

## SIMATIC NET




## Glossary - Specialist terms

## Reference Manual

## Legal information

### Warning notice system

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

 <b>DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.
 <b>WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.
 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
<b>NOTICE</b>
indicates that property damage can result if proper precautions are not taken.


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

### Qualified Personnel

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

### Proper use of Siemens products

Note the following:

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

### Trademarks

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

### Disclaimer of Liability

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

# Preface

## SIMATIC NET glossary

You will also find the current version of the SIMATIC NET glossary on the Internet at the following address:

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



# Table of contents

Preface ..... 3  
Glossary ..... 7



# Glossary

## **1000Base-LX**

IEEE 802.3z standard for data transmission of 1 Gbps on fiber-optic cable (single mode, 1300 nm wavelength)

## **1000Base-SX**

IEEE 802.3z standard for data transmission of 1 Gbps on fiber-optic cable (multimode, 850 nm wavelength)

## **1000Base-T**

IEEE 802.3ab standard for data transmission of 1 Gbps on twisted pair, 8-wire cables

## **1000Base-TX**

Standard for data transmission of 1 Gbps Ethernet on twisted pair cables

## **1000Base-X**

IEEE 802.3 standards family for Ethernet, comprising 1000Base-CX, 1000Base-LX and 1000Base-SX

## **100Base+C168TX**

Standard for data transmission of 100 Mbps Ethernet on twisted pair category 5 cables up to 100 m

## **100Base-FL**

IEEE 802.3 standard Fast Ethernet for data transmission of 100 Mbps on fiber-optic cable

## **100Base-FX**

IEEE 802.3u standard Fast Ethernet for data transmission of 100 Mbps on fiber-optic cable

## **100Base-T**

IEEE 802.3u standard Fast Ethernet for data transmission of 100 Mbps on 4-wire twisted pair cables

**100Base-TX**

IEEE 802.3u standard for data transmission of 100 Mbps Ethernet on twisted pair category 5 cables up to 100 m

**10Base2**

IEEE 802.3a standard for data transmission of 10 Mbps Ethernet on thin coaxial cables, segment length 185 meters

**10Base5**

IEEE 802.3 standard for data transmission of 10 Mbps Ethernet on coaxial cables (yellow cable), segment length 500 meters

**10BaseFL**

IEEE 802.3 standard for data transmission of 10 Mbps Ethernet on fiber-optic cables

**10BaseT**

IEEE 802.3i standard for data transmission of 10 Mbps Ethernet on 4-wire twisted pair cables

**2.5G**

→ 2G

**2G**

Mobile wireless standard of the second generation, for example GSM.

Occasionally the term 2.5G is also used. In this case, the expansions of GSM are meant (EDGE, GPRS).

**3DES**

Data Encryption Standard

Symmetrical encryption algorithm with block encryption and 56-bit key length. Replacement for → DES, predecessor of → AES. Unlike DES, the encryption algorithm is applied three times to each data block.

**3G**

Mobile wireless standard of the third generation, for example UMTS.

**4G**

Mobile wireless standard of the fourth generation (LTE)



**5-4-3 rule**

→ *Repeater rule*

**5G**

Mobile wireless standard of the fifth generation

**AAA**

Security concept for network nodes. It uses user authentication (Authentication), authorization (Authorization) and accounting (Accounting).

**Access Point**

AP

Node in a WLAN that also performs administrative functions in the network and, for example, provides clients with a connection to wired networks, to other clients in the same wireless cell or in other wireless cells.

**Access Point Name**

→ *APN*

**ACL**

Access Control List

List with MAC addresses of devices that have the right to log on in a wireless network.

Compare "IP ACL"

**Ad hoc network**

Wireless network between individual devices in which devices without access point communicate directly with each other.

**Address Resolution Protocol**

→ *ARP*

**Advanced CP**

CP modules with E-mail, FTP or Web functions and PROFINET CBA

**Advanced Encryption Standard**

→ *AES*

## AES

Advanced Encryption Standard

Symmetrical encryption algorithm with block encryption and variable key length. Successor of the Data Encryption Standard (DES).

## Aggressive Mode

→ *Identity Protection*

## Aging Time

The time after which a learned MAC address is discarded if the device has not received frames with this MAC sender address during this time.

## AH

Authentication Header

Protocol in the IPSec protocol suite that provides the authenticity and integrity of IP packets. Unlike with Encapsulating Security Payload, the user data is not encrypted.

## Alarm

Context: OPC Alarms & Events

An event triggered by a condition that no longer represents the normal state.

## ALI

Application Layer Interface

Interface to the application layer; it maps the interface of an application process to the standardized interface of the application layer and vice versa.

## A-MPDU

Aggregated MAC Protocol Data Unit

Larger data packet resulting from frame aggregation.

## Antenna diversity

Method with which wireless receivers are equipped with two antennas so that they can select the better signal from two received signals.

**Antenna gain**

Improvement of the efficiency of an antenna through design and arrangement not depending on direction. The value is determined by comparing the maximum radiated power of the antenna with that of an isotropic radiator. Specified in dB.

**Anti-spoofing**

→ *Spoofing*

**AP**

→ *Access Point*

**APDU**

Application Protocol Data Unit  
Data unit of a PDU

**API**

Application Programming Interface  
Programming interface

**API**

Application Process Identifier  
Term from the PROFINET IO standard; this value specifies the process (application) processing the IO data. The IEC assigns profiles to certain APIs; refer to IEC 61158. The standard API has the value 0.

**APN**

Access Point Name  
DNS host name of the access point of a network to an external network.  
For Telecontrol: Name of the access point from the mobile wireless network to the Internet or private intranet. Depending on the type of network connected, this is a public or private APN.

**Application Layer Interface**

→ *ALI*

## Application relation

Logical connection between two applications (for example with OPC) or devices (for example with PROFINET) that communicate with each other. An application relation can be based on several communication relations (connections).

## AR (Application Relation)

→ *Application relation*

## ARD

Automatic Redundancy Detection

Method for automatic detection of redundancy roles for Siemens devices in ring topologies

## ARP

Address Resolution Protocol

Protocol that determines physical addresses of the network access layer from network addresses of the Internet layer. ARP is mainly used to determine MAC addresses from IP addresses. The assignment of MAC addresses to IP addresses is entered in ARP tables.

## AS-Interface

Aktuator Sensor Interface

Fieldbus system for networking basic sensors and actuators. Serial transmission of small amounts of information.

## Asymmetrical encryption

Encryption algorithm with key pair consisting of private and public key.

Messages are sent encrypted by the sender with the public key and decrypted by the receiver with the private key.

For communication with digital signatures, the sender encrypts with the private key and the receiver decrypts with the public key.

## Asynchronous Transfer Mode

→ *ATM*

## ATM

Asynchronous Transfer Mode

Technology in which the data traffic is handled in small packets with a fixed length (53 bytes) and using asynchronous time multiplexing.

**AUI**

Attachment Unit Interface

Interface of the Ethernet bus system between node and bus coupler

**Authorisation**

Assignment of permissions in communications networks to increase data security

**Auto Edge Port**

This function helps a port in detecting automatically whether or not an end device is connected. This option is useful in conjunction with passive listening because reconfiguration is faster if the main link fails.

**Auto fall back**

Step-by-step reduction of the transmission speed when there are bad reception conditions to retain the connection

**Auto Polarity Exchange**

Method that automatically detects at the connecting cable of an electric OSM/ESM port when the receiving cable pair is connected incorrectly (RD+ and RD- swapped). The OSM/ESM automatically reverses the polarity in this case.

**Autocrossover**

Method specified in IEEE 802.3 for automatic assignment of the send and receive contacts of an Ethernet port depending on the cable with which the communications partner is connected. This means that it does not matter whether the port is connected using a patch cable or crossover cable.

**Autonegotiation**

Method specified in IEEE 802.3 for detection and automatic negotiation of the transmission speed and transmission mode (half/full duplex). The mode with the highest possible speed is set. The method is supported for Ethernet nodes connected via twisted pair cable.

**Autosensing**

Method specified in IEEE 802.3 with which an Ethernet node automatically detects the transmission speed of a signal and where possible sets itself to this speed. The method is supported for Ethernet nodes connected via twisted pair cable.

**AWG**

American Wire Gauge

Value that describes the cross-sectional area of a wire. If an additional number is specified following this value, this indicates whether it is a solid or stranded wire.

Examples:

22 AWG = wire cross-sectional area of 0.33 to 0.38 mm<sup>2</sup>

22/1 AWG = solid wire

22/7 AWG = 7-strand wire

## **Backbone**

Network at the highest level in hierarchically structured plant networking.

## **Backpressure**

Flow control for ports operating in half duplex mode. With this flow control, the device lowers the number of frames received at a port if there is overload due to additionally generated collisions.

## **BDC**

Backup Domain Controller

Substitute server of a domain controller in redundant configuration. The domain controller stores the user and logon information and is used for authentication and authorization of users in a domain.

## **BFOC**

Bayonett Fiber Optic Connector

Plug-in connector for fiber-optic cables with bayonet lock. Also known as an ST connector. Suitable for single mode and multimode fibers.

## **Bonding network (BN)**

Interconnected conductive constructions that form an "electromagnetic shield" for electronics systems and personnel in the frequency range of DC current up to the lower high frequency range. The phrase "electromagnetic shield" means any structure for diverting, blocking or attenuating electromagnetic energy.

## **BOOTP**

Protocol for automatic assignment of IP addresses. The IP addresses are provided by a BOOTP server. Predecessor of DHCP.

## **BPDU**

Bridge Protocol Data Unit

Configuration frames of the Spanning Tree protocol, subdivided into Configuration BPDU and the Topology Change Notification BPDU (TCN). Devices exchange Configuration BPDUs to determine the root bridge and specify the network topology. TC BPDUs provide information about topology changes.

