, ICMP types
- Network interfaces via which the IP packet reaches the packet filter or leaves it again.

Not all packet filters implement these parameters. The administrator defines a set of filter rules which remain unchanged during operation. Each rule defines for a combination of the above-listed parameters whether an IP packet is to be routed on or not. When processing a specific IP packet, a comparison is made with the existing filter rules to establish whether a rule matches the packet parameters (Fig. 8.3). If this is the case, the action (pass on or block) defined in the rule is carried out. If no filter rules match the packet, a default setting is applied (which, in the interest of security, should result in blocking of the packet).

A classic packet filter processes each IP packet individually, and the decision concerning passing on or blocking is independent of which IP packets have already been processed. Many packet filters are implemented based on routers. An alternative is the so-called “bridging firewalls” where the filter rules control the data

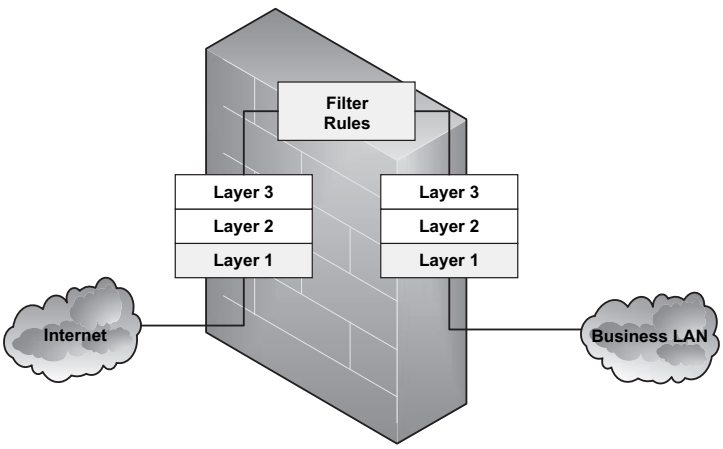


Fig. 8.3 Filter rules in the OSI protocol stack

traffic via a network bridge, i.e. at OSI layer 2. From the security aspect, they largely correspond to the packet filters at the routing layer. A slight advantage is that they are configured without an own IP address and are therefore invisible at the IP layer. From the network aspect, they are advantageous if the network segments connected are not to form independent subnets in each case or if integration without feedback is necessary.

8.2.3 Stateful Packet Inspection

The filter properties of a packet filter can be significantly improved if the IP packets are checked in their context. It is desirable, for example, to only pass on a UDP datagram coming from an external computer to the inside if a different UDP datagram was sent from the inside to the same computer shortly before (e.g. with a DNS inquiry of a client in the internal network to an external DNS server). In order to enable this, the packet filter must manage a status for all current connections. Packet filters which can do this are therefore referred to as stateful. In the case of TCP connections, they imitate the status monitoring of a complete TCP/IP protocol stack, and simulate virtual connections in the case of UDP.

Another important property of a Stateful Packet Inspection is the capability to dynamically generate and delete filter rules. In the above case, for example, a rule must be activated for a limited period following passage of the first UDP data packet from inside to outside which accepts the “response packet” and passes it on to the client. Following expiry of the time window for the response, this rule must be deleted again. Configuration is therefore easier for the firewall administrator since certain rule definitions need no longer be explicitly entered. On the other hand, the response of the firewall is partially no longer under the administrator‘s control. Stateful Packet Inspection thus provides the additional security property that it is not necessary to permanently open a large number of ports for IP packets arriving from outside, but to only open them when required. Permanently open external ports are then only necessary for connections which are initiated from outside.

8.2.4 Application Level Gateways

This type of firewall concentrates its monitoring functions at the application layer. A special test program, also referred to as proxy, exists for each application protocol handled, and completely analyzes the data stream of this application. This type of firewall is therefore also referred to as proxy firewall. A proxy always checks observation of the application protocol for which it has been written. Further possibilities are provided depending on the protocol and configuration:

- Filtering of protocol elements: not everything defined in the application protocol may be permissible in a specific case. An imaginable example would be filtering of the PUT command in the FTP protocol if the addressed FTP server is not to receive any uploads.
- Search for malware: at the application layer, the data are present in a format which enables checking for viruses, Trojans, worms and other malware using a standard virus scanner.

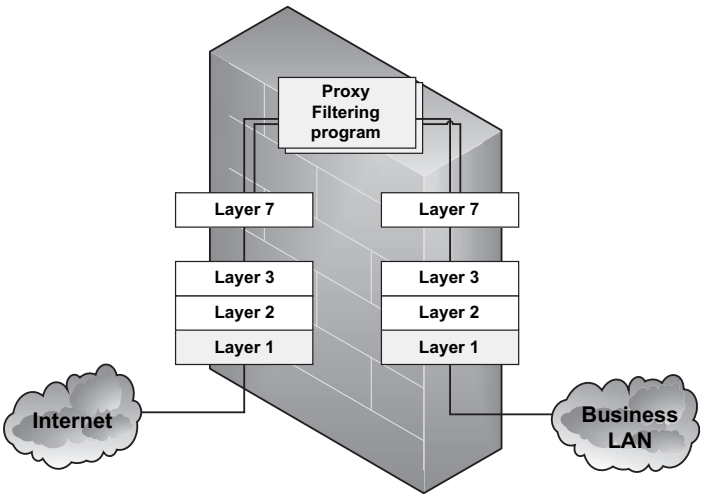


Fig. 8.4 Application Level Gateway in the OSI protocol stack

- User authentication: if the application protocol already provides user authentication, this can already be requested by the proxy before the server is actually addressed. A non-authorized user can then no longer reach the server.

Proxy programs are application-specific. Therefore an Application Level Gateway must always provide a matching proxy for each protocol which is to be routed via the firewall (Fig. 8.4).

8.3 Network Address Translation (NAT, NAPT)

The name NAT firewall is frequently used in association with a normal firewall. However, Network Address Translation (NAT) is neither a special firewall function, nor is it always a true security mechanism. It is rather the case that the procedure has been primarily provided to enable several computers in a local network to have an Internet connection, even though the Internet service provider only assigns them one single IP address or a different address band. NAT then translates the IP addresses of the local computers into an IP address for the public Internet. At the same time, NAT “hides” the private IP addresses of your computers from the public Internet. Since the individual PCs cannot thus be directly accessed from the Internet using the public IP address, a number of router vendors refer to an NAT firewall in their advertisements. However, this is not a firewall function in the true sense which only allows certain data packets to pass.

The NAT service can be executed on a router or other device instead of on a firewall. The procedure with NAT is comparatively simple: in outgoing packets, the (private) source IP address is replaced by an unused (public) IP address. The NAT device records this conversion in a translation table (Fig. 8.5). The function is the same for incoming packets, but is configured separately.

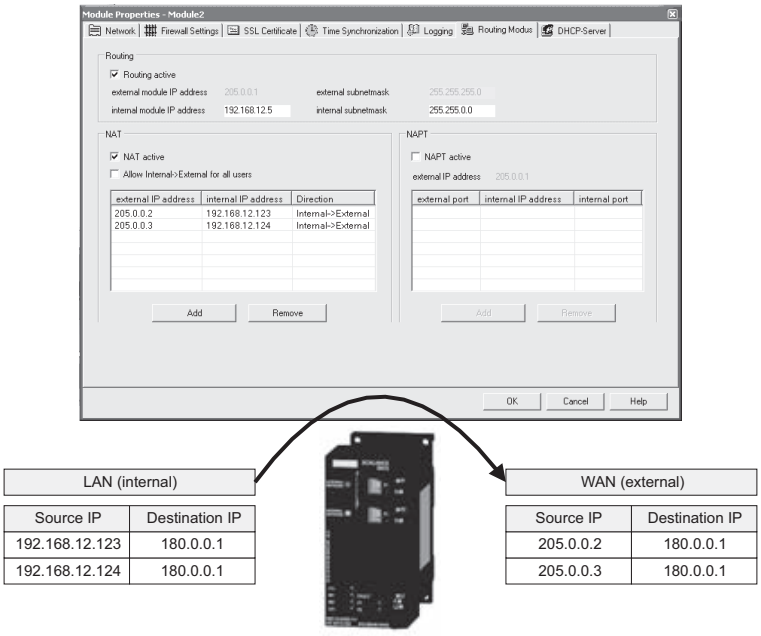


Fig. 8.5 Principle of NAT with outgoing packets using example of Scalance S. The translation table is configured in the Security Configuration Tool.

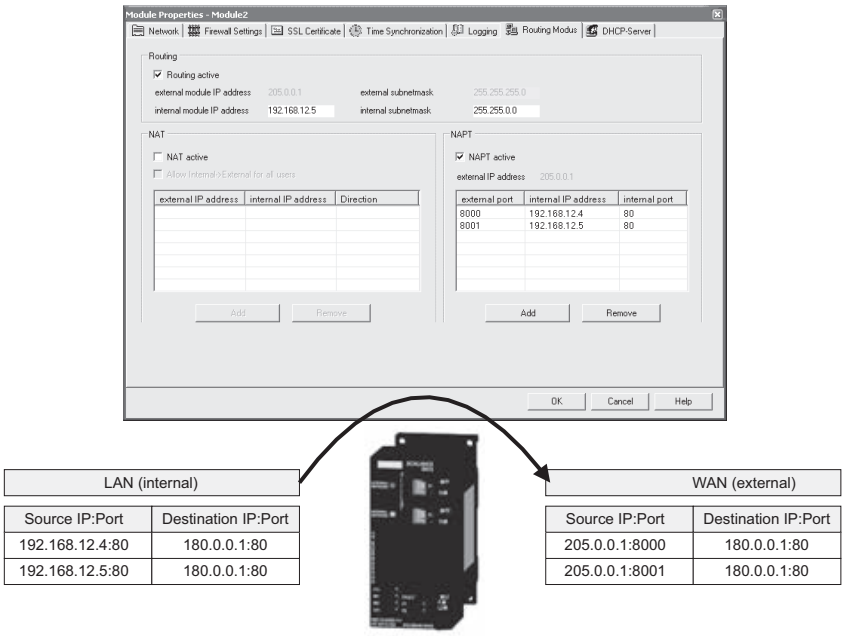


Fig. 8.6 Principle of NAPT with outgoing packets using example of Scalance S. The translation table is configured in the Security Configuration Tool.

Nowadays, the most common form of NAT is the Network Address Port Translation (NAPT) which permits conversion of port numbers in addition to conversion of IP addresses. It is then possible to map several (private) IP addresses and associated port numbers in just one public IP address (Fig. 8.6).

In association with IPSec, it is necessary to use NAT-Transversal. The port number 500 used to negotiate IPSec security associations is defined by the IPSec standard and must not be changed. A change would be interpreted as a modification to the packet, and prevent the establishment of an IPSec connection. In a remote access application, there is therefore no possibility for an NAT device to connect returned data packets to the inquiring stations since these all have the same port number. In particular, it is not possible to permit an IPSec-protected connection for several users simultaneously if address conversion is carried out by an NAT device on the data path.

NAT-Traversal eliminates this limitation in that it packs the IPSec packets in standard UDP packets again. The unique port numbers can then be used for delivery of the packets, without disturbing the IPSec functionality. Several remote workers can thus be provided with secure access to the company network via NAT devices, e.g. in -hotels or hotspots. Capsulation and decapsulation take place at the two ends of the communication path and must be supported by both the IPSec client and the VPN gateway.

8.4 Virtual Private Network (VPN)

If two stations in a network wish to communicate with each another without eavesdropping, a virtual private network (VPN) on the basis of IPSec (Internet protocol security) is recommended. A VPN is understood to be a closed communications structure implemented on a public IP-based network such as the Internet using encrypted data channels. The VPN technology places a virtual network above an existing network as a further layer.

To achieve this, the VPN establishes a virtual tunnel between the stations in which the data are transported. This procedure means that the network protocols used at the individual locations are irrelevant. In order to guarantee data security when

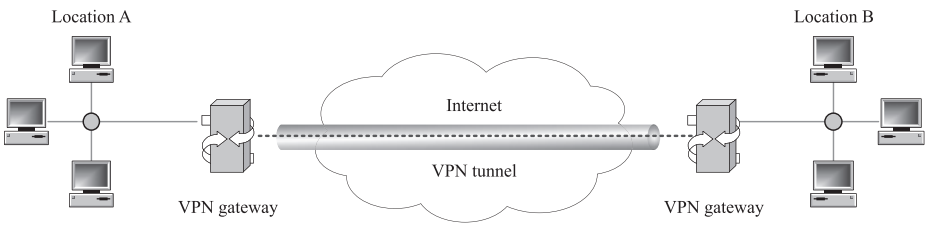


Fig. 8.7
Two locations are securely connected over VPN gateways on a non-secure network – the Internet in this case. Encrypted communication is used between the two locations.

transmitting on the Internet, the data are encrypted before being sent, and decrypted by the receiver. A single station or complete LANs can be connected at the two ends of the tunnel. The end points of the connection are special VPN gateways (Fig. 8.7). These VPN gateways encrypt the data to be transmitted at the protocol layer using so-called tunneling protocols in order to protect the data traffic against espionage and manipulation.

Common VPN protocols are:

- IPSec (IP Security)
- PPTP (Point-to-Point Tunneling Protocol)
- OpenVPN

IPSec is the VPN protocol which is currently most frequently used, and is also used in the Scalance S. For this reason we shall not consider the other standards here any further, but shall consider IPSec in detail.

8.5 IPsec Protocol

The IPSec protocol (IP Security) can be found in almost every firewall product, and has been part of the Microsoft operating system since Windows 2000. Using IPSec it is possible to transport cryptographically protected IP packets over public networks. The basic procedures and protocols are described in several RFCs (RFC 2401-2409).