**BPSK**

Binary phase shift keying

Modulation technique in wireless LAN. This modulation method known as phase shift keying takes into account the phase position of the modulated signal at the time the signal is sampled. The aim of the method is the simple recovery of the digital signal from the wireless transmission.

**BQTF**

Bluetooth Qualification Test Facility

Facility for monitoring the interoperability of the products of different vendors.

**BRI**

Basic Rate Interface

Standard network connection to ISDN.

**Bridge**

Network component that interconnects network segments. This makes sure that local data traffic remains local. Data packets that are intended for a node in another segment are forwarded by the bridge. Errors in one network segment are restricted to the relevant network segment.

**Broadcast**

→ *IP broadcast*

**Broadcast address**

IP or MAC address in the network to which frames are sent that are intended to be read by all nodes.

**BSS**

Basic Service Set

Wireless LAN wireless network with access to the infrastructure via a single access point

**BSSID**

Basic Service Set Identification  
Indication of the MAC address of the access point

**Burst**

Briefly increased network load due to a shower of data or alarm flood

**Bus connector**

Physical connection between the node and bus cable

**Bus parameter**

Bus parameters control transfer characteristics on the bus. Each PROFIBUS node must use bus parameters that match the bus parameters of other nodes.

**Bus segment**

Part of a subnet. Subnets can be formed from bus segments using segment connectivity devices such as repeaters and bridges. Segments are transparent for addressing.

**Bus system**

All stations physically connected to a bus cable form a bus system.

**Byonet Fiber Optic Connector**

→ *BFOC*

**CA**

Certification Authority  
Certification authority that creates digital certificates (CA certificates) and certifies the origin of the certificates with digital signatures.

**CA certificate**

Root certificate that identifies a Certification Authority and is used for checking certificates that were issued by the certification authority.

**Cache**

Context: OPC Data Access  
Interim buffer for all variables of an OPC server that are referenced over OPC items. The cache is global for all users. This means that if more than one user references the same variable,



this is stored only once in the cache. Read operations (read or refresh) can read the data from the server cache with the OPC\_DS\_CACHE option.

**Canonical data type**

Original data type of a variable as represented internally and returned by the OPC server.

**Category x components**

Depending on their transmission properties, cabling components are divided into various categories. Various physical limit values have been defined for the individual categories, for example, maximum signal attenuation at a defined transmission frequency.

- Category 3: Data transmission up to 16 MHz
- Category 4: Data transmission up to 20 MHz
- Category 5: Data transmission up to 100 MHz
- Category 6: Data transmission up to 200 MHz (draft standard)

**CBA**

→ *PROFINET CBA*

**CCK**

Complementary code keying

Modulation technique in wireless LAN (802.11b)

**CDMA**

Code Division Multiplex Access

Multiplex method that allows the simultaneous transfer of different data streams in a common frequency range.

**Cell Signal Quality**

→ *CSQ*

**Central Processing Unit**

→ *CPU*

**Certification Authority**

→ *CA*

## CFP

Contention free Period

Time during which access is managed by the access point (to support time-critical services).

## Channel bonding

Grouping together of neighboring channels to increase the transmission speed and data throughput.

## Channel Bonding

→ *Channel bonding*

## CHAP

Challenge Handshake Authentication Protocol

Authentication protocol used within the framework of the Point-to-Point Protocol (PPP). PPP is located at the data link layer in the Internet protocol family.

## Chart view

Display of the chart hierarchy in SIMATIC IMAP with all function instances and charts.

Context: PROFINET CBA

## CIDR

Classless Inter-Domain Routing

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

Example: IP address 192.168.0.0 with network mask 255.255.255.0

The network part of the address covers 3 x 8 bits in binary representation; in other words 24 bits. This results in the CIDR notation 192.168.0.0/24.

The host part covers 1 x 8 bits in binary notation. This results in an address range from  $2^8$ , in other words 256 possible addresses.

## CLEAR mode

Mode of the DP master; inputs are read cyclically, outputs remain set to 0.

## CLI

Command Line Interface

Command input area for controlling a computer program with a command interpreter. Commands are entered as text using the keyboard and are supplemented by control characters.

## Client

→ *Client-server model*

## Client-server model

Concept for communication services based on a relationship between a client and a server. The server processes a job and sends the result back to the client.

A server can often service several clients. Example: OPC

A client can often query multiple servers. Example: NTP

## CM

Communications module

Module for communications tasks that is used in an automation system as an interface expansion of the CPU. Same interface types of a CPU and a CM are functionally identical.

## CMG

Communications general purpose cable

Cable type of the NEC

UL approval of a copper cable for use in buildings complying with Section 800-53(d) of the NEC

## CMIP

Common Management Information Protocol

Network management protocol of the ITU-T Recommendation X.711 according to ISO/IEC 9596-1.

## CMIS

Common Management Information Service

Standard for connection of Content Management systems.

## CMP

Communications plenum cable

Cable type of the NEC

UL approval of a copper cable for unprotected plenum use without additional protection.

## **CMR**

Communications riser cable  
Cable type of the NEC  
UL approval of a copper cable for use as riser cable in buildings

## **CMX**

Communications cable, limited purpose  
Cable type of the NEC  
UL approval of a copper cable for use in buildings where the wiring or cables are enclosed in a cable duct or in a nonflammable sheath.

## **Collision**

A collision results when end devices attempt to transmit at the same time. The collision is resolved according to a method defined in IEEE 802.3.

## **Collision domain**

To ensure that the CSMA/CD protocol functions correctly, the propagation time of a data packet from one node to another is restricted. This propagation time results in a spatially limited span for the network depending on the transmission speed known as the collision domain. In 10 Mbps Ethernet, this is 4520 m and in Fast Ethernet, it is 412 m. Several collision domains can be interconnected via bridges/switches.

## **COM**

Configuration Management  
Configuration software for communications processors

## **COM interface**

→ *COM port*

## **COM library**

Part of the operating system (runtime environment) that manages information on the COM objects known in the system in a register, for example OPC servers.

COM = Component Object Model

## **COM port**

A COM port (communication port) denotes a serial interface (RS-232) on a Windows PC. Application programs use COM ports for transferring data to various devices, for example modems, PCs etc.

**COM/DCOM**

Component Object Model/Distributed Component Object Model

Object model which allows an object to make its functionality available to other components. DCOM is an expansion of COM for communication via a network.

**COML**

Configuration Management lokal

Configuration software for SIMATIC NET communications processors

**Command Line Interface**

→ *CLI*

**Command line interpreter**

A computer program that reads in, evaluates and executes a command line and displays the result to the user.

**Common bonding network (CBN)**

The CBN is the primary way to create effective bonding and earthing inside a telecommunication building. The CBN is the set of metallic components that are intentionally or unintentionally interconnected to form the principal BN in a building. These include structural steel or reinforcing rods, metal plumbing, conduits for AC cables, PE conductors, cable racks, and equipotential bonding conductors. The CBN always has a mesh topology and is connected to the earthing network.

**Common Management Information Service**

→ *CMIS*

**Communications module**

→ *CM*

**Communications processor**

→ *CP*

**Component Object Model/Distributed Component Object Model**

→ *COM/DCOM*

### **Configuration data**

Parameters that are generated with a configuring tool (such as STEP 7) and downloaded to modules where they specify the method of operation and function of the module.

### **Configuration Management**

→ *COM*

### **Configuration Management lokal**

→ *COML*

### **Continuation line**

Graphic display of the endpoint of an interconnection. Interconnections are represented in SIMATIC iMap by lines or continuation lines.

Context: PROFINET CBA

### **Contol job**

Control command for DP mode.

Examples: CLEAR, SYNC, FREEZE, UNFREEZE, ACT, DEACT

### **CoS**

Class of Service

Priority with which a VLAN frame is processed. See IEEE 802.1Q.

### **Coupling loss**

Loss where an electromagnetic wave leaves a coaxial cable and enters the surrounding space

### **CP**

Contention Period

Time during which access is controlled according to CSMA/CA (to support time-critical services).

### **CP**

Communications Processor

Module for expanded communications tasks that provides the CPU with additional interface types or communications options.

**C-PLUG**

Exchangeable storage medium for storing the configuration data of a device. The configuration data is available on the C-PLUG when replacing the basic device and the device must not be loaded again.

**CPU**

Central Processing Unit  
Main processor of a SIMATIC controller

**CRC**

Cyclic Redundancy Check  
Checksum used in transmission protocols to detect errors in frames.

**CSD**

Circuit Switched Data  
Service for transferring data in the GSM network. Possible are dial-in connections of GSM modems to GSM/ISDN/analog modems and other devices with modems. The transmission speed is 14400 bps full duplex for non-secure transmission and 9600 bps for secure transmission. See also "HSCSD".

**CSMA/CA**

Carrier Sense Multiple Access with Collision Avoidance  
Access mechanism with collision avoidance in Ethernet networks.

**CSMA/CD**

Carrier Sense Multiple Access with Collision Detection  
Access method of a wired Ethernet network complying with IEEE 802.3

**CSQ**

Cell Signal Quality, parameter for the received signal strength (signal quality) in mobile wireless networks.

The CSQ values correspond to the received field strength RSSI [dBm] according to the following formula:

$$\text{dBm} = -113 + \text{CSQ} * 2$$

- CSQ = 0..1 (< -110 dBm): No connection to the network
- CSQ = 2..11 (-109 ... -90 dBm): Poor quality

- CSQ = 12..19 (-89 ... -74 dBm): Medium quality
- CSQ = 20..31 (-73 ... -51 dBm): Good quality

See also "RSSI".

## CTRL

Data field containing control information for the LLC protocol.

## CTS

→ *RTS*

## Cut Through

Technique with which a frame is forwarded as soon as the destination address is recognized. The delay is therefore not dependent on the frame length. If there are problems in a network, however, defective frames are also forwarded.

## Cyclic Redundancy Check

→ *CRC*

## Data Encryption Standard

→ *DES*

## Data frame

Data unit transferred between communication partners.

Meaning in the SIMATIC NET documentation:

- Data unit transferred on the application layer (OSI layer 7)
- General term for a transferred data unit regardless of the relevant OSI layer.

## Data point

Context: Telecontrol

Data points are used to identify signals in automation and control technology.

A data point is identified by its name. Typical attributes are address, data type and value.

Depending on the use of the data point, additional attributes such as time stamp, status, limit values, transmission parameters etc. can be assigned.

The data point address of a CP is the reference to an input/output address of the CPU (process value), to a memory (process value or calculation value) or to a variable of the CPU.



**Datagram**

UDP frame on the transport layer (OSI layer 4).

**dBi**

Decibel (isotropic)

Unit for antenna gain compared with an isotropic radiator

**DCF**

Distributed Coordination Function

Mechanism for the non-deterministic access control of several nodes in the WLAN with the help of CSMA/CA and a random wait time if the channel is occupied.

**DCP**

Discovery and basic Configuration Protocol

Protocol for discovery of address parameters of Ethernet components

**Decibel (isotropic)**

→ *dBi*

**DECT**

Digital Enhanced Cordless Telecommunications

European standard for wireless voice and data communications

**Default Gateway**

Forwards all frames not addressed to stations in the same LAN (subnet) and for which no specific gateway exists.

**Delay equivalent**

Signal delay of a network component in the signal path. The value of the signal delay is specified in meters instead of seconds. The value in meters corresponds to the distance that a signal could propagate within the time if the signal propagated through a cable rather than passing through the component.

**Demilitarized zone**

→ *DMZ*

## DES

Data Encryption Standard

Symmetrical encryption algorithm with block encryption and 56-bit key length. Predecessor of the standard → 3DES.

## Destination NAT

NAT method in which a destination IP address in the source network is replaced with a different destination IP address in the destination network.

## Device

In PROFINET CBA: Part of the PROFINET component that 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 components were created. It is displayed in the network view of SIMATIC iMap as an object with one or more bus attachments. See also: → PROFINET device → PROFIBUS device

Context: PROFINET CBA

## Device replacement without exchangeable medium/PG

PROFINET IO devices with this function are simple to replace: No exchangeable medium (for example Micro Memory Card) with stored device name necessary; the device name does not need to be assigned with the PG.

The replacement PROFINET IO device no longer receives the device name from the exchangeable medium or from the PG but from the PROFINET IO controller.

For identification, the PROFINET IO controller uses the configured topology and the neighborhood relations discovered by the PROFINET IO devices.

## DFS

Dynamic Frequency Selection

Dynamic frequency selection (channel change) in the 5 GHz band (802.11h)+C166

## DHCP

Dynamic Host Configuration Protocol

Protocol for automatic assignment of IP addresses even while the device is in operation. A DHCP server assigns the required parameters, such as IP address, subnet mask, default gateway, to the connected clients.

## DHCPv6

Dynamic Host Configuration Protocol v6

Procedure for assignment with or without status of IPv6 information to a client

**Diffie-Hellmann groups**

Selectable cryptographic algorithms in the Oakley key determination protocol

**Diffie-Hellmann key agreement**

Protocol for secure exchange of secret keys over an unsecure line.

**Digital signature**

Asymmetrical cryptography method that is used to ensure the authenticity of data. A digital signature is encrypted with the private key of the sender and decrypted with the associated public key of the receiver. To ensure data integrity, a hash value is formed prior to data encryption which is sent along with the original data. After the hash value has been formed by the receiver, the identity of the two values can be checked.

**Direct communication**

Context: Telecontrol

With direct communication, the S7 stations communicate directly with each other without the frames needing to be forwarded by a master station or station.

Compare "Inter-station communication"

**Dispersion**

Broadening and distortion of light pulses in fiber-optic cable due to signals arriving at different times. On multimode FO cable, the distortion of the output signal is greater than with single mode FO cables.

**Distributed I/O**

→ DP

**Diversity**

Strategy for increasing reliability in the event of failure of wireless connections by using several transmitters/receivers and taking the best signal for further use.

**DLF**

Destination Lookup Failure

This occurs when the IE switch processes a frame with a destination address that has not yet been learned. Such frames are normally forwarded over all ports.

**DMZ**

Demilitarized zone

Subnet with restricted access options that is used to disconnect trusted networks from untrusted networks such as the Internet.

## **DNS**

Domain Name System

System for alphanumeric resolution of host names in IP/IPv6 addresses in IP/IPv6-based networks

## **DNS server**

The DNS server manages the tables for resolution of the host names of network nodes into IP addresses.

## **Domain**

→ *Domain Name*

## **Domain Name**

Name of a domain as part of the "Domain Name System" (DNS) for addressing in IP-based networks. The domain name consists of name parts separated by dots, for example "this.domain.com".

See also "Host name".

## **Double NAT**

NAT method in which a source IP address as well as a destination IP address in the source network is replaced with a different source IP address or destination IP address in the destination network.

## **Downstream**

Communication from access point to node (client)

## **DP**

Distributed I/O

Input or output modules used at a distance from the CPU (central unit of the controller) or a PC via a PROFINET/PROFIBUS CP. The connection between the programmable controller and the distributed I/O can be established via the PROFIBUS DP bus system.

## **DP I/O module**

DP slaves have a modular structure. A DP slave has at least one DP I/O module.

**DP master**

A node with master functionality on PROFIBUS DP. The following must be distinguished:

DP master (class 1) or DP master 1

The DP master 1 handles cyclic user data traffic with the DP slaves assigned to it.

DP master (class 2) or DP master 2

The DP master 2 provides asynchronous services such as :

- Reading input/output data
- Diagnostics

**DP master system**

A DP master and all DP slaves with which this DP master exchanges data.

**DP mode**

Communication between the DP master and DP slaves can be divided into four modes: OFFLINE, STOP, CLEAR, RUN (corresponds to OPERATE according to the DP standard)

Each of these modes is characterized by defined actions between the DP master and the DP slaves.

**DP module name**

Name of one of the DP I/O modules entered in the DP module list.

**DP module type**

Name to identify a DP I/O module in the generic station data of a DP slave in compliance with EN 50170, Vol 2.

**DP protocol**

The rules for communication and data transmission according to the communications standard for the field area (IEC 61158) and PROFIBUS standard (EN 50170).

The DP protocol is used in the distributed I/O (DP) and allows distributed use of numerous modules and other field devices in the immediate vicinity of the process.

**DP slave**

A node with slave functions in PROFIBUS DP

**DP slave name**

To identify a DP slave in the configured DP configuration, a DP slave name is entered in the DP slave list.

**DP subnet**

PROFIBUS subnet or network on which only distributed I/O is operated.

**DSL**

Digital Subscriber Line

Standards for transmission of telephone and Internet data

**DSSS**

Direct Sequence Spread Spectrum

Spread spectrum technique for wireless data transmission

**DTIM**

Delivery Traffic Indication Message

The variable decides the number of beacons sent before the collected data packets are sent.

**Dual client**

Method for achieving a high data throughput with very short handover times. The connection is implemented over two clients; the client with the better signal is always active, and the other that is searching for a better signal is passive. The changeover is achieved within only a few milliseconds. This function must be supported by all devices in the relevant WLAN.

**Dynamic DNS**

Dynamic Domain Name System

Similar to network service → DNS for subscribers with changing IP addresses. The service updates the address entries on the Name Server in real time so that the subscriber is always accessible under a specified host name.

**Dynamic Domain Name System**

→ *Dynamic DNS*

**EAP**

Extensible Authentication Protocol

Protocol with which servers and clients can agree on a procedure for authentication prior to the actual authentication.

**EDGE**

Enhanced Data Rates for GSM Evolution

Further development of GSM technology. With an additional modulation method, the available transmission speeds in mobile wireless networks are increased. With EDGE, the packet-oriented mobile wireless service GPRS becomes EGPRS and HSCSD becomes ECSD.

**EEC**

Enhanced Environmental Conditions

Siemens specification for use of devices in environments with enhanced requirements.  
Examples: SCALANCE switches 300EEC and XR-300M EEC

**EGPRS**

Enhanced GPRS

Packet-oriented service for IP-based data transmission in GSM networks. By using an additional modulation procedure (EDGE technology), a higher transmission speed is achieved compared with GPRS.

**EIB**

European Installation Bus

Registered trademark of the European Installation Bus Association, Brussels  
A standard that describes how sensors and actuators in a house installation are interconnected and communicate with each other.  
The KNX standard is the successor to the EIB standard.

**EIRP**

Effective Isotropic Radiated Power

Unit of measurement for radiated power in reference to an isotropic radiator. Product from supplied energy and antenna gain, specified in [Watt] or logarithmically in [dBi].  $EIRP = 1.64 * ERP$  (see ERP)

**Electrical Lean Switch**

→ *ELS*

**Electrical Link Module**

→ *ELM*

**Electrical Switch Module**

→ *ESM*

## **ELM**

Electrical Link Module

Network component for Industrial Ethernet (electrical structures)

## **ELS**

Electrical Lean Switch

Electrical network component for Industrial Ethernet with switching function

## **E-mail connection**

Connection type that can be configured in STEP 7 that establishes a logical connection between a SIMATIC S7 CPU and an Advanced/IT-CP within a SIMATIC S7 station. The configured e-mail connection is necessary for sending e-mails from a SIMATIC S7 station.