8.5.1 Security Modes of IPSec

IPSec offers two security modes: Authentication Header (AH) and Encapsulation Security Payload (ESP), each in combination with the tunnel or transport modes. AH can be used to guarantee data integrity and authenticity by generating a cryptographic checksum for each packet sent. This procedure is referred to as hashing, where the Hashed Message Authentification Code (HMAC) with the MD5 or SHA-1

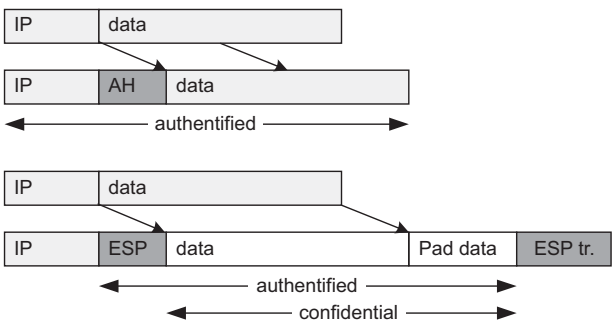


Fig. 8.8 The outer headers are retained in transport mode

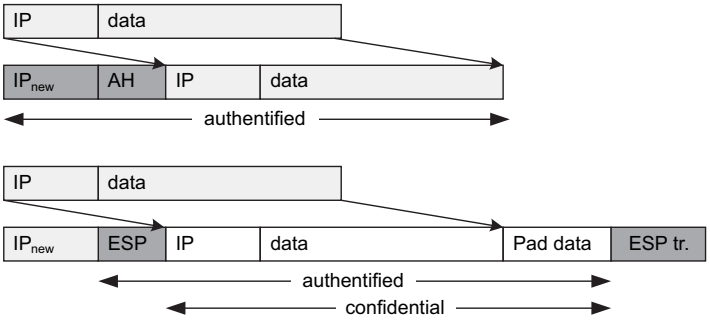


Fig. 8.9 The original address is hidden in tunnel mode, protected against changes by the checksum (authenticated) with AH, and encrypted in the confidential range with ESP.

algorithms is used as the standard procedure. If the checksum does not match the packet, integrity is no longer guaranteed. Authentication Header is rarely used on its own since there are hardly any applications where only the integrity is important.

Communication confidentiality is provided by ESP which encrypts the packets. In addition, integrity protection protects against manipulation, but not for the complete packet as with AH. With ESP, the IP address is not included in the calculation of the cryptographic checksum, meaning that this could be manipulated. However, this still does not permit IP spoofing since authentication of communications partners takes place during establishment of the tunnel. The standard procedures for encryption are Data Encryption Standard (DES), Rivest Cipher (RC4), 3 DES (extension of DES with more encryption depth) and Advanced Encryption Standard (AES).

In addition to selection of AH or ESP, it is possible to send the packets on the network in transport or tunnel mode. With transport mode (Fig. 8.8), the original IP header, i.e. IP address plus IP options, is used further. In tunnel mode, IPSec encapsulates the complete package including IP header, and writes a new IP header in front of this (Fig. 8.9). Thus the original IP address is no longer visible. The IP address together with the rest of the packet is only revealed again during the decryption at the other end.

The combination of ESP and tunnel mode is used as standard on VPN gateways if remote subnets are to be connected together over an insecure network. If two computers are to communicate with each other by means of IPSec in the LAN, transport mode is normally selected.

8.5.2 Key Management with Internet Key Exchange (IKE)

The most complex part of IPSec is secure exchange of keys over an insecure network. The use of keys with a fixed configuration such as the so-called Manual Keying certainly cannot be recommended since this is considered as insecure. Automatic key management with IPSec is implemented using the Internet Key Exchange protocol (IKE) and is based on the Internet Security Association and Key

Management Protocol (ISAKMP). The IKE negotiates the keys dynamically when establishing the connection. Furthermore, IKE carries out authentication of the stations and negotiation of the Security Associations (SA) in which the configuration of the connection is recorded. A Security Association is an agreement between the two communicating parties and considers the following points:

- Identification/authentication (either using Pre Shared Keying or Certificate-based procedure).
- Definition of key algorithm to be used for the IPsec connection.
- From which (IP) network is the IPsec connection made.
- To which (IP) network is the connection to be made.
- Periods in which renewed authentication is required.
- Period following which the IPsec key must be renewed.

The actual IKE works in two phases:

1. Establishment of a Security Association for negotiation of the used keys, for authentication of the communications partners, and for exchange of the integrity and confidentiality algorithms to be used.
2. Establishment of one or more SAs for communication of user data.

The Pre Shared Keying (PSK) or Certificate procedure is used for authentication in phase 1. Pre Shared Keying is a symmetrical key procedure. The key must be made known to both parties prior to communication. This key is automatically generated when creating a group. The major disadvantage: if someone obtains unauthorized access to this key, the key must be replaced on all involved stations in order to reestablish security. If a network is to grow, this procedure should also be rejected if only a few nodes are initially involved. The extra requirement for certificate-based authentication usually pays for itself after just a short time.

Certificate-based authentication has a different approach: X.509 certificates are used. This system is based on trustworthy CAs (Certification Authorities) or a hierarchy of these. The principle is that each individual end point knows its CAs, and that all certificates signed by these authorities are recognized as being valid. In practice, this means that all certificates from trustworthy CAs are accepted and that all certificates provided by these CAs therefore have access. The certificates for the Scalance S can be generated by a certification authority included in the Security Configuration Tool.

8.5.3 Limits of IPSec

One of the greatest problems when using IPSec is the NAT. IPSec provides authentication for computers, and NATs hide it – the two technologies are therefore directly contradictory. Depending on the NAT mode (Basic NAT or Network Address Port Translation, NAPT), a packet receives a new IP address and possibly also a new source port number. AH immediately surrenders its arms in this case because the packet header has been changed and thus the HMAC is no longer correct.

It is somewhat more complicated with ESP: in order to rewrite ports, an NAT router must be able to read the TCP/UDP header. However, the original header is encrypted, and an assignment is therefore impossible. To prevent having to rely on the router, the original IPSec is hardly usable at all. It is better to use it with the IPSec extension NAT-T (Traversal) (RFCs 3947 and 3948). In this case, the two parties exchange various information using the NAT Traversal protocol. The ESP packets are subsequently packed in UDP packets and sent via port 4500. NAT routers can then rewrite both IP addresses and ports.

8.6 Simatic Net Scalance S612 and S613

The hardware network components have two RJ45 ports and can therefore protect individual units or complete network segments. These are connected to one of the ports, generating the so-called internal protected network. The other port is the connection to the non-secure network (Fig. 8.10).

Different conditions exist in the industrial environment compared to offices. The hardware security modules are therefore provided with the following “I features”:

- Temperature range from -20°C to +70°C. In contrast to this, standard routers, switches or VPN gateways from the office sector have a limit of 40°C.
- IP30 degree of protection so that the inside of the module is protected against dust and dirt.
- Assembly on standard or Simatic rails, or wall mounting, where the housing can be installed in various positions.
- Redundant power supply (24 V DC).
- LED diagnostics on site.
- Alarm contact for immediate signaling if the module should fail for any reason.
- C-Plug to save the configuration data in order to enable replacement of the basic device without a programming device.

Fig. 8.10
Scalance S module with two RJ45 ports – bottom RJ45 socket for protected internal segment – top RJ45 socket for non-protected external segment

Table 8.1 DSummary of the Scalance S module functions

	S602	S612 V1	S612 V2	S613 V1	S613 V2
Firewall	x	x	x	x	x
NAT/NAPT router	x	–	x	–	x
DHCP server	x	–	x	–	x
Network Syslog	x	–	x	–	x
IPsec tunnel (VPN, Virtual Private Network)	–	x	x	x	x
Softnet Security Client (only in flat networks)	–	x	x	x	x

x function present – function not present

The Scalance S602, S613 and S614 devices differ with regards to the types of function (see Table 8.1) and the quantity framework of the VPN channels and connectable internal nodes. With a maximum of 128 VPN tunnels which can be used simultaneously and a maximum of 64 connectable internal nodes for the Scalance S613, a convenient quantity framework is available for users.

8.7 Simatic Net SOFTNET Security Client

The SOFTNET security client enables programming devices, PCs and notebooks to access network stations or automation systems protected by Scalance S. Communication can only be carried out between authenticated and authorized devices in an IPsec tunnel.

The SOFTNET security client PC software permits secure IP-based access from PCs/programming devices to the PLCs protected by Scalance S. By means of the software, a PC/programming device is automatically configured such that IPsec tunnels can be established to one or more Scalance S modules. This IPsec tunnel communication means that it is possible to access devices or networks located in an internal network protected by Scalance S using programming device/PC applications such as NCM diagnostics or Step 7 on a secure path.

The SOFTNET security client is provided for use with Windows 2000 Professional and XP systems. The client can manage up to 128 Scalance S modules with the associated internal nodes. The PC software has a GUI which is easy to use to configure the Windows security features. Following the configuration, the SOFTNET security client is executed in the background – visible by means of an icon in the Systray on your programming device/PC.

With the associated configuration tool, the creation and management of security rules can be carried out without special IT knowledge. In the simplest case, it is only necessary to create and configure the Scalance S modules or SOFTNET security clients which are to communicate securely with each other. Communication can be established as soon as the security client knows which PLCs are to be accessed (Fig. 8.11).

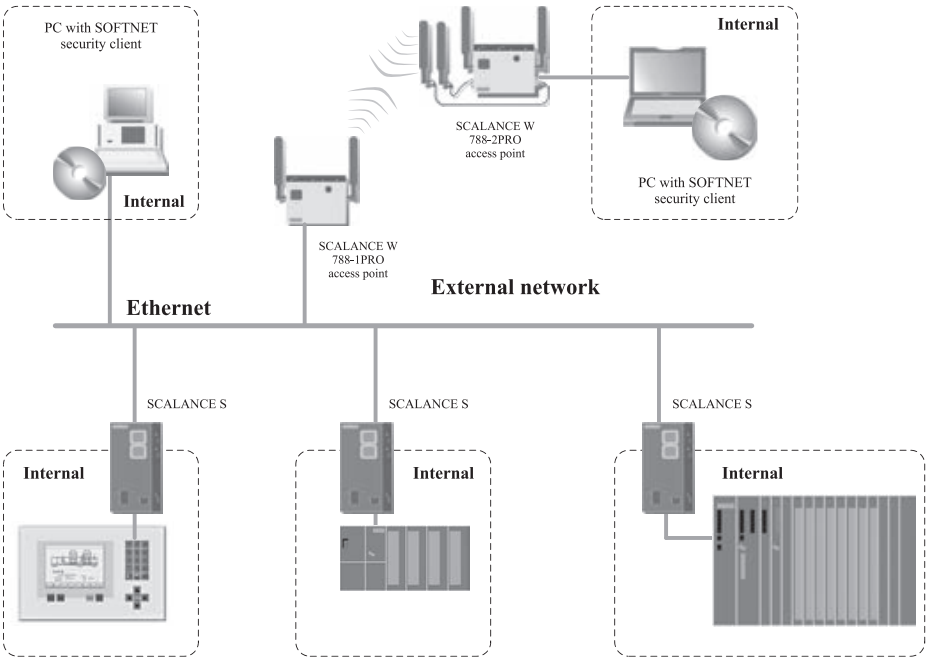


Fig. 8.11
Secure communication (wire-based or wireless) between programming devices (PGs) and devices protected by Scalance S

How does the SOFTNET security client function? The client reads the configuration generated by the security configuration tool, and uses the file to determine the certificates to be imported. The root certificate and the private keys are imported and saved in the local programming device/PC. Security settings are subsequently carried out in Windows using the configuration data; the security settings can be imported into the Windows IP security guidelines. If training mode is activated for the internal stations or PLCs, the configuration module initially sets the IP security guideline for the Scalance S module. The SOFTNET security client then address the Scalance S module in order to determine the IP addresses of the respective internal stations. The client enters these IP addresses into the IP filter lists of the security guideline. Applications such as Step 7 can subsequently communicate with the PLCs over VPN.

In the event of faults on the programming device/PC, the SOFTNET security client responds as follows:

- Configured security guidelines are retained following switching off and on of the programming device/PC.
- Messages are output if the configuration is faulty.

8.8 Example Configurations

Using a simple test network, you will now be introduced to the handling of Scalance S and the security configuration tool. You will see how the Scalance S protection functions can be implemented in the network without large configuration requirements. Two different security examples will be implemented, the two basic functions of Scalance S:

- Configuration of Scalance S as firewall
- Configuration of a VPN with Scalance S as IPsec tunnel end points.

8.8.1 Operation of Scalance S as Firewall

In this example, you configure the firewall in standard mode. The firewall functionality of Scalance S is responsible for protecting the internal network from influences or faults from the external network. This means that only specific, previously-defined communications relations between nodes from the internal network and nodes from the external network are allowed.

Using packet filter rules, you define the enabling or limitation of the passing data traffic based on properties of the data packets. The firewall can be used both for encrypted data traffic (IPsec tunnel) or for non-encrypted traffic. The default setting for the firewall is selected such that no IP data traffic is possible. Communication is only approved between the nodes in the internal networks of Scalance S modules via configured IPsec tunnels.

The standard mode includes predefined rules for the firewall according to Table 8.2, and you can select these rules in the input area “Configuration”.

The following example clarifies how you can initiate only IP traffic from an internal network. Only a reply is permissible from the external network. Rule: “Allow outgoing IP traffic” from internal network to external network.

Table 8.2 Possible rules for the Scalance firewall

Rule/option	Function
Only tunneled communication	This is the standard setting. Only encrypted IPsec data transfer is permissible with this setting; only nodes in internal Scalance S networks can communicate with one another. The option can only be selected if the module is present in a group. If this option is deselected, tunneled communication as well as the communication mode selected in the other option boxes are permissible.
Permit IP traffic from internal network to external network	Internal nodes can initiate a communications link to nodes in the external network. Only reply frames from the external network are passed on to the internal network. The external network cannot initiate a communications link to nodes in the internal network.
Permit IP traffic with S7 protocol from internal network to external network	Internal nodes can initiate an S7 communications link (S7 protocol, TCP/port 102) to nodes in the external network. Only reply frames from the external network are passed on to the internal network. The external network cannot initiate a communications link to nodes in the internal network.

Table 8.2 Possible rules for the Scalance firewall *(continued)*

Permit access to DHCP server from internal network to external network	Internal nodes can initiate a communications link to a DHCP server in the external network. Only the reply frames of the DHCP server are passed on to the internal network. The external network cannot initiate a communications link to nodes in the internal network.
Permit access to NTP server from internal network to external network	Internal nodes can initiate a communications link to an NTP server (network time protocol) in the external network. Only the reply frames of the NTP server are passed on to the internal network. The external network cannot initiate a communications link to nodes in the internal network.
Permit SiClock time-of-day frames from external network to internal network	This option is used to enable SiClock time-of-day frames from the external network to the internal network.
Permit access to DNS server from internal network to external network	Internal nodes can initiate a communications link to a DNS server in the external network. Only the reply frames of the DNS server are passed on to the internal network. The external network cannot initiate a communications link to nodes in the internal network.
Permit configuration of internal network nodes using DCP from external network to internal network	The DCP protocol is used by the PST tool to set the IP parameters with Simatic NET components. This rule permits nodes in the external network to access nodes in the internal network per DCP protocol.