## **Enhanced Environmental Conditions**

→ *EEC*

## **Enhanced GPRS**

→ *EGPRS*

## **Enhanced Passive Listening Compatibility**

For sending TCN frames (Topology Change Notifications) via RSTP edge ports. In conjunction with the "Auto Edge Port" function, this parameter is necessary to link (R)STP networks with HRP rings.

TCN frames are usually not sent via edge ports. However, this is necessary for the passive listening function on ring nodes.

## **Enterprise Resource Planning Connect**

→ *ERPC*

## **Equipotential bonding conductor**

A protective conductor for ensuring equipotential bonding.

## **ERPC**

Enterprise Resource Planning Connect

Connection between the process level (SIMATIC S7) and the enterprise level



In ERPC communication, a SIMATIC S7 station with CP 343-1 ERPC communicates with an ERP subscriber over TCP/IP. An ERP subscriber can, for example, be an Enterprise Resource Planning (ERP) system at the enterprise management level or an MES.

## ERPC application

Software package of the cooperation partners ILS Technology LLC for communication between an S7 station and ERP subscribers. The ERPC software is also loaded on the CP 343-1 ERPC. The ERPC software consists of the following two parts:

- The ERPC firmware  
Firmware part of ILS Technology LLC for communication between the CP 343-1 ERPC and an ERP subscriber. This installs the ERPC application on the CP. The application handles the ERPC communication.
- The ILS Workbench configuration  
This supplies the ERPC application with the required parameters for ERPC communication.

## ERTEC

Enhanced Real-Time Ethernet Controller

The Industrial Ethernet ASIC is a high-speed Ethernet controller, optimized for PROFINET with integrated switch functionality and processor.

## ESM

Electrical Switch Module

Industrial Ethernet switch with twisted pair connectors (D-sub or RJ45)

## ESMTP

Extended Simple Mail Transfer Protocol

Extended protocol of the Internet protocol family for transmitting E-mails based on → SMTP.

## ESP

Encapsulating Security Payload

Protocol in the IPSec protocol suite that provides the authenticity and integrity of IP packets. Unlike with Authentication Header, the user data is encrypted.

## ESS

Extended Service Set

Wireless network based on several overlapping basic service sets (BSS)

### **Ethernet flow control**

Flow control during data transfer using Ethernet to IEEE 802.3x. Pause frames stop or release sending of new frames from the connected partner device.

### **Ethernet header**

Header that has a format specified in IEEE802.3 and contains address information (source, destination) and control information.

### **Ethernet packet**

A packet sent over Ethernet. These packets have a structure specified in IEEE802.3. A Ethernet packet consists of a header and the payload data.

### **ETSI**

European Telecommunications Standards Institute  
European institute for telecommunications standards

### **European Installation Bus**

→ *EIB*

### **Event**

Context: OPC

Incident or occurrence that could be of interest for an OPC client. Events do not need to be linked to the occurrence of a condition. Events that are not related to conditions include, for example, error messages from the communications system.

### **Exchange Identification**

Auxiliary protocol for exchanging information on the ISO layer 2

### **Fast Ethernet**

Ethernet standard for a transmission speed of 100 Mbps

### **Fast Learning**

Function of a switch with which a dynamically learned MAC address is deleted immediately from the address table as soon as there is a link at the relevant port.

### **FastConnect**

→ *FC*

**Fault-tolerant communication**

→ *H communication*

**FC**

Fast Connect

Cabling system with technology for fast connector assembly in the field from SIMATIC NET

**FDDI**

Fiber Distributed Data Interface

ANSI specification for data transfer up to 100 km at a transmission speed of 100 Mbps. Counter-rotating double optical fiber cables serve as the transmission medium.

**FDL**

Fieldbus Data Link

Layer 2 on PROFIBUS; it consists of Fieldbus Link Control (FLC) and Medium Access Control (MAC).

**FDL connection**

Type of communications connection that allows program/event-controlled communication via PROFIBUS.

Previously known as: AGAG connection

**FDMA**

Frequency Division Multiplex Access

Frequency-controlled multiplex method with which several signals can be transferred on several frequency carriers at the same time.

**FDX**

→ *Full duplex*

**FEC**

Forward Error Correction

Addition of redundant bits to the user data to achieve high immunity of the signal to disturbances

**FHSS**

Frequency Hopping Spread Spectrum

Frequency spread method according to IEEE 802.11b in which the wanted signal is modulated to a hopping carrier frequency.

### **Fiber Monitoring Protocol**

Protocol for monitoring the received power and the loss of power on optical links between two switches.

### **Fiber Optic Inter Repeater Link**

Standard for the fiber-optic cable link between two repeaters of an Ethernet bus system

### **Fiberoptic**

→ *FO*

### **Fiber-optic cables**

→ *FOC*

### **Filtering**

A switch filters data traffic based on the source and destination addresses in a data packet. An incoming data packet is forwarded only to the port to which the end device with the destination address is connected.

### **Firewall**

Function that restricts data access to devices or systems with the help of packet filter rules.

### **Flow Control**

Function of the OSM/ESM with which the number of frames received can be reduced in case of overload to reduce the risk of frame loss.

### **FM**

Factory Mutual Research

US certificate for the installation of devices in hazardous locations

### **FMS**

Fieldbus Message Specification

Upper sublayer of layer 7 in PROFIBUS It includes the protocol machine, generation of PDUs and coding/decoding and interpretation of the protocol data unit.

**FMS connection**

Type of communications connection that allows program/event-controlled communication between devices that comply with the FMS standard. Device-specific data formats are converted to standardized FMS formats for transmission.

**FMS protocol**

The rules for connecting, communicating and transmitting data according to the Fieldbus Message Specification (FMS).

**FO**

Fiber optic

Fiber-optic cable, glass fiber cable

**FO port**

Fiber optic port

Port with FO connector

**FOC**

Fiber-optic cables

Transmission medium in an optical network for connecting optical Industrial Ethernet components.

**Forced Roaming**

Automatic roaming when the cable connection of the access point is interrupted.

**FQDN**

→ *Host name*

**Frame**

Frame on the transport layer (OSI layer 2)

Data unit transferred between communication partners.

Meaning in the SIMATIC NET documentation:

- Data unit transferred on the application layer (OSI layer 7)
- General term for a transferred data unit regardless of the relevant OSI layer.

## Frame

→ *Data frame*

## Frame Aggregation

Grouping together of individual data packets to form a larger data packet. Aggregated data packets can only be sent between stations that support this.

## Frame header

Preceding data record within a frame that consists not only of other parameters but generally an identifier for the frame as well as the source and destination node address.

## Frame trailer

Data record in the final section of the frame; generally contains a checksum and the end identifier of the frame.

## Free UDP connection

Type of UDP connection that can be configured in STEP 7. In contrast to a UDP connection, the address information relating to the communications partner on a free UDP connection is not specified during configuration of the connection, but is specified in the call in the user program. This means that in SIMATIC S7, a configured free UDP connection can be used for program-controlled transmission to changing communications partners.

## FREEZE mode

The FREEZE mode is a DP mode in which process input data is obtained at the same time from one or more (group) or from all DP slaves. The time of acquisition is signaled by the FREEZE command (this is a control frame for synchronization).

## FRNC

Flame Retardant Non Corrosive

Flame retardant, halogen-free jacket material of a cable

## FTEG

Law regarding wireless systems and telecommunications end devices in Germany

Law regarding wireless systems and telecommunications end devices in Germany

## FTP

File Transfer Protocol

Network protocol for transmission of files via TCP/IP networks. FTP operates at the application layer (layer 7) of the OSI layer model. It is used to transfer files from the server to client (download), from the client to server (upload) or client-controlled between two end devices. FTP folders can also be created and read out and folders and files can be renamed or deleted.

**Full duplex**

Value of the dependence on direction: Data can be sent and received simultaneously.

**Full Duplex Flow Control**

Flow control complying with the IEEE 802.3x standard. If there is overload, the switch or OSM/ESM generates so-called pause frames that disable or enable the sending of new frames on the connected partner device.

**Fully Qualified Domain Name (FQDN)**

→ *Host name*

**Functions (FCs)**

STEP 7 program block of the type "function"

**GAP factor**

GAP update factor

Number of token rotations the master waits before checking whether there is another node that wants to be included in the logical ring. The gap between the local PROFIBUS address of the master to the next PROFIBUS address of a master (active node) is known as the GAP .

**GAP update factor**

→ *GAP factor*

**GARP**

Generic Attribute Registration Protocol

Registration protocol with which VLANs and multicast groups can be defined. There are two versions of this protocol: GMRP for setting up multicast groups. GVRP for registering VLANs.

**Gateway**

Intelligent interface device that connects different types of local area networks. The gateway operates as a protocol converter between the various networks.

## Gateway

→ *Gateway*

## General Packet Radio Service

→ *GPRS*

## General request

With a general request, a central station requests the current process image from the connected nodes.

Context: TeleControl

## General Station Description

→ *GSD*

## GFSK

Gaussian Frequency Shift Keying

Modulation method in IEEE 802.11

## Gigabit Ethernet

Ethernet standard for a transmission speed of 1 Gbps

## Gigabit interface

Ethernet interface that supports the 1000Base-X (IEEE 802.3z) standard.

## Global I/O

→ *GP*

## Global Positioning System

→ *GPS*

## GMRP

GARP Multicast Registration Protocol

With a GMRP frame, a node can register at a switch as recipient for a multicast address. The switch propagates this registration in a separate frame to its ports. As a result, this address is also known to other switches and they send multicast frames for this address only to ports that have received a registration for this address.



**GP**

Global I/O

**GPRS**

General Packet Radio Service

Packet-oriented service for IP-based data transmission in GSM networks. The data is transmitted using the Internet protocols TCP/IP or UDP/IP.

**GPS**

Global Positioning System

Satellite supported system for determining the position of a GPS receiver. With three of the total 24 satellites, a GPS receiver can be clearly localized worldwide. GPS receivers are typically part of a navigation system.

**Group identification**

DP slaves can be assigned to one or more groups using a group identifier. The DP slaves can be addressed specifically when transferring control frames using the group identification.

**GSD**

General Station Description

A GSD or GSDML file contains a description of the properties (device master data) of a PROFIBUS or PROFINET device, such as device name, communication parameters, etc. The file can, for example, be used in configuring systems or for diagnostics. GSDML-files are XML based.

**GSM**

Global System for Mobile Communication

Worldwide standard for mobile communication (2G)

**Guard interval**

Wait time between two transmissions, to prevent them being mixed.

**GVRP**

Generic VLAN Registration Protocol

Protocol with which switches can exchange information over VLANs. With a GVRP frame, a node can register at a port for a specific VLAN-ID.

## **H communication**

Fault-tolerant communication

Fault-tolerant, redundant communication with SIMATIC S7 H systems

## **Half duplex**

Value of the dependence on direction: Data can either be received or transmitted at a time.

## **Half Duplex Flow Control**

Flow control for ports operating in half duplex mode. With this flow control, the OSM/ESM lowers the number of frames received at a port if there is overload due to additionally generated collisions.

## **Handover**

Transition of a mobile client from the RF field of an access point to the next. Includes mainly the re-integration into the network.

## **Handshake**

Acknowledgement procedure to establish a connection between stations wishing to communicate.

## **HARDNET module**

In contrast to SOFTNET modules, HARDNET modules are communications processors that preprocess protocols and therefore relieve the PC from time-critical tasks such as connection monitoring.

## **Hard-Polymer Cladded Silica Fibre**

FO fiber with a core of quartz glass and a plastic jacket.

## **Hardware product version**

Identification of the hardware version of SIMATIC NET products

## **HART**

Highway Addressable Remote Transducer

Specification of a communications protocol for digital fieldbuses. Existing cables for the transfer of 4-20 mA analog sensor signals can also be used to transfer the HART signals. The publisher of the specification is the HART Communication Foundation (HCF), see <http://www.hartcomm.org>.

**HART Version 7**

HCF specification

The main focus is on "WirelessHART" communication of HART devices.

**HCF**

→ *HART*

**Hidden node problem**

Two nodes are arranged in a wireless cell so that they are located outside each other's ranges. If the medium is accessed at the same time, collisions result.

**High-availability Seamless Redundancy Protocol**

→ *HSR*

**Highest (station) PROFIBUS address**

→ *HSA*

**Highest PROFIBUS address**

→ *HSA*

**HIPERLAN**

High Performance Radio LAN

Wireless network in the 5 GHz band

**HMAC**

→ *MAC*

**Home RF**

Standard for wireless communication between PCs and consumer devices in the home environment. Was squeezed out of the market by IEEE 802.11.

**Host name**

Unique designator in a domain associated with the IP address of a device. In the address example "device.this.domain.com", "device" is the host name.

## HRP

High Speed Redundancy Protocol

Media redundancy method used with SIMATIC NET switches to increase the network availability in a ring topology.

The previous name "High Speed Redundancy" (HSR) is no longer used for this method.

## HSA

Highest PROFIBUS Address

Highest (station) PROFIBUS address

Bus parameter for PROFIBUS. Specifies the highest PROFIBUS address of an active node on PROFIBUS. For passive nodes, PROFIBUS addresses higher than the HSA are permitted (range of values: HSA 1 to 126).

## HSCSD

High Speed Circuit Switched Data

Expansion of the CSD method (Circuit Switched Data) for dial-in data connections in GSM networks. By bundling channels, higher transmission speeds are achieved in HSCSD.

## HSDPA

→ *HSPA*

## HSPA

High Speed Packet Access

Further development of the UMTS technology that allows higher data transmission speeds for downloading and uploading. HSPA is divided into HSDPA (download) and HSUPA (upload).

## HSR

High-availability Seamless Redundancy Protocol

HSR is a redundancy protocol for Ethernet networks. It is specified in IEC 62439-3. In HSR, frames are sent at the same time via two sides of a ring. HSR allows bumpless path redundancy without reconfiguration times.

## HSR (High Speed Redundancy)

→ *HRP*

## HSUPA

→ *HSPA*

**HTML process control**

Technology with which process information is accessed using HTML pages.

**HTTP**

Hypertext Transfer Protocol

Transmission protocol for Web pages on the Internet

**HTTPS**

Hypertext Transfer Protocol Secure

Expansion of HTTP for secure transmission of confidential data with the aid of SSL.

**Hub**

Active network components with repeater functionality, synonym for star coupler.

**Hypertext Transfer Protocol**

→ *HTTP*

**IAPP**

Inter Access Point Protocol

Protocol for communication between access points

**IBSS**

Independant Basic Service Set

Ad-hoc network for spontaneous and simple establishment of wireless links without a network infrastructure

**ICMP**

Internet Control Message Protocol

Test protocol of the IP family of protocols that you can use to determine if a network node can be reached at the IP level.

This protocol exists on every Windows computer under the same name as a console application (command prompt level). With "Ping", you can prompt a reply (sign of life) from an IP network node within a network as long as you know its IP address.

**ICMP Echo Request**

Display of the incoming ping

## ICMP subnet broadcast

To find the IP nodes in an internal network, a host can send an ICMP echo request with the IP subnet broadcast address, in other words, an address that contacts all IP nodes in the internal subnet.

## ICNIRP

International Commission on Non-Ionizing Radiation Protection

International Council on Non-Ionizing Radiation Protection

## IDE

Integrated Development Environment

Examples: eclipse, Borland JBuilder etc.

## Identity Protection

Difference between the two options of the IKE mode under VPN (see also IKE)

- Main Mode

IKE phase 1 runs slower in Main Mode but more secure than in the alternative Aggressive Mode.

In Main Mode, the identity of the sender is transmitted encrypted (Identity Protection).

- Aggressive Mode

In Aggressive Mode, the identity is transmitted unencrypted. The transmission is faster.

## I-Device

The "I-device" (intelligent IO device) function allows a device (CPU or CP) to exchange data deterministically with an IO controller which makes it possible to use the device as an intelligent preprocessing unit of sub processes. The I-device is connected to an IO controller as an IO device.

## IE

Industrial Ethernet

## IEEE

Institute of Electrical and Electronics Engineers - The world's largest technical professional organization for the advancement of technology

<http://www.ieee.org>

## IEEE 802

Project of the IEEE for standardization of LAN and MAN networks

Includes, among other things, the following working groups and standards:

- IEEE 802.3  
Industrial Ethernet working group
- IEEE 802.3af  
Power-over-Ethernet (PoE)
- IEEE 802.3at  
Extended Power-over-Ethernet (PoE+) with higher power
- IEEE 802.3j  
Fiber-optic 10Base-F working group
- IEEE 802.3u  
Fast Ethernet 100Base-T working group
- IEEE 802.11  
First version of the standard for wireless networks in the 2.4 GHz band with transmission speeds up to 2 Mbps
- IEEE 802.11a  
Wireless networks in the 5 GHz band with transmission speeds up to 54 Mbps
- IEEE 802.11b  
Wireless networks in the 2.4 GHz band with transmission speeds up to 11 Mbps
- IEEE 802.11e  
Expansion for support of QoS. Prioritization of data packets permitted. Optimization for voice over wireless LAN and streaming multimedia
- IEEE 802.11g  
Expansion for wireless networks in the 2.4 GHz band with transmission speeds up to 54 Mbps
- IEEE 802.11h  
Expansion for wireless networks in the 5 GHz band with transmission speeds up to 54 Mbps Standard for the European continent; condition DFS/TPC
- IEEE 802.11i  
Among other things, the standard describes the WPA2 method, the TKIP method and the AES encryption algorithm. IEEE 802.11i closes a series of weak points in the WEP security mechanism.

- IEEE 802.11n  
Expansion for wireless networks in the 5GHz band with a high transmission speed up to 600 Mbps
- IEEE 802.1x  
Standard for use of a radius server as authentication server. In IEEE 802.1x the entire communication is encrypted.

ON overview can be found at:

<http://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68>

#### **IEEE 802.15.4**

Specification for a protocol for wireless data transmission of devices with a low power consumption and short range. It is used mainly for WirelessHART networks (WSN).

#### **IE-Switch / Industrial Ethernet Switch**

→ *Switch*

#### **IETF**

Internet Engineering Task Force

Syndicate involved in all aspects of the Internet that prepares proposals for standardization.

#### **IGMP**

Internet Group Management Protocol

Expansion of the IP protocol that allows the assignment of IP addresses to multicast groups.

#### **iHOP**

industrial Hopping

Adaptive channel hopping method with which the WLAN access point sets the time of the hop and the send channels for the clients.

#### **IKE**

Internet Key Exchange

Protocol for automatic key management for IPsec.

#### **ILM**

Infrared Link Module

Infrared network component



**ILS Workbench**

Configuration and diagnostics tool of the cooperation partner ILS Technology LLC

See also ERPC.

**Image memory**

Memory area for the process image in a telecontrol module

Each data frame is saved exactly one time in the image memory. New values of a data point overwrite the existing value in the image memory.

See also send buffer

Context: TeleControl

**In-band IP address**

IP address with which a switch can be addressed from the routed or switched network.