Description of the example (Fig. 8.12):

- Internal network – connection to Scalance S port 2: in the internal network of the test structure, the network node is implemented by a PC which is connected to the “internal port” (port 2, green) of a Scalance S module.
  - PC2: represents internal network 1
  - Scalance S module 1: Scalance S module for internal network 1
- External network – connection to Scalance S port 2: the non-protected network (“external network”) is connected to the “external port” (port 1, red) of a Scalance S module.
  - PC1: PC with security configuration tool

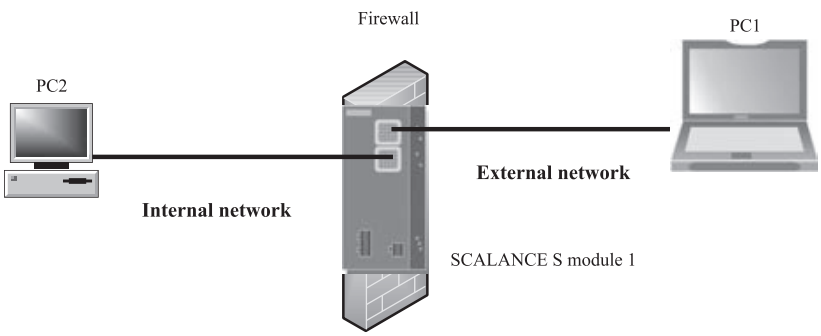


Fig. 8.12
Structure of the test network: PC1 is in the external network, PC2 is in the internal network, Scalance S works as a firewall

Step 1: Configure the Scalance S and network

Establish the physical network connections by inserting the plugs of the network cables into the provided ports (RJ45 sockets). In our example, connect PC2 to port 2 of module 1 and port 1 of module 1 to PC1. Caution: the Ethernet connections at port 1 and port 2 are handled differently by Scalance S, and therefore must not be interchanged when connecting to the communications network, otherwise the device will lose its protective function:

- Port 1 – external network: top RJ45 socket, red marking = non-protected network segment
- Port 2 – internal network: bottom RJ45 socket, green marking = network protected by Scalance S.

Step 2: Configure IP settings of PCs

The two PCs used are to receive the following IP address settings for the test:

- PC1: IP address = 191.0.0.1; subnet mask = 255.255.0.0
- PC2: IP address = 191.0.0.2; subnet mask = 255.255.0.0

To set the IP addresses, proceed as follows for PC1 and PC2:

1. On the associated PC, open the control panel with the menu command Start > Customize > Control panel > Network connections.
2. In the dialog “LAN connection properties”, activate the option box “Internet protocol (TCP/IP)” and click the “Properties” button.
3. In the dialog “Internet protocol properties (TCP/IP)”, select the option box “Use following IP address” and enter the values assigned to the PC in the fields provided. Close the dialogs with “OK” and exit the control panel.

Step 3: Create project and module in the configuration software (Fig. 8.13)

In order to create the projects and modules, install and start the configuration software “Security Configuration Tool” on PC1.

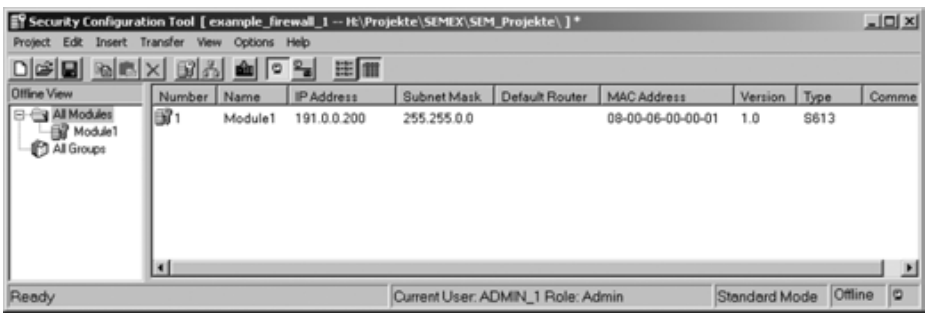


Fig. 8.13 Security configuration tool with configured module 1

1. Generate a new project using the Menu command Project > New.
2. Click “All modules” in the navigation area, and subsequently the line with “Module 1” in the contents area.
3. Click in the “Type” column, and select the type of module used.
4. Click in the “MAC address” column, and enter this in the defined format. You can find this address on the front of the Scalance S module.
5. Then click in the “IP address” column, and enter this in the defined format: 191.0.0.200

Step 4: Configure the firewall (Fig. 8.14)

Simple operation of the firewall in standard mode is based on predefined functions which provide you with immediate help. These functions can be activated by clicking.

1. Select “Module 1” in the contents area.
2. Select the menu command Edit > Properties... > and then the tab “Firewall” in the displayed dialog.
3. Deselect the option “Tunnel communication only” and select the option “Allow outgoing IP traffic”. This means that IP traffic can only be initiated by the internal network; only the reply is permissible from the external network.
4. Additionally select the log options for recording the data traffic.
5. Close the dialog with “OK”.
6. Now save this project with an appropriate name using the menu command Project > Save as...

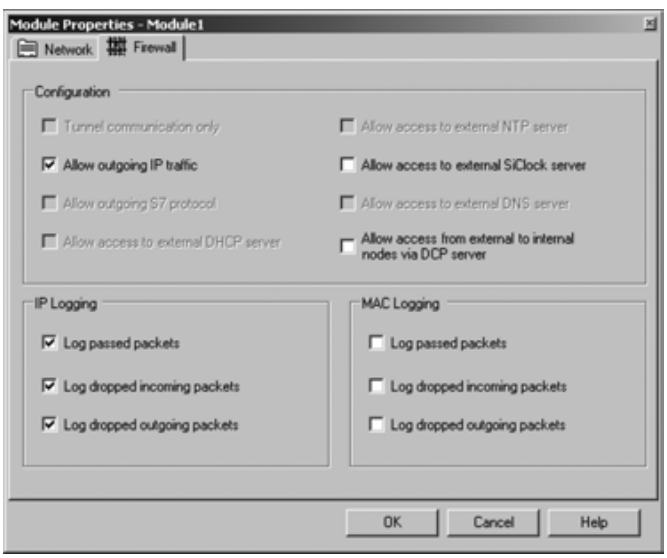


Fig. 8.14 Module Properties – setting of firewall rules

Step 5: Upload configuration into module

To upload the configuration into the module, proceed as follows in the security configuration tool on PC1:

1. Select the module in the contents area.
2. Select the menu command Transfer > To module.
3. Start the upload procedure using the “Start” button.
4. If the upload procedure has been completed without errors, the Scalance S module is automatically restarted, and the new configuration activated. Scalance S is now in productive mode. This state is signaled by a green lamp on the fault LED.

Starting of the configuration has thus been completed, and Scalance S now protects the internal network (PC 2) by means of the configured firewall according to the rule “Allow outgoing IP traffic” from the internal network to the external network.

How can you test the configured function?

You can best carry out the function test of the configured firewall with outgoing IP data traffic allowed as follows using a ping command:

1. Select the menu command Start > Run in the start bar on the PC2.
2. Enter the “cmd” command in the opened “Run” dialog.
3. Enter the ping command of PC2 on the PC1 (IP address 191.0.0.1) > ping 191.0.0.1
4. PC2 then sends small data packets to PC1. If PC1 receives these data packets, it signals this immediately back to PC2. When the IP frames have reached PC1, the displayed “Ping statistics” outputs the following for 191.0.0.1: Sent = 4; Received = 4; Lost = 0 (0% loss).

With Windows XP SP2, the firewall can be set as standard such that ping commands cannot pass. If necessary, you must enable the ICMP services of type Request and Response.

As a result of the configuration, the ping frames can be transferred from the internal network to the external network (Fig. 8.15). The PC in the external network

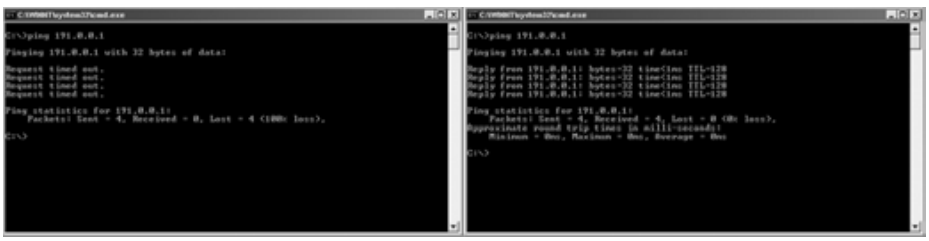


Fig. 8.15 Left: ping command from PC 2 to PC 1 is replied to by PC1; right: ping remains unanswered

has replied to the ping frames. As a result of the “Stateful inspection” function of the firewall, the response frames coming from the external network are automatically passed on into the internal network.

Now test the function of the firewall configuration with outgoing IP data traffic disabled as follows:

1. Change to offline mode again on the PC1 in the security configuration tool using the menu command View > Offline.
2. Call the firewall dialog again as already carried out previously.
3. In the tab “Firewall”, disable the option “Allow outgoing IP traffic” again. Close the dialog with “OK”.
4. Upload the modified configuration again onto the Scalance S module.

Following the upload procedure executed without errors, again enter the same ping command (ping 191.0.0.1) in the window with the input prompt of PC2, as already carried out.

The IP frames of PC2 must not now reach PC1 since data traffic from the “internal network” (PC2) to the “external” network (PC1) is not allowed. This is indicated as follows in the display “Ping statistics” for 191.0.0.1: Sent = 4; Received = 0; Lost = 4 (100% loss).

8.8.2 VPN Tunnel with Scalance S

In the internal networks protected by Scalance S, the node of a secure data link is made available by the non-secure, external network through an IPsec tunnel.

Data exchange between units via the IPsec tunnel in the VPN therefore exhibits the following properties:

- Confidentiality: the exchanged data are tap-proof.
- Integrity: the exchanged data cannot be falsified.
- Authenticity: tunnels can only be established by those with appropriate privileges.

Scalance S uses the IPSec protocol (tunnel mode of IPSec) for tunneling.

In this example, the tunnel function is configured in the configuration view “Standard mode”. Scalance S modules 1 and 2 are the two tunnel end points in this example for the secure VPN tunnel link. With this configuration, IP traffic is only possible via the configured tunnel links between authorized partners.

Description of the example:

- Internal network – connection to Scalance S port 2: in the internal network of the test structure, the network node is implemented in each case by a PC which is connected to the “internal port” (port 2, green) of a Scalance S module.

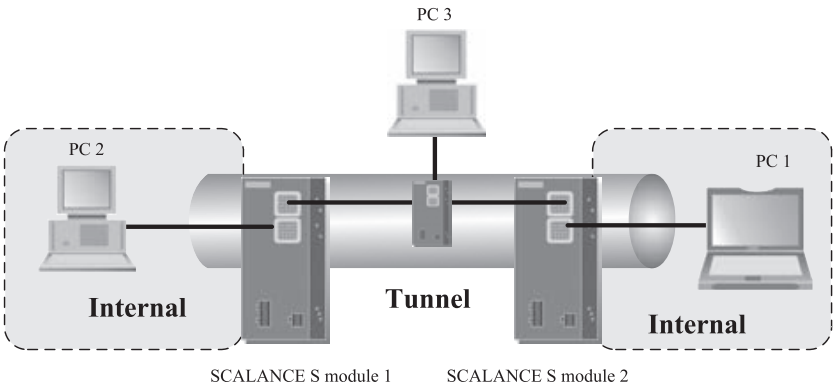


Fig. 8.16
Structure of the test network: PC1 and PC2 form an internal network which is connected by a VPN tunnel between two Scalance S modules.

  - PC2: represents internal network 1
  - PC2: represents internal network 2
  - Scalance S module 1: Scalance S module for internal network 1
  - Scalance S module 2: Scalance S module for internal network 2
- External network – connection to Scalance S port 2: the non-protected network ("external network") is connected to the "external port" (port 1, red) of a Scalance S module.
  - PC3: PC with security configuration tool

Step 1: Configure the Scalance S and network

Establish the physical network connections by inserting the plugs of the network cables into the provided ports (RJ45 sockets). Connect PC1 to port 2 of module 1 and PC2 to port 2 of module 2. Connect port 1 of module 1 and port 1 of module 2 using a switch to which PC3 is connected.

Step 2: Configure IP settings of PCs

The three PCs used are to receive the following IP address settings for the test:

- PC1: IP address = 191.0.0.1; subnet mask = 255.255.0.0; standard gateway 192.168.10.100
- PC2: IP address = 191.0.0.3; subnet mask = 255.255.0.0; standard gateway 192.168.10.101
- PC3: IP address = 191.0.0.3; subnet mask = 255.255.0.0; standard gateway 192.168.10.102

To set the IP addresses, proceed as follows for PC1, PC2 and PC3:

1. On the associated PC, open the control panel with the menu command Start > Customize > Control panel > Network connections.
2. In the dialog “LAN connection properties”, activate the option box “Internet protocol (TCP/IP)” and click the “Properties” button.
3. In the dialog “Internet protocol properties (TCP/IP)”, select the option box “Use following IP address” and enter the values assigned to the PC in the fields provided. Close the dialogs with “OK” and exit the control panel.

Step 3: Create project and module in the configuration software (Fig. 8.17)

In order to create the projects and modules, start the configuration software “Security Configuration Tool” on PC1.