**Industrial Ethernet**

Bus system complying with IEEE 802.3 (ISO 8802-2)

**Industrial Ethernet Security**

→ *Industrial Security*

**Industrial Security**

System properties for data security and information security covers mainly guarantee the authenticity, confidentiality, integrity and availability of data as well as access protection for the data.

**Industrial Twisted Pair**

→ *ITP*

**Industrial Wireless LAN**

→ *IWLAN*

**Infrared Link Module**

→ *ILM*

### **InProcess server**

Server that is in the same process space as the client and can only be addressed from this process space. Normally, inprocess servers are implemented as DLLs.

Example: The OPC Automation interface is implemented as an in-process server. The in-process server accesses the local server via the OPC Custom interface.

### **Instabus<sup>®</sup>**

Installation bus system for building technology. Registered trademark of Siemens AG, which members of the "Insta community" have the right to use.

### **Instrumentation Tray Cable**

→ *ITC*

### **Interconnection**

Logical data connection between two objects in for PROFINET CBA in SIMATIC iMap

Connection between two technological functions. An output is interconnected with an input of the same data type. Interconnections are represented in SIMATIC iMap by lines or continuation lines.

### **International Commission on Non-Ionizing Radiation Protection**

→ *ICNIRP*

### **Inter-station communication**

Context: TeleControl

Communication between two stations that is forwarded by a master station.

For dial-up networks, a direct connection between the two stations is established in ST7 networks.

### **IO controller**

→ *PROFINET IO controller*

### **IO device**

→ *PROFINET IO device*

### **IP**

Internet Protocol

Represents the network layer of the OSI model for TCP/IP-based networks.

The most important information is the unique IP address.

The packets are sent to the destination node independently. IP does not negotiate anything with the destination node. There is no end-to-end error check. Packets can arrive in a different order from the order they were sent in. TCP is responsible for putting them together in the correct order.

## IP

### Ingress Protection

Degree of protection with enclosure to IEC / EN 60529 consisting of two digits/letters for protection against intrusion / particles and water. Examples:

- IP20  
Protection against the ingress of particles with diameter > 12.5 mm; no special water protection.
- IP65  
Protection against the ingress of dust and water jets.

### IP Access Control List

→ *IP-ACL*

### IP access protection

Access protection based on IP addresses. This makes it possible to restrict access to the device (e.g. communications processor) via defined IP address ranges or single IP addresses.

### IP address

The IPv4 address consists of a numeric code made up of four numbers (4 bytes) each from 0 to 255 (e.g. 192.168.0.55). It is the numeric address of a particular computer in the network / Internet.

### IP broadcast

Broadcast in a network Broadcast telegrams reach all nodes in the network that are ready to receive broadcast telegrams or have been enabled to do so.

### IP multicast

Message transmission from one node to multiple nodes in a network. The receivers must have multicast addresses (224.0.0.0 ... 239.255.255.255).

### IP packet filter rule

Firewall rule with filter criteria of the OSI layers 3 to 8.

## **IP/MAC service definition**

Using the IP and MAC service definitions, you can define succinct and clear firewall rules. You select a name and assign the service parameters to it.

These services defined in this way can also be grouped together under a group name. When you configure the packet filter rule, you simply use this name.

## **IP-ACL**

IP Access Control List

Access control list for IP access protection in Ethernet. Connections are only possible to communications partners whose IP address is listed in the IP ACL.

## **iPCF**

industrial Point Coordination Function

Functional expansion of the IEEE 802.11 standard for applications requiring real-time and a deterministic response (predictable reply times). This makes rapid roaming of mobile nodes from one wireless cell to the next possible and supports wireless and secure PROFINET IO communication.

## **iPCF-MC**

Industrial Point Coordination Function – Management Channel

Management expansion of iPCF in which a second wireless interface of the access point operates as a management interface and sends beacons with administrative information. The other channel is used only for data traffic.

## **IPsec**

IP protocol expansion for VPN at OSI layer 3

IPsec only allows encryption of IP packets but does not transfer multicast frames and only supports static routing.

## **IPv4**

Internet protocol version 4

Format for IP addresses. IPv4 uses 32-bit addresses, this makes a maximum of 4,294,967,296 unique addresses possible. IPv4 addresses are normally written in decimal in four blocks. Each block contains 8 bits resulting in a range of values of 0 to 255 for each block.

## **IPv6**

Internet protocol version 6

Standard for IP addresses. IPv6 uses 128-bit addresses. The address space of 2<sup>128</sup> has been significantly expanded compared to IPv4. The addresses consist of 8 blocks of 16 bits each

that are separated by a colon. In URL notation an IPv6 address is placed in brackets, example:  
http://[<Address>]

**IRC**

Industrial Remote Communication  
SIMATIC NET product group for telecontrol.

**IrDA**

Infrared Data Association  
Data communication with infrared over short distances

**IRT**

Isochronous Realtime  
Isochronous real-time operation based on Ethernet with deterministic and isochronous transmission of frames.

**IRT communication**

Isochronous Real-Time communication  
Transmission mechanism for cyclic exchange of IO data between PROFINET IO devices. For the IO data, there is a reserved time frame within the send clock cycle. This guarantees that the IO data is exchanged at constant intervals. By using suitable hardware, clock frequencies up to 1 ms are possible.

**ISAKMP**

Internet Security Association and Key Management Protocol  
Protocol for establishing Security Associations (SA) and exchange of cryptographic keys

**ISDN**

Integrated Services Digital Network  
Standard for a digital transmission network for telephone, telefax, telex, teletext and datex-J/L/P services. The data of various services can be transferred simultaneously. Telephone connections normally operate at transmission speeds of 56 to 64 kbps.

**ISM band**

Industrial, Scientific and Medical band  
Frequency band whose use is controlled by general assignments. You will find more detailed information on this from the "network agency" of your country.

### **ISO network nodes**

Network nodes without IP capability but that can be addressed using ISO protocols.

### **ISO transport connection**

Communication connection of the transport layer ISO transport connections allow program/event-controlled communication via Industrial Ethernet. On an ISO transport connection, blocks of data can be exchanged in both directions.

### **Isochronous Realtime**

→ *IRT*

### **ISO-on-TCP**

Communication protocol for Industrial Ethernet communication according to the TCP/IP with the extension RFC 1006.

### **ISP**

Internet Service Provider  
Provider of Internet services

### **IT**

Information technology with email, FTP and Web technology for Siemens communications processors

### **ITC**

Instrumentation Tray Cable  
Approval for IE FC TP standard cable

### **ITP**

Industrial Twisted Pair  
Bus system suitable for industrial use based on the twisted pair standards IEEE 802.3i: 10Base-T and IEEE 802.3j: 100Base-TX. ITP is an industrial cable variant with S/STP cable structure. While typical network cables have four pairs of wires, ITP is restricted to just two pairs.

### **ITP port**

Port with Industrial Twisted Pair (ITP) connectors (D-sub 9-pin female)

**ITP Standard Cable**

Twisted-pair cable for industrial use that complies with category 5 and is particularly densely shielded.

**IWLAN**

Industrial Wireless LAN

WLAN suitable for industry complying with the IEEE 802.11 standard

**Jabber function**

This function prevents a defective end device from blocking the bus line with overlong data packets (jabber). At the start of each transmission, a timer is started that monitors the length of the data being sent.

**Jabbers**

Frames with an invalid CRC and a length greater than 1536 bytes.

**JavaScript**

A scripting language developed by Netscape. JavaScript allows Web documents to be designed interactively and dynamically. As a programming language, JavaScript is considered easy to work with.

**JVM**

Java Virtual Machine

Interpreter that interprets the native machine code generated by the Java compiler. The JVM is a central element in SUN's Java programming environment that ensures that Java programs are not platform-dependent.

**Kerberos**

Security system for encryption of sensitive data

**KNX**

Konnex (EN 50 090, ANSI EIA 776)

Universal bus system for the entire house and building system technology.

KNX was developed by the Konnex Association based on the EIB (European Installation Bus).

**L2F**

Layer 2 Forwarding

Network protocol (similar to PPTP) that supports various protocols and multiple independent tunnels.

## **L2TP**

Layer 2 Tunneling Protocol

Network protocol that tunnels frames of protocols of the data link layer (layer 2) of the OSI model between two networks to establish a virtual private network (VPN).

## **LACP**

Link Aggregation Control Protocol

Network protocol according to IEEE 802.3ad that allows the dynamic bundling of physical network connections

## **LAN**

Local Area Network

A LAN is a local or locally restricted network.

## **Latency**

Throughput time of a data packet through a switch

## **Law regarding wireless systems and telecommunications end devices in Germany**

→ *FTEG*

## **Layer 3 routing**

Function for communication between different IP subnets based on layer 3. Also referred to as "IP routing".

## **LC**

Lucent Connector

Special type of connector for fiber-optics

## **Link Aggregation**

Mechanism for bundling several physical interfaces to create one logical channel. This is used to increase the data throughput between two Ethernet switches. Implementations can also bind together servers and other systems using link aggregation.



## Link Class

Quality of a complete link from the active component to the end device (patch cord, patch panel, installation cable, telecommunication outlet, connecting cable). This link must meet the value specified in the structured cabling standard ISO/IEC 11801. In contrast to this, there is also the specification regarding "categories", where only requirements of products are defined, for example cable according to Category 5. The suitable interaction of components of a link is ignored.

## Link Control

Context: OSM

With regular test pulses complying with the 100Base-TX standard, OSM/ESMs monitor the connected TP/ITP cable segments for short-circuits or interruptions. OSMs/ESMs do not send any data to a segment from which they are not receiving connection test pulses. An unoccupied interface is evaluated as a line interruption because the device without power cannot send any connection test pulses.

## LLC

Logical Link Control

Standardized network protocol according to the IEEE 802.2 standard; the protocol can be assigned to OSI layer 2.

## LLDP

Link Layer Discovery Protocol

Vendor-neutral protocol of the data link layer via which an Ethernet device can communicate its identity and characteristics. The data is used to support topology analysis and representation.

This information is stored in the Management Information Base (MIB) and can be read via SNMP.

## LLI

Lower Layer Interface

Part of layer 7 of PROFIBUS, in which layer 7 services are mapped to layer 2 services.

## Local Server

A server located on the same computer as the client. Like every independent application, it has its own process area and namespace.

Example: The OPC server for SIMATIC NET is a local server. It is implemented as an EXE file.

### **Local TIM**

A TIM connected to a PC (ST7cc, ST7sc) or an S7 CPU over the MPI bus, Industrial Ethernet or an IP-based network.

### **Logging**

Recording events in a system or network.

### **Logical trigger**

Method for event-oriented data transfer in ERPC communication. Data is read from the CPU of the S7 station containing the CP 343-1 ERPC. The data read out is sent by the ERPC application in the CP to one or more ERP subscribers.

### **Longitudinal loss**

Loss during propagation of electromagnetic waves within a coaxial cable

### **Loop Detection**

With the loop detection function, the port sends special test frames, the loop detection frames. If these frames are sent back to the device, there is a loop.

### **Loop resistance**

Total resistance of the outward and return line of a cable

### **MAC**

Media Access Control

Protocol with which access to a transmission medium (cable, wireless) is controlled if it cannot be used by all nodes at the same time.

### **MAC**

Message Authentication Code (MAC)

Method for authentication of messages. The MAC is the checksum from the message and a secret key.

The Keyed-Hash Message Authentication Code (HMAC) is based on cryptographic hash functions and is used for example in IPsec or SSL.

### **MAC address**

Hardware address for the unique identification of a device in an Ethernet network. The MAC address is assigned by the vendor. On some devices, this can be changed.

**MAC packet filter rule**

Firewall rules with filter criteria of OSI layer 2.

**MAC-Protokoll**

→ *MAC*

**Main Mode**

→ *Identity Protection*

**MAN**

Metropolitan Area Network

Data network with the geographical span of a city or town. An MAN can have a span up to 100 km.

**MAP**

Manufacturing Automation Protocol

Set of protocols for industrial communication from the 80s that has mostly been replaced by other protocols.

**Master**

Active node on PROFIBUS that can send frames unsolicited when it has the token.

**Master station**

Station in the top hierarchy of a telecontrol network with ST7 protocol. It is connected to the control system and the substations or node stations.

The WAN interfaces of the TIM are set to the network node type "Master station".

**Master-slave process**

Bus access method where only one node is master and all other nodes are slaves.

**MAU**

Medium Attachment Unit

Transceiver that implements the actual access to the transmission medium

**Max TSDR**

→ *Maximum Station Delay*

### **Max. Retry Limit**

Bus parameter for PROFIBUS. Sets the maximum number of call repetitions when the addressed node (DP slave) does not reply.

Note:

Here, a value of that least 1 should be set so that if an error occurs with acyclic frames there is at least one repetition

### **Maximum Station Delay**

Maximum protocol processing time

Bus parameter for PROFIBUS

Max. TSDR specifies the longest interval required by a node in the subnet between receiving the last bit of an unacknowledged frame and sending the first bit of the next frame. After sending an unacknowledged frame, a sender must wait for the max. TSDR to elapse before sending a further frame. A DP slave may only wait for the time of max. TSDR before sending a response. Max. TSDR must be shorter than the slot time.

### **MCC - Mobile Country Code**

→ *PLMN*

### **MD**

Message Digest

Group of cryptographic protocols.

### **MD5**

Message Digest Version 5

Hash function that generates a 128-bit hash value from any message.

### **MDI**

Medium Dependent Interface

Port or cable, on which the receive (Rx) and the send (Tx) lines are not crossed over.

### **MDI / MDI-X autocrossover function**

Function allowing end-to-end cabling without external, crossover Ethernet cables being necessary. This prevents malfunctions resulting from mismatching send and receive wires. This makes installation much easier for the user.

### **MDI-X**

Medium Dependent Interface – Cross Over

Port or cable with crossover receive (Rx) and send (Tx) lines

### **Media Access Control**

→ *MAC*

### **Media module**

A media module is a modular network component. Media modules are used in the module slots of module devices. End devices and other network segments are connected according to the media modules being used. Within the MM900 product group, there are electrical media modules, optical media modules and the SFP media module.

### **Media redundancy**

Method for increasing availability in Industrial Ethernet networks in which devices can be reached over different paths. This might be achieved by meshing networks, arranging parallel transmission paths or by closing a linear bus topology to form a ring. Media redundancy within a ring topology is available with SIMATIC NET products with the HSR and MRP methods.

### **Media Redundancy Protocol**

→ *MRP*

### **Media Redundancy with Path Duplication**

→ *MRPD*

### **MES**

Manufacturing Execution System at the factory management level

### **Mesh bonding network (MESH BN)**

A bonding network in which all associated equipment frames, racks, cabinets, and the DC power return conductor are bonded together and also bonded at multiple points to the CBN. Consequently, the MESH BN augments the CBN.

### **Message Authentication Code**

→ *MAC*

### **Messages**

Emails and SMS in the TeleControl context

See also Data frame.

**MIB**

Management Information Base

Standardized data structure written in a language not dependent on the target system. Elements of this data structure are known as MIB objects. Is used for example by SNMP.

**MIB browser**

Program for displaying MIB objects. Is normally included in network management applications.

**MIB variable**

Placeholder for a scalar value or a value defined as a string that is read out of or written to the MIB using SNMP.

**MIC**

Message Integrity Protocol

Method for improving the integrity of data in WLAN

**Middleware**

Software that acts as an intermediary between operating systems and drivers on the one hand and user applications on the other.

**MIMO**

Multiple Input Multiple Output

Method for the use of several transmit/receive antennas for the transmission. This improves the quality and increases the transmission speed.

**Min TSDR**

→ *Minimum Station Delay*

**Mini PCI**

Special design for wireless LAN cards for direct integration into products.

**Minimum Station Delay**

Minimum protocol processing time

Bus parameter for PROFIBUS

Min. TSDR sets the minimum period that the recipient of a frame must wait before sending the acknowledgement or before sending a further frame. Min TSDR is based on the longest time required by a node in to receive an acknowledgement after sending the frame.

## Mirroring

Method with which the incoming and outgoing data traffic of a port (mirror port) is mirrored to another port (monitor port) to allow traffic to be investigated. Protocol analysis devices can be connected to the monitor port. The monitor port is not available for data exchange. Mirroring has no effect on the mirror port.

## MMS

Manufacturing Message Specification  
User interface of MAP

## MNC - Mobile Network Code

→ *PLMN*

## Modes

Discrete waves used to transmit data within a fiber-optic cable. With single mode fibers, only one wave propagates, whereas in multimode fibers several waves propagate. Modes are patterns of electromagnetic fields in FOCs.

## Monomode fiber

Type of fiber-optic cable that can only transfer one mode (light wave). The monomode fiber (also known as single mode fiber) has a core diameter of 5 to 9  $\mu\text{m}$ . The outer diameter is 125  $\mu\text{m}$ . The information is transmitted through the core of the fiber.

## MPI

Multi Point Interface  
Multipoint interface for SIMATIC S7

## MRP

Media Redundancy Protocol  
A method specified in IEC 61158 Type 10 for increasing network availability in a ring topology.

## MRPD

Media Redundancy with Path Duplication

Media redundancy method for ring topologies with IRT.

## **MSS**

Mobile Satellite Service  
Satellite wireless within UMTS.

## **MSTP**

Multiple Spanning Tree Protocol  
MSTP allows several independent transfer paths of RSTP in different VLANs. This allows the traffic from different logical networks to be routed via different paths.

## **MTBF**

Mean time between failures  
Measure of the likelihood of failure of components

## **MTU**

Maximum Transmission Unit  
Specifies the permitted size of a data packet for transmission on the network.

## **Multicast**

→ *IP multicast*

## **Multi-master polling with time slots**

When stations need to communicate with more than one master station in dedicated line or wireless operation, the multimaster polling with time slots mode is used. Each of the connected master stations is assigned one or more defined time slots per minute for polling. The master stations then have their turn to poll in every minute.

## **Multimode**

Type of transmission on optical fibers in which the pulse is transferred using many modes (light waves) that travel along curved paths or are reflected within the core.

## **Multipath propagation**

Reflections of a radio wave caused by various objects in the transmission path. This means that the radio wave arrives with different intensities and at different times at the receiver.



**Multiple Spanning Tree Protocol**

→ *MSTP*

**NAPT**

Network Address Port Translation

Method in which a destination IP address as well as a destination port in the source network are replaced with a different destination IP address or a different destination port in the destination network.

**NAT**

Network Address Translation

Method in which the IP address in a frame is replaced with a different IP address.

**NAT traversal**

Method in which it is made possible for IPsec data to traverse NAT devices. To do so, IPsec packets are packaged in UDP packets because the header of the IP packets encrypted by IPsec cannot be changed by NAT devices.

**NAT/NAPT router**

Router with NAT/NAPT function

**National Electrical Code**

→ *NEC*

**NCM**

Network and Communication Management

Group of SIMATIC NET management products

**NCM S7 for Industrial Ethernet**

Software for configuration and diagnostic functions of Ethernet CPs

**NCM S7 for PROFIBUS**

Configuration software for configuration and diagnostics functions of PROFIBUS CPs.

**NDIS**

Network Driver Interface Specification

Interface from Microsoft and 3Com

## NEC

National Electrical Code

UL directive for laying cables in buildings

## Network

Consists of one or more interconnected subnets with any number of nodes. Several networks can exist side by side.