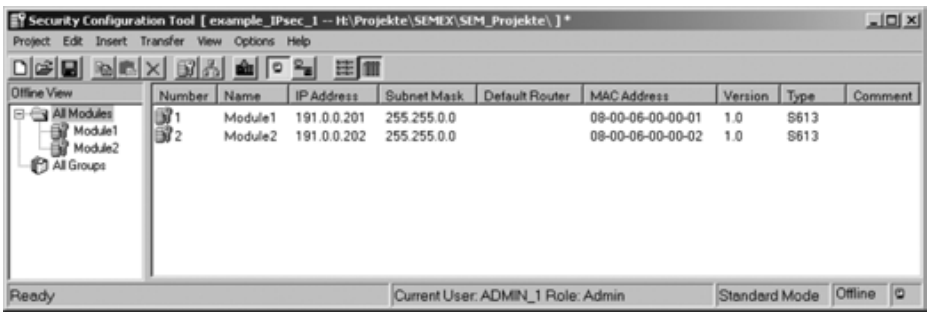


Fig. 8.17 Security configuration tool with configured modules 1 and 2

1. Generate a new project using the menu command Project > New.
2. Click “All modules”.
3. Generate a second module using the menu command Insert > Module. This module is automatically assigned the name “SEM2” and also predefined parameter values. The IP address is incremented compared to “Module 1”, i.e. it is different.
4. Click “All modules” in the navigation area, and subsequently the line with “Module 1” in the contents area.
5. Click in the “Type” column, and select the type of module used.
6. Click in the “MAC address” column, and enter this in the defined format. You can find this address on the front of the Scalance S module.
7. Then click in the “IP address” column, and enter this in the defined format: 191.0.0.201 for module 1.
8. Repeat steps 5. to 7. with “Module 2” and the IP address 191.0.0.202.

Step 4: Configure the VPN tunnel connection (Fig. 8.18)

Two Scalance S modules establish an IPSec tunnel for secure communication if they are assigned to the same group in the project. Proceed as follows to configure the connection:

1. Generate a group. To do this, select “Groups” in the navigation area, and generate a new group with the menu command Insert > Group. This group is automatically assigned the name “Group 1”.
2. Select the Scalance S module 1 in the contents area, and drag it to “Group 1” in the navigation area. The module is now assigned to this group, or is a member of this group. The color of the key symbol of the module icon changes from gray to yellow.
3. Select the Scalance S module 2 in the contents area, and drag it to “Group 1” in the navigation area. The module is now also assigned to this group.
4. Configuration of the VPN tunnel connection has now been completed.

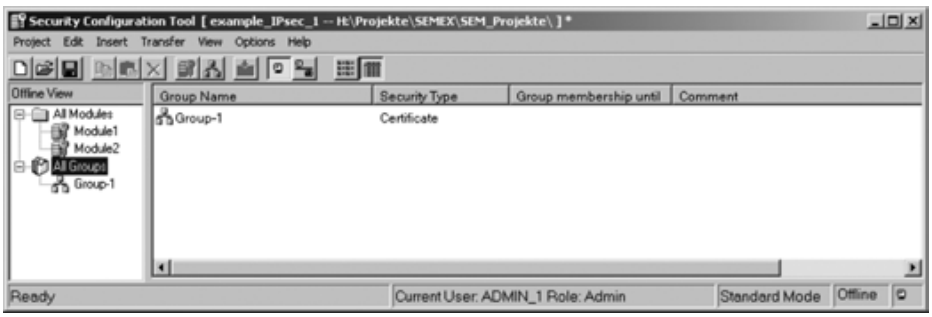


Fig. 8.18
Security configuration tool with configured VPN connection between module 1 and module 2

Step 5: Upload configuration into the Scalance S module

To upload the configuration into the module, proceed as follows in the security configuration tool (Fig. 8.19):

1. Select the dialog “Upload all security modules” using the menu command Transfer > To all modules.
2. Select the two modules using the “Select all” button.
3. Start the upload procedure using the “Start” button.
4. If the upload procedure has been completed without errors, the Scalance S module is automatically restarted, and the new configuration activated. Scalance S is now in productive mode. This state is signaled by a green lamp on the fault LED.

Starting of the configuration has thus been completed, and the two Scalance S modules can establish a communications tunnel via which the network nodes of the two internal networks can communicate in secure mode.

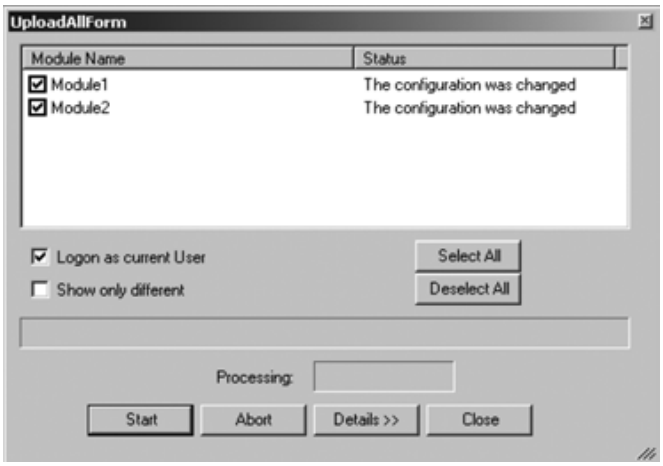


Fig. 8.19 Uploading the configuration data onto all modules

Please note: layer 2 frames are only tunneled if a router is not present between two Scalance S modules. In addition: non-IP frames are only transmitted via a tunnel if the devices sending or receiving the frames were already previously able to communicate, i.e. without the use of Scalance S. Whether the network nodes can communicate prior to the use of Scalance S depends on the IP networks in which the Scalance S modules are present. If the Scalance S modules are in the same IP subnet, it is assumed that the data terminals could also communicate with non-IP frames in the secure networks of the Scalance S even before use of the Scalance S. The non-IP frames are then tunneled.

How can you test the configured tunnel?

You can most appropriately carry out the function test of the tunnel between PC2 and PC3 as follows using a ping command:

1. Select the menu command Start > Run in the start bar of the PC2. Entered the “cmd” command in the opened “Run” dialog.
2. Enter the ping command of PC2 on the PC3 (IP address 191.0.0.3) > ping 191.0.0.3
3. PC2 then sends small data packets to PC3. If PC3 receives these data packets, it signals this immediately back to PC2. When the IP frames have reached PC2, the displayed “Ping statistics” outputs the following for 191.0.0.3: Sent = 4; Received = 4; Lost = 0 (0% loss).

Since no other communication was permissible, these frames can only have been transported through the VPN tunnel.

Now repeat the test with tunnel communication switched off:

1. Select the line “Module 1” in the contents area of the security configuration tool. Select the line “Module 1” in the contents area.

2. Select the menu command Edit > Properties...
3. Select the tab “Firewall” in the displayed dialog. Deselect the option “Only tunneled communication”.
4. Once the upload procedure has been executed without errors, enter the same ping command again (ping 191.0.0.3) in the input prompt window of PC2 as already carried out. The IP frames of PC2 must not reach PC3 since neither tunnel communication is configured between these devices nor is normal IP data traffic permissible. This is output in the displayed “Ping statistics” for 191.0.0.3 as follows: Sent = 4; Received = 0; Lost = 4 (100% loss).

9 Safety Technology and Profinet

Until a few years ago, safety technology was frequently a separate part of the automation function. It was designed using conventional relay technology, and the data of the safe automation function had to be incorporated into the standard automation function at great effort. New international standards (e.g. IEC 61508) made it possible to also implement the safety technology using program-controlled systems and communication. The next step was thus already predestined: integration of safety technology into the Simatic standard automation – Safety Integrated.

According to current understanding, safety functions are an integral component of an automation solution. A separate solution using conventional technology is now only used with small applications, usually for cost reasons.

For a number of years already, Siemens has been offering this facility of complete integration by means of Safety Integrated. Using Simatic S7 fail-safe controllers, both standard and fail-safe programs can be executed in one CPU. The engineering functionality is integrated into the Simatic Manager using the "Distributed Safety" option package, thus providing users with an engineering environment for standard and fail-safe automation. Using the PROFIsafe profile it is possible to also implement this integration for communication with Profibus DP and the distributed I/O.

These technologies have made it possible for users to develop new applications, to redesign existing applications significantly more effectively, to improve machine productivity, and furthermore to reduce the risks for personnel.

The acceptance of Profinet by users was therefore linked right from the beginning to the availability of the safety technology. It was only necessary to slightly revise the PROFIsafe specification (buzzword: "V2 mode") in order to also be able to use Profinet in safety-related plants. This opens up completely new fields of application, especially with regards to the use of WLAN technology in combination with PROFIsafe.

Profinet with PROFIsafe is the first communications standard which permits both standard and safety-related communication over "one cable" on the basis of Ethernet.

9.1 Introduction to Safety Technology

The objective of safety technology is to keep the risks for personnel, investments and the environment as low as possible using technical equipment, without limit-

ing industrial production, use of machines or manufacture of chemical products more than absolutely necessary.

From the viewpoint of the commodity to be protected, safety is an indivisible entity. However, since the causes of risks and thus also the technical measures required to avoid them can be highly different, a distinction is made between different types of safety, e.g. by specifying the respective cause of the possible danger. One therefore refers to “electrical safety” when reference is to be made to protection against dangers by electricity, to “intrinsic safety” when the reference is to protection against explosions, or “functional safety” if the safety depends on correct functioning.

There are therefore also special standards associated with functional safety, in particular the basic standard IEC 61508 (also EN 61508 and DIN EN 61508/VDE 0803) which has introduced the new SIL term and covers the functional safety of electrical, electronic and programmable electronic systems independent of a special field of application. In the machine safety sector, these are supplemented by EN 954, ISO 13849 and IEC 62061.

In order to achieve functional safety for a machine or plant, it is necessary for the safety-relevant parts of the protection and control equipment to function correctly and respond in the event of a fault such that the plant remains in a safe state or is set to such a state.

This requires the application of particularly qualified technology which satisfies the requirements of the associated standards. The requirements for achievement of functional safety are based on the fundamental objectives:

- Avoidance of systematic faults
- Control of systematic faults
- Control of random faults or failures.

9.1.1 Objective of Standards

The vendors and users of technical equipment and products are responsible for their safety. This means that it is necessary to make plants, machines and other technical equipment as safe as possible using state-of-the-art technology. To achieve this, economic partners define standards to describe the state-of-the-art with respect to all aspects of the complete safety lifecycle, from risk analysis up to taking out of service. Through observation of the respective standards it can be guaranteed that the state-of-the-art is achieved and that the constructor of a plant or the manufacturer of a machine or device has observed his or her obligation to exercise diligence.

Important standards for machine safety:

- EN 292 (ISO 12100-1) “Safety of machinery – Basic concepts, general principles for design”
- EN 1050 (ISO 14121) “Principles for risk assignment”

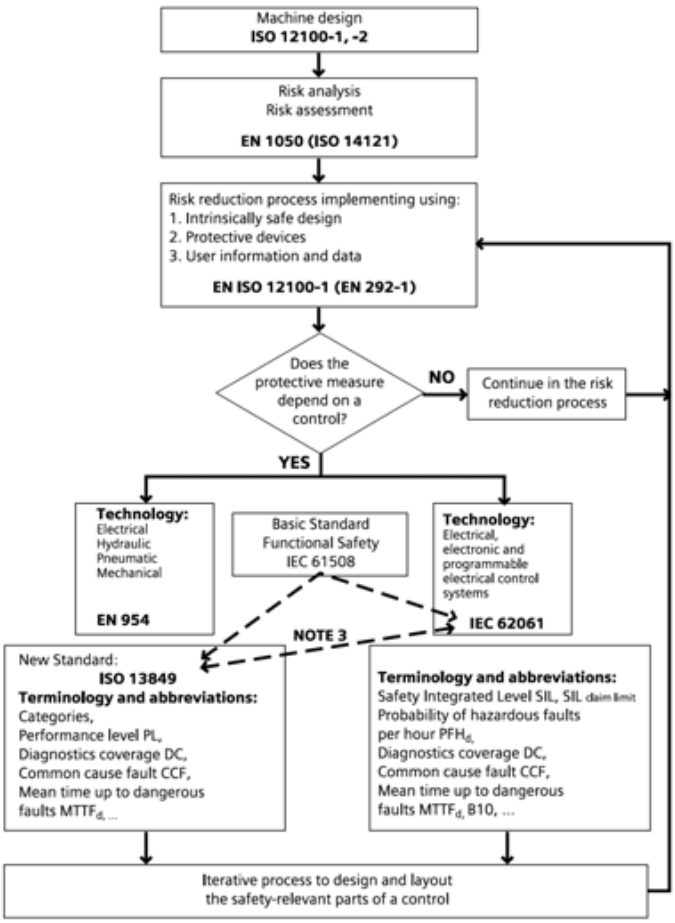


Fig. 9.1 Design process for a machine – in the case of non-electric technologies, parts are used as subsystems which correspond to EN ISO 13849-1

- EN (IEC) 60204-1 “Electrical equipment of machines – General requirements”
- EN 954 (ISO 13849-1) “Safety-related parts of control systems – General principles for design”
- IEC (EN) 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”. Is ratified as EN, i.e. national standards in Europe (e.g. VDE 0801) are being withdrawn.

The machine directive specifies that the manufacturer or his/her authorized representative in the EU (European Union) is obliged to:

- only bring into circulation machines with the maximum degree of safety
- carry out risk assessment in order to analyze all risks present in a machine and to minimize them as necessary

- observe and document the machine conformity with regards to the basic occupational health and safety requirements, and
- to guarantee that the stipulated documentation is archived up to 10 years following production of the last machine.

The structure shown in Fig. 9.1 is based on the lifecycle model, i.e. the sequence of individual tasks is oriented according to the sequence in which the individual phases of the machine and plant engineering are carried out.

9.1.2 Risk Assessment

Machines and plants also present risks because of their design and functionality. Therefore the machine directive specifies a risk assessment for each machine and also the minimization of risks as necessary until the residual risk is smaller than the tolerable risk. The following standards cover the procedure for evaluation of these risks:

- EN ISO 12100 “Safety of machinery – Basic concepts, general principles for design” and
- EN 1050 (ISO 14121) “Safety of machinery, Principles for risk assessment”.

EN ISO 12100 mainly describes the risks to be considered and the design principles for their minimization, EN 1050 describes the iterative process with risk assessment and minimization in order to attain the desired level of safety.

Risk assessment is a sequence of steps allowing systematic investigation of dangers resulting from machines (Fig. 9.2). Where necessary, risk assessment is followed by risk reduction.

Repetition of this procedure results in the iterative process with which dangers can be eliminated as far as possible and corresponding protective measures can be taken.

Risk assessment comprises:

- **Risk analysis**
  a) Determination of the limits of the machine (EN ISO 12100, EN 1050 Section 5)
  b) Identification of the dangers (EN ISO 12100, EN 1050 Section 6)
  c) Procedures for risk estimation (EN 1050 Section 7)
- **Risk evaluation** (EN 1050 Section 8)

According to the iterative process for achieving safety, risk estimation is followed by risk evaluation. It is necessary to decide whether minimization of the risk is necessary. If the risk is to be reduced even further, appropriate protective measures must be selected and applied. The risk assessment must then be repeated. Risk elements are defined to help in the risk evaluation. If the required safety is still not achieved, measures are necessary to minimize the risk. Risk minimization must be carried out using appropriate design and implementation of the machine, e.g. using controllers or protective measures suitable for safety func-

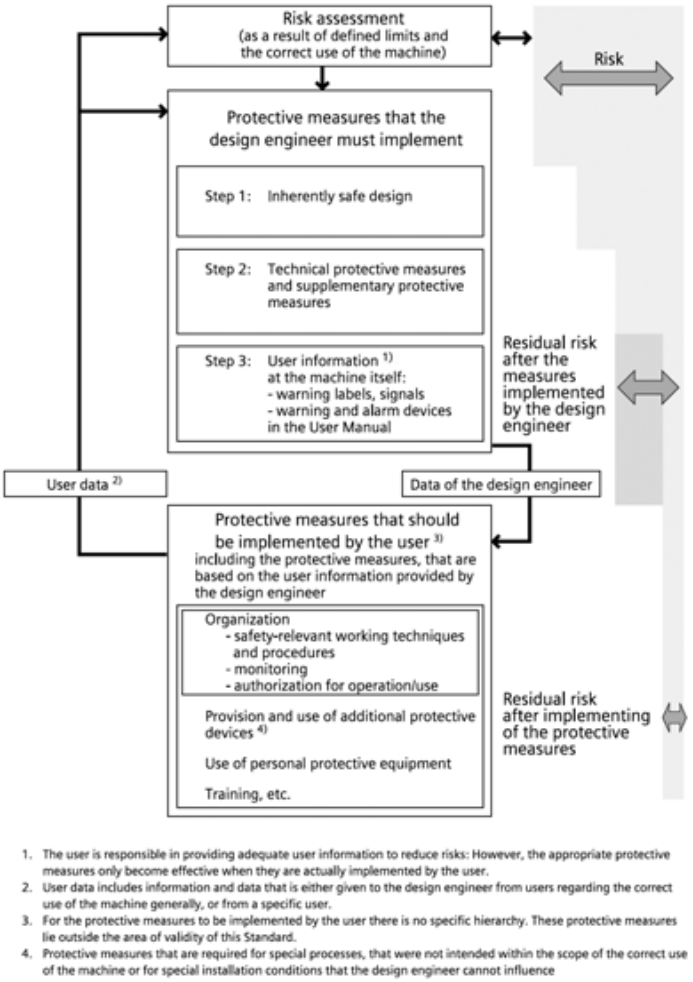


Fig. 9.2 Risk assessment of a machine

tions. If the protective measures include interlocking or control functions, these must be designed in accordance with EN 954 (successor standard: ISO 13849). Furthermore, electronic controllers and bus systems must also comply with IEC/EN 61508. For electrical and electronic controllers, EN 62061 can be used as an alternative to EN 954.

Note: This book can only present a small section of the topic of machine safety. For further information, please refer to the “System Manual Safety Integrated” which deals with the topic in detail. Important contents have already been reproduced above. It is available as a PDF file free-of-charge at www.siemens.com/safety.

9.2 Integrated Safety Technology

Up until now, it was standard procedure to solve safety tasks and standard tasks using different systems. This resulted in non-conform systems and considerable additional overhead. With Simatic Safety Integrated, standard automation and safety technology are integrated in an innovative complete system through application of PROFIsafe. Existing Simatic know-how and knowledge of safety technology are sufficient in order to solve safety-related tasks with Simatic.

Standard automation has become far more flexible and open through the change to intelligent control and decentralization. This has greatly increased machine and plant productivity. Automation becomes even more efficient if safety technology consistently follows this trend and is integrated seamlessly into standard automation. This means:

- Utilization of existing Step 7 know-how from engineering up to maintenance
- Application of existing network structures for fail-safe communication, too
- Application of existing components and infrastructure for safety technology, as far as possible.

Through integration of safety functions into the world of Totally Integrated Automation, standard automation and safety automation grow together into a uniform complete system. Simatic Safety Integrated comprises fail-safe Simatic PLCs as well as the I/Os and engineering included in the product range of Safety Integrated.

If a fault occurs, the PLC or a partial process can be brought to a safe state and retained there. Such fail-safe PLCs are based on proven Simatic standard PLCs. Both Profibus and Profinet have been expanded for safety-related communication

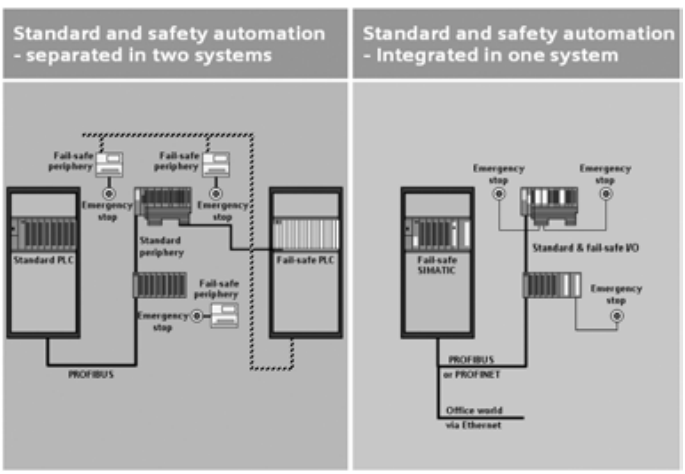


Fig. 9.3 Separate and combined standard and safety automation

by means of the multi-vendor PROFIsafe profile. Thus safety-related and standard communication are possible over just one standard cable.

Engineering for the standard and safety functions of the fail-safe Simatic PLCs is always carried out with the same Step 7 configuring and programming tools. Thus the safety technology is integrated seamlessly into the standard automation in a Simatic PLC. This also simplifies operation of the total plant. The training requirements are reduced in addition to lower engineering costs.

A further advantage is that comprehensive diagnostics of safety-related signals can be directly monitored on standard panels and HMI devices. As a result of the bit modular design of the fail-safe I/O, safety technology needs only be used where it is actually necessary. It is easy to design a combined strucutre featuring safety and standard components. Furthermore, the joint presence of safety-related and non-safety-related programs in one PLC and on a common bus system presents no problems. The interfacing of fail-safe fieldbus devices from other vendors is also simple to implement using Profibus or Profinet and the multi-vendor PROFIsafe profile (Fig. 9.3).

9.3 Technological Concept of PROFIsafe

The major point when defining the PROFIsafe profile was the reaction-free coexistence of safety-related and standard communication on the same bus cable. Furthermore, the required safety should be possible on a single-channel communications system, but the optional possibility for increased availability using redundancy of message channels should not be blocked.

Profibus International (PNO) already published the results of a working party in spring 1999 covering guidelines for safe communication on the standard Profibus with the protected trade name PROFIsafe. This was confirmed by positive technical reports from BGIA and TÜV (German Technical Inspectorate). Right from the beginning, the objective of the working party was to involve as many partners as possible in the definition and solution-finding processes and to openly present the results. In addition to manufacturers of safety systems, more than 25 renowned national and international manufacturers of fail-safe sensors and actuators, machine tool factories, end users and university institutes were represented. Intermediate and final results were constantly agreed upon with the BGIA and TÜV. Significant contributions came from the German Association of Machine Tool Manufacturers (VDW). As a result of this common exchange of safety scenarios, a semi “standardized” and complete requirement profile for distributed safety technology was produced in which the PROFIsafe concept could always be reflected. The requirement also existed for integrating more complex devices associated with optical safety technology, e.g. laser scanners and light curtains. The following sections show how PROFIsafe satisfied all the mentioned requirements.

PROFIsafe can be used to implement safety-related plants extremely flexibly. On the one hand, a single-cable solution is possible with combined standard and safety automation in one CPU. On the other hand, two separate CPUs and bus cables

can be used for this purpose, if the user so desires. The “homogenous solution” with just one bus system obviously has advantages – especially with regards to engineering.

Development of the PROFIsafe specification was already carried out according to the IEC 61508 standard. The inspiration was the prEN 50159-1 which indicated similar solutions for the rail sector. Further relevant standards were also taken into consideration. The safety levels achieved are Safety Integrity Level 3 (IEC 61508), Cat. 4 (EN 954-1).

9.3.1 Technical Advantages of PROFIsafe

PROFIsafe is based on previously introduced standard communication components (cables, ASICs, software packages). The safety measures are present in the safety-related communication end stations. The PROFIsafe layer implements this above the bus protocol using a transmission channel which is considered as a “black channel” analogous to a “black box” (Fig. 9.4).

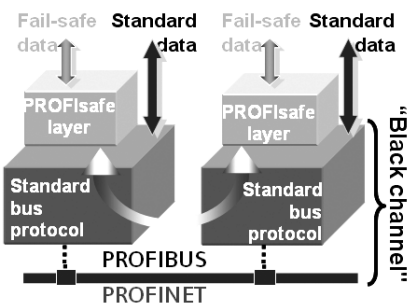


Fig. 9.4
Black channel: the safety mechanisms are present in the stations

There are basically no limitations with regards to baud rate, number of bus stations or transmission technology providing the response times required by the automation task are observed. Furthermore, PROFIsafe provides the advantage that users need not take any special measures with regards to bus cable, shielding, bus coupler etc. To summarize, PROFIsafe offers the following advantages:

- Open, multi-vendor protocol profile for Profinet and Profibus
- Single-cable solution for safety-related and standard communication
- No special measures required if safety technology is added

Error detection with PROFIsafe

In order to guarantee the functional safety, all communication errors are recorded by the PROFIsafe protocol. To achieve this, PROFIsafe makes sure that the values are transmitted correctly in the frames and that the frames arrive within a defined period. Furthermore, PROFIsafe also allows safety-related and complex terminal

equipment to be connected which require more extensive parameterization or can deliver complex data.

Fields of application for PROFIsafe

PROFIsafe is always used if safety during communication over Profibus is required with distributed plants. This is particularly the case if fail-safe stations are to be additionally connected to an existing bus without having to carry out complex hardware extensions.

9.3.2 PROFIsafe in the 7-layer Communications Model

The safety measures with the PROFIsafe profile are found above layer 7 of the ISO/OSI communications model (Fig. 9.5). A further layer is required for this which takes care of the safety-related provision and conditioning of the user data. This function can be implemented in a fail-safe field device e.g. using its technology firmware. The process signals or values are packed in corresponding user frames just like in standard mode. With fail-safe data, they are merely supplemented by safety information. A standard mechanism is also used to send the safety-related frames, i.e. master/slave mode: a master, which is usually assigned to a CPU, exchanges frames cyclically with all its configured slaves.

On the one hand, PROFIsafe permits fail-safe communication through mastering of all communication errors, whereby the safety is continuously monitored on the Profibus. On the other hand PROFIsafe also allows the interfacing of complex terminal equipment through corresponding extensions to the protocol. Complex parameters or their modifications can be conveniently loaded via the communications channel.

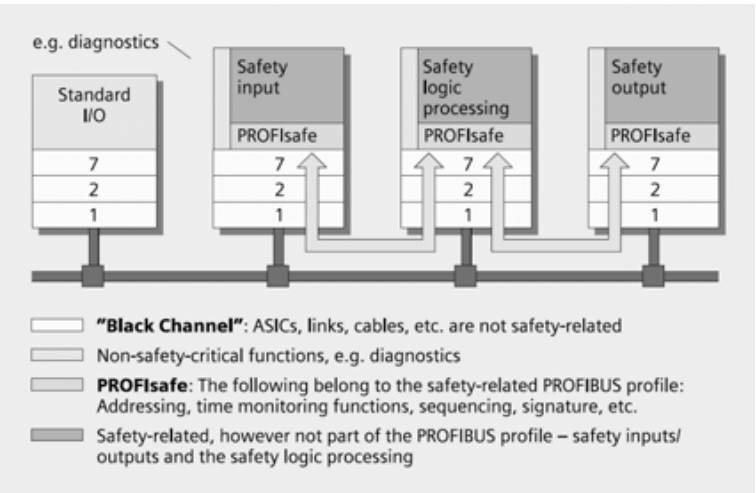


Fig. 9.5 PROFIsafe in the 7-layer model: the safety mechanisms are based on layer 7

9.3.3 Discovery of Possible Communication Errors to Achieve Functional Safety

A number of faults can occur when sending frames: they can be lost, appear repeatedly, be inserted additionally, appear in the wrong sequence or with a delay, or exhibit data falsification. Faulty addressing is also possible, i.e. a standard frame appears erroneously at a safety station and presents itself as a safety frame (masquerade).

Table 9.1 shows the possible causes of faults and the countermeasures possible with PROFIsafe. These include:

- Continuous numbering of the safety frames
- Anticipated time with acknowledgment
- Code for sender and receiver ("password" = PROFIsafe address)
- Additional protection of data with CRC (cyclic redundancy check).

Using the consecutive number, a receiver can recognize whether all frames have been received in the correct sequence.

In safety technology, it is not only important that a frame transmits the correct process signals or values but that these must also arrive within a defined time (fault tolerance time) so that the respective station can automatically initiate safety reactions on site if necessary. To this end, the stations have an adjustable timeout which can be reset when a safety frame has been received. The 1:1 relationship between master and a slave facilitates recognition of misdirected frames. The master and slave need only have a unique code (password) on the network with which they can check the authenticity of a frame. Data protection using CRC plays a key role. This is additionally responsible for ensuring the integrity of the parameters deposited in the respective terminal equipment in addition to the integrity

Table 9.1 Possible communication errors, and PROFIsafe countermeasures

Fault	Measure			
	Consecutive number (sign-of-life)	Anticipated time with acknowledgment	Code for sender and receiver	Data protection
Repetition	X			
Loss	X	X		
Insertion	X	X	X	
Incorrect sequence	X			
Falsification of user data				X
Delay		X		
Mixing of safety-related and standard frames (masquerade), including incorrect and double addressing		X	X	X
FIFO, fault within the router		X		

of the user data transported. Since data protection measures were used neither by the standard Profibus nor by the standard Profinet for proof of safety, this proof was therefore somewhat more costly for PROFIsafe, but provided decisive advantages for users: these need not take any special measures fpr PROFIsafe with regards to bus cables, shielding, bus couplers etc.

9.4 Simatic Products with PROFIsafe Capability

The first PROFIsafe products introduced worldwide were the Simatic S7-414FH and S7-417FH with the distributed ET 200M fail-safe I/O system in 1999. These can also be of redundant design, and guarantee additional fault tolerance, making them particularly suitable for process automation. Simatic S7-315F-2PN/DP, S7-317F-2PN/DP and S7-416F-3PN/DP fail-safe PLCs are also available with production engineering as the focal point, and support both Profibus and Profinet. In addition to the ET 200M (currently only Profibus), the ET 200S, ET200pro (Profibus and Profinet) and ET 200eco extend the range of fail-safe I/O systems. This is also supplemented by complex sensors and actuators and proximity-type protective equipment from the SIGUARD Safety Integrated range with direct connection to Profibus/PROFIsafe. The fail-safe Sinumerik 840D can be linked in the same manner.

9.5 PROFIsafe and Profinet with IWLAN

The use of Profinet in automation engineering provides a completely new range of applications in addition to various advantages. Wireless communication permits applications to be designed far more efficiently using new approaches. Versatile applications are possible, starting from the replacement of sliprings subject to wear and extensive maintenance up to the use of mobile operator panels.

In such applications, both standard and safety-related data have to be transmitted. For example, drives have to be brought to the safe state in the event of a fault, irrespective of whether the signal is from a safe sensor or a mobile operator panel.

It has been confirmed for PROFIsafe by both the TÜV and BGIA that the fault detection measures of the protocol profile are also suitable for radio transmission links, so that these can also be counted to the “black channel”. However, there are conditions which absolutely have to be observed. These concern data security, availability and special mobile applications.

For data security, it has been accepted that the measures described in the IEEE standard 802.11i or comparable measures provide sufficient protection with regard to authentication and encryption. Only the so-called “Infrastructure mode” is permissible, but not the “Ad hoc mode”. Infrastructure mode necessitates configuration of the radio equipment and the approved participants (e.g. maintenance personnel).

A prerequisite for safe communication is sufficient availability of the basic transmission path. Cable-based transmission requires appropriate installation in order to minimize EMC problems. Radio transmissions depend on good planning of the radio field, where the possible signal strengths can be determined in advance using simulations.

There are two basic classes of radio-based applications:

1. The plant components move along fixed paths and are connected via radio (e.g. rotary tables, stacker cranes)
2. The plant components can move around “freely” (e.g. mobile operator panels).

Configuration of the plant is relatively simple in the first case, and no special considerations are necessary with regards to the safety technology. In the second case, measures must be taken, for example, to clarify the plant components on which the emergency stop button of the mobile panel is to act if the operator is outside the range, or if he/she is present with the panel in the range of a different machine, or if the strength of his/her panel’s battery becomes weaker.

All these questions will be answered soon by certified radio panel solutions. However, it can be said that IWLAN is being increasingly combined with safety technology and that the initial hurdles have been overcome.

PROFIsafe monitors the delivery of a frame within a configured time. Profinet handles this using deterministic cyclic data traffic. These deterministics are also expected of the radio link. Extensions to the protocol have resulted in an improvement in performance above the IEEE standard. For example, the rapid roaming mechanism (RR) from Siemens provides guaranteed cycle times even when the participant moves from one access point to the next (roaming). This situation is basically critical since the radio participant requires a certain time to log-on with the new access point.

PROFIsafe is based on a model of independent processing elements: record – transmit – evaluate – transmit – react. For a safety function, each part of the system is provided with a time monitoring function which triggers in the event of a failure or an excessively long delay. The response time achievable is therefore based on a combination of the worst case delays of the individual elements plus the longest time monitoring on failure of the associated element. With PROFIsafe, cable-based (safety) response times of approximately 30 milliseconds can be achieved for digital inputs/outputs. At least the worst case time of the radio transmission in both directions must be added to this.

Data security plays an important role in addition to deterministics and performance. Access control is important in addition to data encryption, since prevention of access to a data network is already the first barrier for an unauthorized intruder. It is then impossible to change the safety-relevant data, and malfunctions resulting from manipulation are avoided.

9.6 System Overview of Profinet with PROFIsafe

Figs. 9.6 and 9.7 explain the communication possibilities provided by Profinet in safety-related applications.

Through the use of the standard PN/PB-Link, safety-related data can also be transmitted. A special link is not required. Thus existing plant components are easy to integrate.

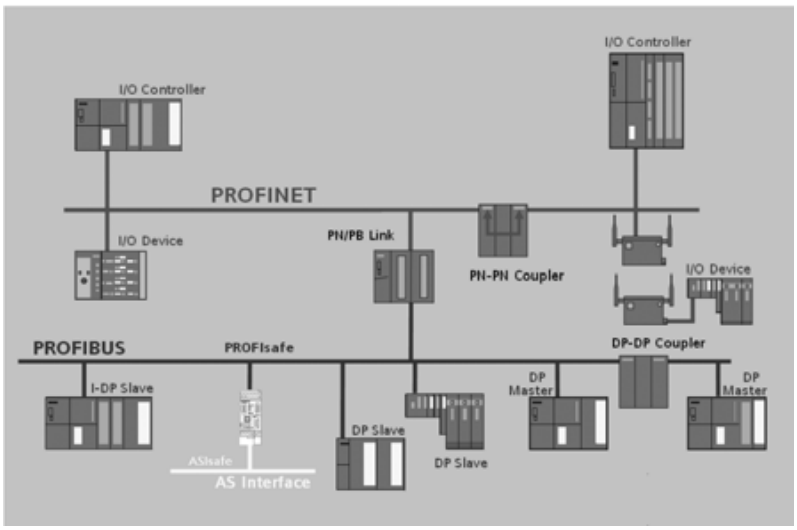


Fig. 9.6 Connection possibilities

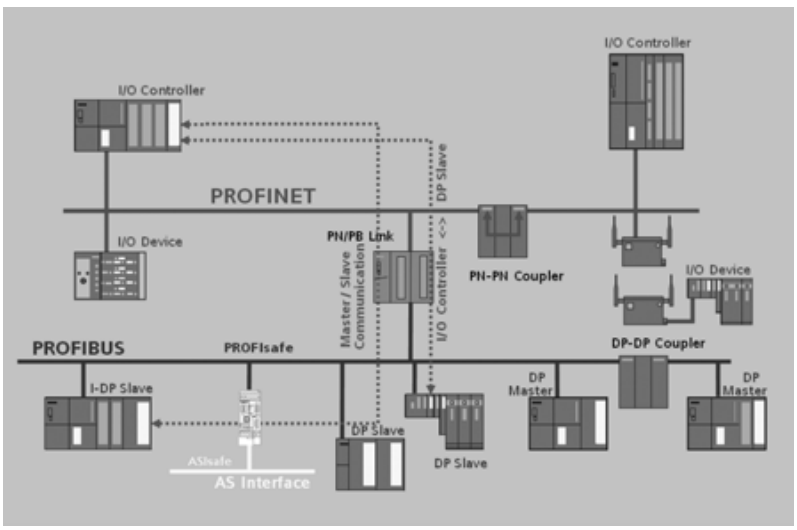


Fig. 9.7 Integration of existing Profibus plant components

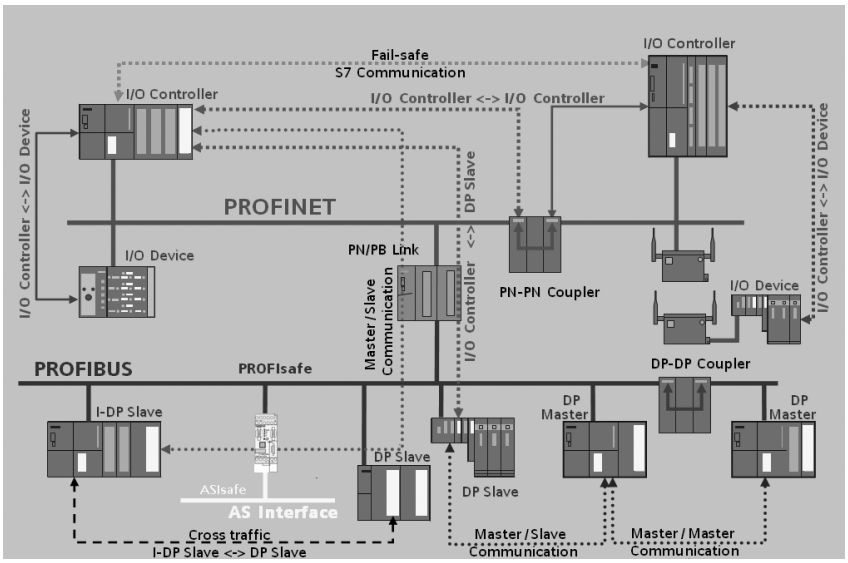


Fig. 9.8 Complete communication paths

Fig. 9.8 provides an overview of the communication possibilities and services.

9.7 Profisafe in Practice

The dangers identified during the risk analysis are monitored and mastered by the safety functions already mentioned. The fail-safe distributed I/O required for this is planned as usual using the hardware configuration. The safety functions themselves are implemented through programming of the PLC. The major advantage of Simatic Safety Integrated is seamless integration into the standard environment. The following section therefore only describes the special features of safety-related programming.

9.7.1 Programming of Safety Programs

The basic prerequisite for programming of a fail-safe Simatic is installation of the Distributed Safety option package. Following installation, new, predefined and certified fail-safe blocks are present in the library. These are objects which permit fast, problem-free programming. Users can also create their own blocks (Fig. 9.9).

In addition to blocks and hardware objects, Distributed Safety also provides a safe development environment. The graphic-based programming languages FBD and LAD are always supported. Fail-safe functions can only be linked to inputs and outputs with a corresponding configuration. It is not possible to simply use standard inputs for a fail-safe function. This protects users from programming errors. The safety program is integrated into the standard program using the cyclic interrupt OB 35.

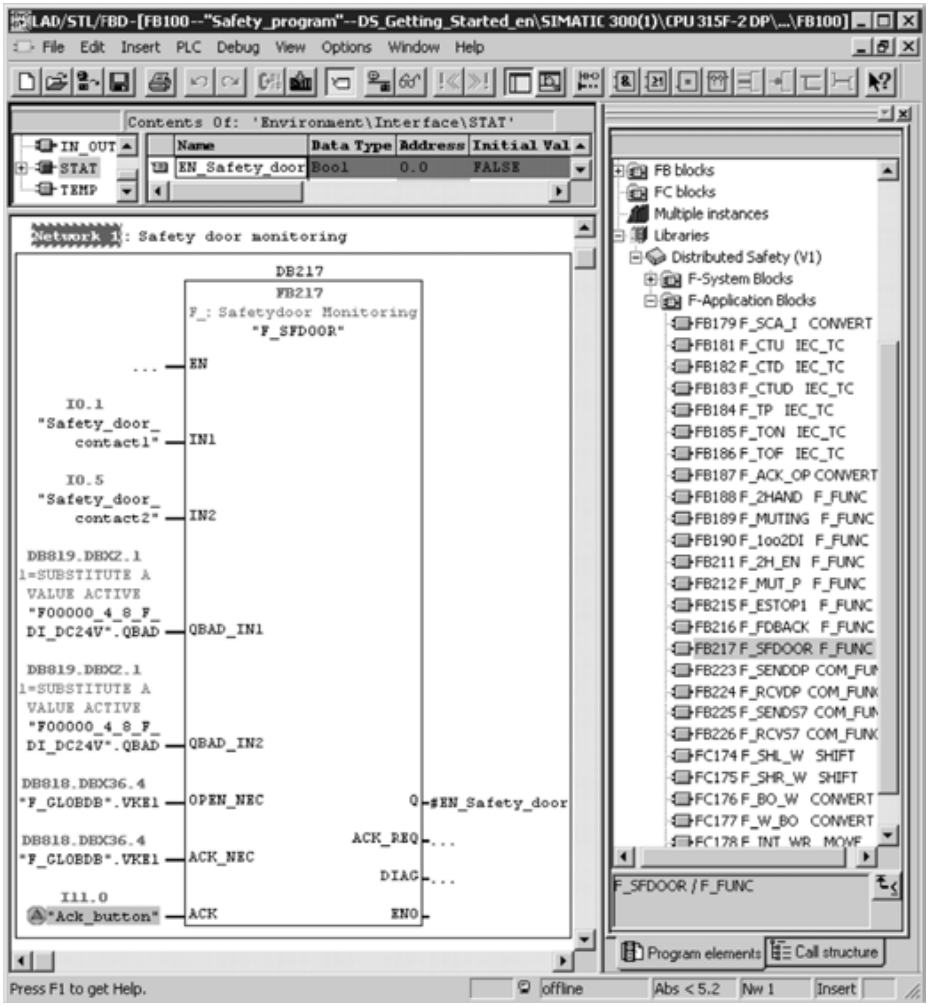


Fig. 9.9 Example: block library “Protective door”

9.7.2 Protection of the Safety-related Application

To achieve functional safety, it is necessary to monitor changes in the program in addition to correct execution of the safety function itself. Distributed Safety includes a number of measures for this purpose.

Protection by password

A password can be set in the properties window of the CPU in order to protect the safety program against unauthorized access (Fig. 9.10).

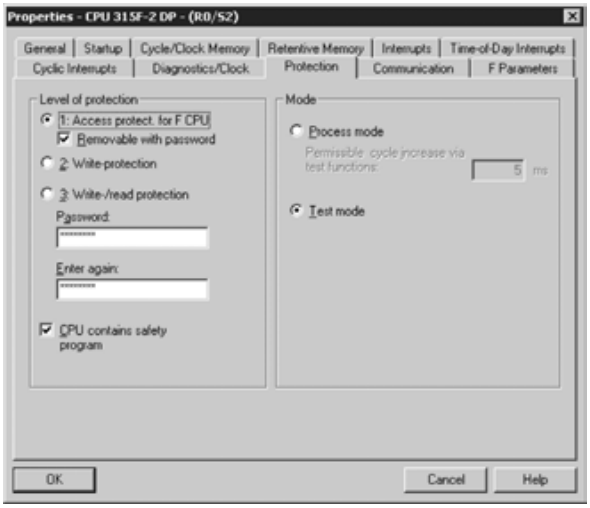


Fig. 9.10
Password protection for the CPU

Logbook function

The logbook function records which users have made changes to the safety program, and when. This (automatic) recording function is particularly advantageous in larger plants with a large number of maintenance personnel. In the event of an accident, sequences can then be exactly reconstructed.

Signature

Machine constructors are obliged to provide the correct safety functions for a machine. This is already specified by the required CE conformity. It is frequently the case that machine owners additionally wish to carry out their own optimization during operation. Distributed Safety generates a unique signature for the entire safety program.

A consistency check of the fail-safe (F) blocks relevant to the sequence is carried out when generating the safety program, i.e. the program is checked for errors. Any error messages are output in an error window. The additionally required F system blocks are generated automatically following the successful consistency check and supplemented in order to generate an executable safety program.

The total signature of all F-blocks with F-attribute of the block container agrees with the total signature of the safety program (as emphasized in Fig. 9.11), i.e. a consistent safety program exists which is available for verification.

9.7.3 Integration of Sensors

Corresponding SILs (Safety Integrity Levels) or categories must be used for the linking of sensors and actuators depending on the results of the danger analysis. The achievable category depends on the safety parameters of the sensor/actuator (proof test interval, MTBF, fault probability etc.) and their linking to the fail-safe

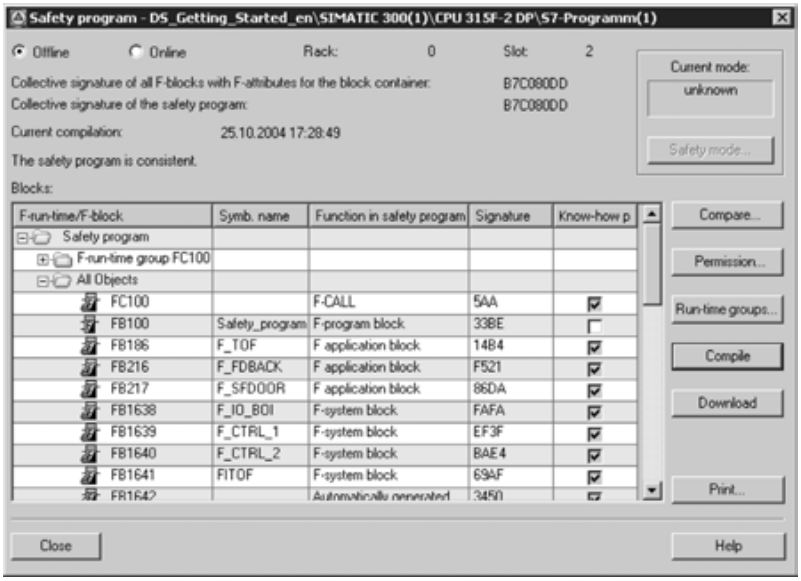


Fig. 9.11 Signatures of the F-blocks and total signature

modules. When linking electronic sensors, it must be ensured that an activated short-circuit test does not result in sensor interference.

Connection of these sensors to the distributed I/O depends on this. Fig. 9.12 shows how the sensors are connected.

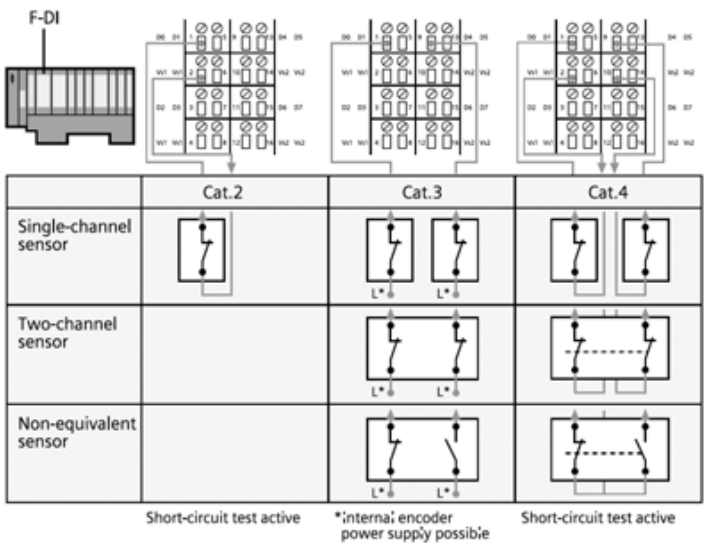


Fig. 9.12 Linking of safety-related sensors to ET200S with 4/8 F-DI

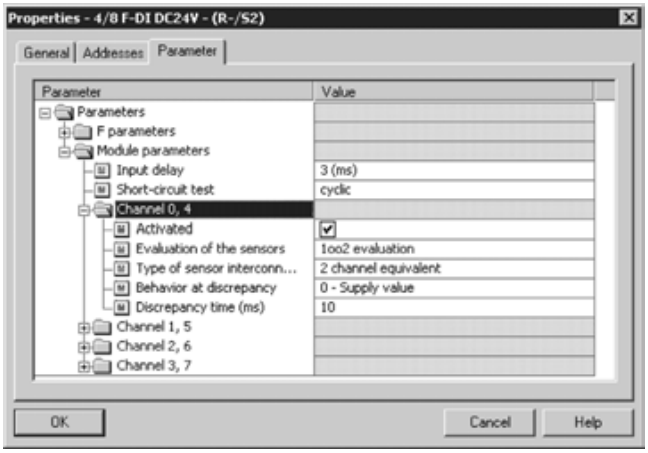


Fig. 9.13 Parameterization of 4/8 F-DI

In addition to the sensor connection, the type of connection must also be saved in the configuration. The corresponding values are set for this by means of the hardware configuration through parameterization of the ET200S module (Fig. 9.13).

These parameter settings are downloaded to the distributed module, and allow correct and local fault monitoring for the connected sensor.

As the result of the distributed fault monitoring, all further steps for programming are omitted. For example, the discrepancy time of an emergency stop with SIL3/Cat. 4 is measured directly by the distributed module, and the signal is declared to be valid by the module. Complex programming of this source of a fault can be omitted in the user program since the signal appears conveniently as a simple signal. The workload on users is thus significantly reduced.

PROFIsafe address

Each fail-safe module has its own PROFIsafe address in addition to the Profinet address. Before fail-safe modules can be installed, the PROFIsafe address must be set on each F-module. The PROFIsafe addresses (F_source_address, F_destination_address) are automatically assigned and displayed by Step 7 during configuration of the fail-safe module. The F_destination_address is represented in binary format in HW-Config in the object properties of the fail-safe module, in the parameter “DIL switch setting”. A 10-pole DIL switch on the module itself is used to set these addresses. A discrepancy between the set address and the address generated automatically in HW-Config results in communication errors.

9.7.4 Verification Support

According to the machine directive, documentation of machine safety is absolutely essential. Distributed Safety provides support by automatically generating the required documents (Fig. 9.14).

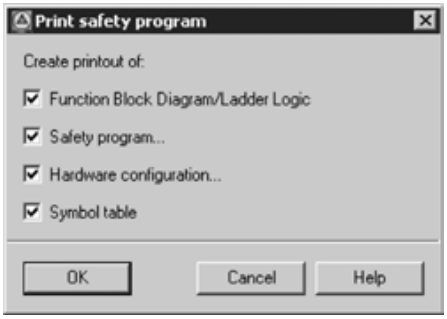


Fig. 9.14
Selection dialog for the documents required by the machine directive

A unique signature is present in the footer of each document (Fig. 9.15). This guarantees unambiguous documentation of the safety-related part of the controller. Subsequent changes always result in a change to the signature, and are therefore easy to prove in the event of an accident.

Fig. 9.15 Unique signature in the footer

Glossary

AC	Alternating Current
AH	Authentication Header
AES	Advanced Encryption Standard for WLAN
ARP	Address Resolution Protocol
AS-i	Actor Sensor Interface
BFOC	Bayonet Fiber Optic Connector
CAT	Cable categories
CBA	Component Based Automation
CP	Communication Processor
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DC	Direct Current
DCP	Discovery and Configuration Protocol
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DP	Distributed I/O – Profibus
DTL	Diode Transistor Logic
EHB	Monorail overhead conveyor
EMC	Electromagnetic Compatibility
ERTEC	Enhanced Real-Time Ethernet Controller
ESM	Electrical Switch Module
ESP	Encapsulation Security Payload
FBD	Function Block Diagram
FC	FastConnect
FDX	Full Duplex
FO	Fiber Optics
FTP	File Transfer Protocol
GNU	Abbreviation for “GNU is not Unix”.
GPL	General Public License: GNU GPL is a license issued by the Free Software Foundation for licensing free software.
GSD	Device master data – configuration data
HDX	Half Duplex
HMAC	Message Authentification Code
HMI	Human Machine Interface

HTTP	Hyper Text Transmission Protocol
HW	Hardware
IANA	Internet Assigned Numbers Authority – administers the address area
ICMP	Internet Control Message Protocol – ping
IGMP	Internet Group Management Protocol
IE	Industrial Ethernet
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IO	Input/Output
IP	Internet Protocol
IPxy	International Protection
IPC	Industrial PC (Personal Computer)
iPCF	Industrial Point Coordination Function
IPSec	IP Security
IRT	Isochronous Real-Time
ISAKMP	Internet Security Association and Key Management Protocol
ITU	International Telecommunications Union
IWLAN	Industrial Wireless Local Area Network
LAD	Ladder diagram – graphics-oriented programming language
LAN	Local Area Network
LD	Long Distance
LLDP	Low Level Discovery Protocol: neighbor recognition
MAC	Media Access Control
NCM	Configuration software for configuration and diagnostics of Simatic modules.
NIC	Network Interface Card
NTP	Network Time Protocol
OLE	Object Linking and Embedding
OP	Operator Panel
OPC	OLE for Process Control
OSM	Optical Switch Module
PB	PROFIBUS
PC	Personal Computer
PCF	Plastic Cladding Silica Fiber
PG	Programming device
PLC	Programmable Logic Controller
PN	PROFINET
PNO	PROFIBUS International
PoE	Power over Ethernet

POF	Plastic Optical Fiber
PPTP	Point-to-Point-Tunneling Protocol
PSK	Pre Shared Keying
PST	Primary Setup Tool
RARP	Reverse Address Resolution Protocol
RC4	Rivest Cipher
RJ	Registered Jack
RM	Redundancy Manager
RR	Rapid Roaming
RT	Real-Time
RTL	Resistance Transistor Logic
SA	Security Associations
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer; System State List
STL	Statement List
STP	Spanning Tree Protocol
SW	Software
SZL	High-noise-immunity and surge-proof logic
TCP	Transmission Control Protocol
TIA	Totally Integrated Automation
TP	Twisted Pair
TTL	Transistor-Transistor Logic
UDP	User Datagram Protocol
VPN	Virtual Private Network
WG	Working Group
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

References

Chapter 1 "From Contactor to Open Standard"
[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]

Chapter 2 "Ethernet – Fundamentals and Protocols"
[4], [11], [12], [13], [14], [15]

Chapter 3 "Real-time Communication"
[16], [17], [18], [19], [20], [21], [22], [23], [24]

Chapter 4 "Profinet IO – Distributed I/O"
[16], [17], [18], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44]

Chapter 5 "Profinet CBA – Distributed Automation"
[17], [18], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60]

Chapter 6 "Profinet User Program Interfaces with Simatic S7"
[16], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73]

Chapter 7 "Profinet Devices and Networking"
[7], [10], [13], [14], [15], [46], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110]

Chapter 8 "Profinet Security"
[15], [94], [98], [112]

Chapter 9 "Safety Technology and Profinet"
[114], [115], [116]

"Glossary"
[7], [10], [50], [117]

[1] Deppe, Manfred: Die Erfolgsgeschichte der SPS, Computer & AUTOMATION Control Guide; 2003

[2] Hahn, Rolf: SIMATIC, Erfolg mit System Vom Transistor zur Totally Integrated Automation, PUBLICIS MCD; Siemens AG; 1. Auflage 04/2001

[3] Siemens Archiv: http://w4.siemens.de/archiv/de

[4] SIMATIC NET – Industrial Ethernet; White Paper, Siemens AG, Bereich A&D; 1999

[5] Metcalf, Robert: Ethernet; 1976

[6] Popp, M.; Weber, K.: Der Schnelleinstieg in PROFINET, PROFIBUS Nutzerorganisation e. V.; 11/2004

[7] Siemens Katalog IK PI 2005

[8] www.siemens-industry.co.uk

[9] www.ethermanage.com

[10] Systemhandbuch SIMATIC, PROFINET Systembeschreibung, Siemens AG, Bereich A&D, 04/2005

[11] Handbuch SIMATIC NET – Kommunikation mit SIMATIC, Siemens AG, Bereich A&D; 1999

[12] Handbuch SIMATIC – Hardware konfigurieren und Verbindungen projektieren mit STEP 7 V5.2, Siemens AG, Bereich A&D; 2003

[13] Handbuch SIMATIC NET – Twisted Pair- und Fiber Optic Netze, Siemens AG, Bereich A&D; 2001

[14] Kurzbeschreibung SIMATIC NET – Netzlösungen für Industrial Ethernet nach IEEE 802.3/802.3u, Siemens AG, Bereich A&D; 2001

[15] Metter, M.; Bucher, R.: IT in der Industrieautomatisierung, Publicis; 2003

[16] Popp, M.: Das Profinet IO-Buch, Hüthig Verlag, 2005

[17] Specification Profinet, Application Layer services for decentralized periphery and distributed automation, V2.1, PROFIBUS Nutzer Organisation e.V.; 06/2006

[18] Specification Profinet, Application Layer protocol for decentralized periphery and distributed automation, V2.1, PROFIBUS Nutzer Organisation e.V.; 06/2006

[19] Weibel, H.: Uhren mit IEEE 1588 synchronisieren, Bullet in Electrosuisse Verband für Elektro-, Energie- und Informationstechnik, SEV/AES 17/04

[20] Siemens Handbuch, ERTEC 400 Enhanced Real-Time Ethernet Controller, V1.1.0; Siemens AG Bereich A&D, 04/2006

[21] Siemens Handbuch, ERTEC 200 Enhanced Real-Time Ethernet Controller, V1.0.0; Siemens AG, Bereich A&D; 04/2006

[22] Metter, M.; Bucher, R.: Industrial Ethernet in der Automatisierungstechnik, 2. Auflage, Publicis Corporate Publishing, Erlangen, 06/2007

[23] Institute of Electrical and Electronics Engineers, Inc. (IEEE), http://standards.ieee.org/

[24] Anwenderbeschreibung, Development Kit – ERTEC 400 PN IO V2.0.0; Siemens AG, Bereich A&D; 04/2006

[25] STEP 7 V5.4 Onlinehilfe; Siemens AG, Bereich A&D

[26] Systemhandbuch Simatic, Profinet Systembeschreibung; Siemens AG, Bereich A&D; 10/2006

[27] Programmierhandbuch Simatic, Von Profibus DP nach Profinet IO; Siemens AG, Bereich A&D; 10/2006

[28] Wikipedia, Die freie Enzyklopädie, www.wikipedia.de

[29] Guideline Profinet, Fieldbus Integration into Profinet IO , V1.0, PROFIBUS Nutzer Organisation e.V.; 09/2006

[30] Systemhandbuch, Kommunikation mit SIMATIC; Siemens AG, Bereich A&D; 09/2006

[31] Gerätehandbuch, Automatisierungssystem S7-400 CPU-Daten; Siemens AG, Bereich A&D; 05/2007

[32] SIMATIC Gerätehandbuch; S7-300 CPU 31xC und CPU 31x, Technische Daten; Siemens AG, Bereich A&D; 12/2006

[33] SIMATIC Betriebsanleitung; S7-300 CPU 31xC und CPU 31x: Aufbauen; Siemens AG, Bereich A&D; 12/2006

[34] SIMATIC Gerätehandbuch, Dezentrales Peripheriesystem ET 200S Interfacemodul IM 153-3 PN; Siemens AG, Bereich A&D; 04/2007

[35] SIMATIC Gerätehandbuch, Dezentrales Peripheriesystem ET 200S Interfacemodul IM 153-3 PN FO; Siemens AG, Bereich A&D; 04/2007

[36] SIMATIC Gerätehandbuch, Dezentrales Peripheriesystem ET 200S Interfacemodul IM 153-3 PN HIGH FEATURE; Siemens AG, Bereich A&D; 04/2007

[37] SIMATIC Net S7-CPs für Industrial Ethernet Handbuch Teil B4A CP 443-1 Advanced; Siemens AG, Bereich A&D; 01/2007

[38] SIMATIC Net S7-CPs für Industrial Ethernet Handbuch Teil B3L CP 343-1 Lean; Siemens AG, Bereich A&D; 03/2007

[39] SIMATIC Net S7-CPs für Industrial Ethernet Handbuch Teil B3S CP 343-1; Siemens AG, Bereich A&D; 01/2007

[40] SIMATIC Net S7-CPs für Industrial Ethernet Handbuch Teil B3A CP 343-1 Advanced; Siemens AG, Bereich A&D, 02/2006

[41] SIMATIC Net S7-CPs für Industrial Ethernet Handbuch, Teil BL1 Netzübergang IE/PB Link PN IO; Siemens AG, Bereich A&D; 05/2005

[42] SIMATIC Net S7-CPs für Industrial Ethernet Handbuch, Teil BL2 Netzübergang IWLAN/PB Link PN IO; Siemens AG, Bereich A&D; 11/2006

[43] SIMATIC Net Handbuch, IE/AS-Interface Link PN IO; Siemens AG, Bereich A&D; 08/2006

[44] SIMATIC Montage- und Bedienhandbuch, Buskopplungen PN/PN Coupler; Siemens AG, Bereich A&D; 08/2006

[45] Lange, R.; Otto, H-P.: Gemeinsame Sprache für verteilte Automatisierungsgeräte, Elektronik Fachzeitschrift für industrielle Anwender und Entwickler; 27.11.2001

[46] Profinet Architecture Description and Specification Version V2.01, PROFIBUS Nutzer Organisation e.V.; 08/2003

[47] DIN EN 61499-1, Funktionsbausteine für industrielle Leitsysteme – Teil 1: Architektur (IEC 61499-1:2005); Deutsche Fassung EN 61499-1:2005; 06/2006

[48] Guideline Profinet, Overview and Guidance for Profinet specifications, V2.1, PROFIBUS Nutzer Organisation e.V.; 06/2006

[49] Eddon, Guy and Henry: Understanding the DCOM Wire Protocol by Analyzing Network Data Packets, Microsoft System Journal, 03/1998

[50] Wikipedia Die freie Enzyklopädie, www.wikipedia.de

[51] Stal, M.: Microsoft DCOM, http://www.stal.de/Downloads/DCOM/DCOM.html

[52] SIMATIC Projektierungshandbuch, Component based Automation – SIMATIC iMap STEP 7 AddOn – Profinet-Komponenten erstellen; Siemens AG Bereich A&D, 01/2006

[53] SIMATIC Projektierungshandbuch, Component based Automation – Anlagen projektieren mit SIMATIC iMap; Siemens AG, Bereich A&D; 01/2006

[54] SIMATIC Inbetriebnahmehandbuch, Component Based Automation – SIMATIC iMap Systeme in Betrieb nehmen; Siemens AG, Bereich A&D; 01/2006

[55] Hilfe zu Component Based Automation und SIMATIC iMap V3.0; Siemens AG, Bereich A&D

[56] SIMATIC iMap V3.0, Hilfe zu Meldungen; Siemens AG, Bereich A&D

[57] SIMATIC NET Gerätehandbuch, Netzübergang IE/PB Link (ab Firmware-Stand V1.3); Siemens AG, Bereich A&D; 05/2002

[58] SIMATIC Benutzerhandbuch, Windows Automation Center – WinAC Basis V4.0; Siemens AG, Bereich A&D; 10/2004

[59] SIMATIC Inbetriebnahmehandbuch, Windows Automation Center WinAC PN Option V4.1; Siemens AG, Bereich A&D; 08/2004

[60] Kurzbeschreibung, Profinet Komponenten-Editor; Siemens AG, Bereich A&D; 06/2006

[61] Weigmann, Josef; Kilian, Gerhard: Dezentralisieren mit PROFIBUS-DP/DP V1, Publicis Corporate Publishing, 3. Auflage 2002

[62] STEP 7 V5.4 Onlinehilfe; Siemens AG, Bereich A&D

[63] Systemhandbuch SIMATIC, Profinet Systembeschreibung; Siemens AG, Bereich A&D; 10/2006

[64] Handbuch SIMATIC Net, S7-CPs für Industrial Ethernet, Teil A, Projektieren und in Betrieb nehmen; Siemens AG Bereich A&D; 01/2007

[65] Referenzhandbuch SIMATIC, Systemsoftware für S7-300/400 System- und Standardfunktionen; Siemens AG, Bereich A&D; 03/2006

[66] Handbuch SIMATIC, Programmieren mit STEP 7; Siemens AG, Bereich A&D; 03/2006

[67] Programmierhandbuch Simatic, Von Profibus DP nach Profinet IO; Siemens AG, Bereich A&D; 10/2006

[68] Spezifikation Profinet, Profiles for Decentralized Periphery V2.1, Profibus Nutzer Organisation e. V.; 06/2006

[69] Guideline Profibus, Profile Guidelines 1: Identification & Maintenance Functions Version V1.1.1, Profibus Nutzer Organisation e. V.; 03/05

[70] Profile ID Table Version V1.0, Profibus Nutzer Organisation e. V.; 09/06

[71] Handbuch S7-CPs für Industrial Ethernet, Projektieren und in Betrieb nehmen, Teil A – Allgemeine Anwendung; Siemens AG, Bereich A&D, 07/2006

[72] Guideline Profibus and Profinet, Communication Function Blocks on Profibus DP and Profinet IO V2.0, Profibus International; 11/2005

[73] Simatic Manager, STEP7 V5.4 Onlinehilfe, Hilfe zu FCs/FBs für Simatic Net-CPs; Siemens AG, Bereich A&D

[74] Handbuch SIMATIC NET, S7-CPs für Industrial Ethernet, Netzübergang IE/PB Link PN IO, Siemens AG, Bereich A&D, 08/2004

[75] Gerätehandbuch SIMATIC NET; S7-CP für Industrial Ethernet, Siemens AG, Bereich A&D, 04/2002

[76] Gerätehandbuch SIMATIC; S7-300 CPU 31xC und CPU 31x, Technische Daten, Siemens AG, Bereich A&D, 08/2004

[77] Benutzerhandbuch SIMATIC, Windows Automation Center – WinAC Basis V4.0, Siemens AG, Bereich A&D; 10/2004

[78] Benutzerhandbuch SIMATIC, Windows Logic Controller (WinLC), Siemens AG, Bereich A&D, 04/2000

[79] Handbuch SIMATIC, Dezentrales Peripheriesystem ET 200S, Siemens AG, Bereich A&D, 07/2004

[80] Handbuch SIMATIC NET, S7-CPs für Industrial Ethernet, Projektieren und in Betrieb nehmen, Siemens AG, Bereich A&D, 01/2005

[81] Handbuch Siemens, ERTEC 400 Enhanced Real-Time Ethernet Controller, Siemens AG, Bereich A&D, 05/2005

[82] Betriebsanleitung SIMATIC NET – Industrial Ethernet Switches SCALANCE X-400, Siemens AG, Bereich A&D, 01/2005

[83] Projektierungshandbuch SIMATIC NET – Industrial Ethernet Switches SCALANCE X-400, Siemens AG, Bereich A&D, 01/2005

[84] Inbetriebnahmehandbuch SIMATIC NET – SCALANCE Industrial Ethernet SCALANCE X-100 und SCALANCE X-200 Produktlinie, Siemens AG, Bereich A&D, 07/2005

[85] Betriebsanleitung SIMATIC NET – SCALANCE W744-1PRO, SCALANCE W746-1PRO, SCALANCE W747-1RR; Siemens AG, Bereich A&D, 07/2005

[86] Handbuch SIMATIC NET – Systemhandbuch RCoax, Siemens AG, Bereich A&D, 03/2005

[87] Betriebsanleitung SIMATIC NET – CP 7515 , Siemens AG, Bereich A&D, 05/2004

[88] Broschüre SIMATIC NET – Industrial Wireless LAN – Grundlagen, Siemens AG, Bereich A&D; 2001

[89] Handbuch SIMATIC NET – Industrial Ethernet OSM/ESM Netzwerkmanagement, Siemens AG, Bereich A&D; 2002

[90] Kurzbeschreibung SIMATIC NET – IT-Lösungen für Industrielle Kommunikation, Siemens AG, Bereich A&D; 2001

[91] Broschüre Switching-Technologie für Industrial Ethernet für alle Fälle von SIMATIC NET, Siemens AG, Bereich A&D; 2003

[92] Broschüre SIMATIC NET – Mit Industrial Ethernet FastConnect in 2 Minuten anschlussfertig, Siemens AG, Bereich A&D; 2003

[93] SIMATIC NET – Netzwerkmanagement – White Paper, Siemens AG, Bereich A&D; 1999

[94] Betriebsanleitung SIMATIC NET – IO-Base Anwenderprogrammierschnittstelle, Siemens AG, Bereich A&D, 08/2005

[95] PROFInet Installationsrichtlinie, PROFIBUS Nutzer Organisation e.V.; 2004

[96] Handbuch SIMATIC NET – Twisted Pair- und Fiber Optic Netze, Siemens AG, Bereich A&D; 2001

[97] Montageanleitung SIMATIC NET – Montageanleitung für FastConnect RJ45 Plug 90, Siemens AG, Bereich A&D, 05/2004

[98] Montageanleitung SIMATIC NET – Montageanleitung für FC RJ45 Modular Outlet, Siemens AG, Bereich A&D; 12/2004

[99] Handbuch SIMATIC NET – S7-CPs für Industrial Ethernet Projektieren und in Betrieb nehmen Teil A – Allgemeine Anwendung, Siemens AG, Bereich A&D, 07/2005

[100] Gerätehandbuch SIMATIC NET – S7-CPs / Teil B1 Beschreibung CP 343-1/CP 343-1EX20, Siemens AG, Bereich A&D, 02/2003

[101] Gerätehandbuch SIMATIC NET – CP 343-1 für Industrial Ethernet Teil B3S, Siemens AG, Bereich A&D, 02/2005

[102] Gerätehandbuch SIMATIC NET – S7-CPs / Teil B2 Beschreibung CP 343-1 PN, Siemens AG, Bereich A&D, 02/2003

[103] Gerätehandbuch SIMATIC NET – S7-CPs / Teil B4 Beschreibung CP 443-1, Siemens AG, Bereich A&D, 02/2003

[104] Gerätehandbuch SIMATIC NET – CP 443-1 Advanced für Industrial Ethernet / Handbuch Teil B4A, Siemens AG, Bereich A&D, 07/2005

[105] Gerätehandbuch SIMATIC NET – CP 443-1 Advanced Teil B6, Siemens AG, Bereich A&D, 08/2004

[106] Gerätehandbuch SIMATIC NET – Installationsanleitung CP 1512 , Siemens AG, Bereich A&D; 12/2004

[107] Gerätehandbuch SIMATIC NET – Installationsanleitung CP 1612 , Siemens AG, Bereich A&D; 12/2004

[108] Handbuch SIMATIC NET – Einführung SOFTNET für Industrial Ethernet, Siemens AG, Bereich A&D; 12/2004

[109] Handbuch SIMATIC – Vision Sensor VS 130-2, Siemens AG, Bereich A&D

[110] Gerätehandbuch SIMATIC NET – Installationsanleitung CP 1616 , Siemens AG, Bereich A&D, 04/2005

[111] Gerätehandbuch SIMATIC NET – Installationsanleitung CP 7515 , Siemens AG, Bereich A&D, 04/2005

[112] Handbuch SIMATIC NET – Dezentrales Peripheriesystem ET 200, Siemens AG, Bereich A&D, 04/2005

[113] Montageanleitung SIMATIC NET – Montageanleitung für FC RJ45 Modular Outlet Insert 2FE FC RJ45 Modular Outlet Insert 1GE, Siemens AG, Bereich A&D; 12/2004

[114] Systemhandbuch Safety Integrated (Das Sicherheitsprogramm für die Industrien der Welt); Siemens AG, Bereich A&D; 2007

[115] Nachtrag zum Systemhandbuch Safety Integrated (Das Sicherheitsprogramm für die Industrien der Welt); Siemens AG, Bereich A&D; 2007

[116] S7 Distributed Safety Getting Started; Siemens AG, Bereich A&D; 2007

[117] http://www.computerbase.de

Index

S

T