## Network Address Port Translation

→ *NAPT*

## Network ID

→ *Subnet ID*

## Network Load Balancing

→ *NLB*

## Network Time Protocol

→ *NTP*

## Network view

- In PROFINET CBA: View of the devices and the networks (Ethernet, PROFIBUS) in SIMATIC iMap.
- In the TIA Portal: A working area of the hardware and network editor

## NLB

Network Load Balancing

Feature of some Windows operating systems that allows server redundancy. Network Load Balancing (NLB) automatically detects the server load and can distribute client data traffic to remaining servers.

## Node station

A node station is a station located between the master station and stations in the hierarchy of a telecontrol network. One or more subordinate stations are connected to a node station. The data traffic between these stations and the master station is handled via the node station.

Direct data exchange between the node station and the subordinate stations is also possible. Multiple node station levels are possible in a SINAUT network.

Context: TeleControl

## **NTP**

Network Time Protocol

TCP/IP based protocol that allows time transmitters to be used on the Internet. The simpler SNTP (Simple Network Time Protocol) was derived from NTP and works with simpler calculations and therefore less accuracy.

## **NTP (secure)**

Network Time Protocol (secure)

The secure method NTP (secure) uses authentication with symmetrical keys. Various configurable hash algorithms are available for the integrity check.

## **OAKLEY Key Determination protocol**

The protocol describes the generation of secret key material. It is part of the Internet Key Exchange Protocol (IKE).

## **Object Identifier**

→ *OID*

## **OCX**

OLE Cumstoms Control

This is an ActiveX control. These are COM objects that can be employed as reusable components in the form of controls.

## **OFDM**

Orthogonal Frequency Division Multiplex

Modulation techniques in IEEE 802.11a, IEEE 802.11g and IEEE 802.11n

## **OFDM/CCK**

Orthogonal Frequency Division Multiplex/Complementary Code Keying

Modulation method in IEEE 802.11a

## **OFN/OFNG**

Optic fiber cable - nonconductive / Optic fiber cable - nonconductive - general purpose

FO cable groups for use in buildings in compliance with UL standard 1651.

**OFNP**

Optic fiber cable nonconductive - Plenum

FO cable groups for unprotected use in cable channels, drop ceilings and subfloors in compliance with UL standard 1651.

**OFNR**

Optic fiber cable nonconductive - Riser

FO cable groups for use in vertical shafts/channels in compliance with UL standard 1651.

**OID**

Object Identifier

Describes a unique path through the hierarchical MIB structure to the relevant MIB object.

**OLM**

Optical Link Module

SIMATIC NET network component with repeater functionality

**Omnidirectional**

Antennas with a radiation pattern both in the 360 degree direction and in the elevation plane

**One-shot buffer**

Recording stops when the buffer is full.

**OP**

Operation Panel

Operator control and monitoring (HMI) device

**OPC**

Standard interface for access to process data

Originally "OLE (object linking and embedding) for Process Control".

**OPC class model**

A class model stipulated in the OPC specification that describes objects, interfaces and methods in three hierarchic classes.

**OPC DA**

OPC Data Access

Standard for Ethernet-based access to data of measurement and control devices, the discovery of OPC servers and simple browsing in the namespaces of the OPC servers based on client/server communication.

**OPC Data Access**

→ *OPC DA*

**OPC Foundation**

Organization founded with the aim of defining and promoting the interaction of components in automation based on the standards of OPC interfaces.

**OPC Group**

Middle class in the OPC class model. An object of the OPC group class manages OPC items and is a container for objects of the OPC item class. With an OPC Group, a client can form meaningful units of OPC items and execute operations with them.

**OPC item**

Lowest class in the OPC class model. An object belonging to the OPC item class represents a connection to a process variable.

**OPC program alarm**

Configured alarm texts in an S7-1200 (V4 and higher) or S7-1500 that are transmitted over an S7 connection between a PC station or OPC server (V14 and higher) and an S7-1200 (V4.0 or higher) or S7-1500. The alarm texts can be configured in an editor.

**OPC server**

Highest class in the OPC class model. An object of the OPC server class has various attributes including information on the status and version of an OPC server object. The OPC server is a container for an object of the OPC Group class.

**OPC UA**

OPC Unified Architecture

Collection of specifications of the OPC Foundation to harmonize different OPC Classic components.

### **OPC UA certificate**

In the OPC UA environment, X.509 certificates are used to authenticate communication between the various components of the system.

### **OPC UA client**

Application that requests data from other applications or devices based on OPC UA (client function).

### **OPC UA redundancy**

OPC Unified Architecture redundancy

The specification created by the OPC Foundation allows the setting up and operation of a redundant server system that is proof against failure. If a server fails in a redundant server structure, a backup server takes over its functions allowing clients connected to the system to continue working uninterrupted.

### **OPC UA SDK**

OPC Unified Architecture Software Development Kit

A set of interfaces, libraries and applications that allow the fast creation of UA applications in a .NET programming environment.

### **OPC UA server**

Application that supplies other applications or devices with data based on OPC UA (server function).

### **OPC UA stack**

UA ANSI C stack developed for the specification created by the OPC Foundation.

### **OPC Unified Architecture**

→ *OPC UA*

### **OPC UA PubSub**

OPC UA Publish-Subscribe

Publisher-Subscriber based communication according to OPC UA specification Part 14

- Publish

Publisher publishes data in form of data sets with associated metadata.

- Subscribe

Subscribers can subscribe to published data by registering with publishers for reading published data sets.

**OPC UA PubSub communication**

→ *OPC UA PubSub*

**Open communication services**

Formerly "S5-compatible communication"

Communication services that allow non-device dependent data exchange based on TCP communication via Industrial Ethernet. Open communication services become accessible in SIMATIC S7, for example, via the SEND/RECEIVE interface.

**Open User Communication**

→ *OUC*

**Operation Panel**

→ *OP*

**Optical Link Module**

→ *OLM*

**Optical power loss**

The optical power loss is the cumulative value of all the losses occurring in the fiber-optic transmission path. These are due mainly to the attenuation of the fiber itself and the splices and couplings. The optical power loss must be less than the optical power budget available between the transmitter and receiver.

**Optical Switching Module**

→ *OSM*

**Organizationally Unique Identifier**

→ *OUI*

**OSI layer model**

→ *OSI reference model*

**OSI reference model**

Model of the International Organization for Standardization (ISO) for the organization of protocols for open communication. It consists of 7 layers one building on the other.

It is also known as the ISO/OSI layer model.

## **OSM**

Optical Switching Module  
SIMATIC NET Ethernet switch with optical ports

## **OSPFv2**

Open Shortest Path First version 2  
Dynamic routing protocol (link state routing protocol) defined in RFC 1247. Each router has an image of the network that it enters in a link state database (OSPF LSDB). Based on this database, the router calculates the routes with the shortest-path-first-algorithm (SPF). In contrast to RIP, OSPF allows hierarchical routing in which the network is divided into independent areas. The routers do not exchange routing tables as in RIP, but rather link state updates.

## **OUC**

Open User Communication  
Communication services for SIMATIC stations that are implemented by program blocks under STEP 7 Basic / Professional.

## **OUI**

Organizationally Unique Identifier  
24-bit number issued by the IEEE Registration Authority to companies. Companies use the OUI for various hardware products among other things as the first 24 bits of the MAC address.

## **Out-band IP address**

IP address with which an IE switch can be addressed externally (not from the routed or switched network).

## **Oversize packets**

Frames with a valid CRC and a length (packet size, see below) greater than 1536 bytes.

## **PA (Process Automation)**

→ *PROFIBUS PA*

## **Packet**

Frame on the transport layer (OSI layer 3)



**Packet filter rule**

Using packet filter rules, you decide whether or not a data packet is allowed to pass through the packet filter. The decision as to whether a packet may pass or not is made based on the protocol fields. Examples of protocol fields are the IP source or the IP destination address.

**Packet Size**

Length of the frame from the destination address to the CRC field.

**PAN**

Personal Area Network

Network for devices located close together.

**PAP**

Password Authentication Protocol

Authentication protocol used within the framework of the Point-to-Point Protocol (PPP) for dial-in of modems.

**Parallel Redundancy Protocol**

→ *PRP*

**Partition Mode**

Context: OSM

Operating status of an OSM/ESM that occurs when more than 60 collisions occur when transmitting. In this mode, OSM/ESM waits for the first valid packet before it changes back to normal transmission mode. In partition mode, it continues to send but no longer receives (segmented).

**Passive Listening**

Function of a switch with which the switch can also react to changes in the configuration without being in (R)STP mode. Even if the (R)STP function is disabled for the switch, it forwards (R)STP configuration frames transparently.

When the switch detects a topology change frame via a Topology Change Notification, it briefly lowers the aging time which allows it to update its MAC address table more quickly.

**Path Variability Value**

The total of the variability values of all active network components along a path between the two nodes. The frame delay time through an active network component varies from frame to frame. This variation specified in bit times is the variability value of this network component.

**PC card**

Special design of Wireless LAN cards (PCMCIA)

**PC station**

PC with communications modules and applications. The role of this PC might be, for example, to communicate with SIMATIC S7 devices and perform process control tasks. The term "runtime station" is also used to describe such PCs equipped with runtime software.

**PCF**

Point coordinated function

Access method to support time-critical services in a WLAN.

**PCF**

Polymer Clad Fiber

Optical fiber that can be assembled in the field and whose core is made of glass and jacket made of plastic.

**PDA**

Personal Digital Assistant

Mobile end device

**PDU**

Protocol Data Unit

Protocol data unit

**PEM**

Privacy Enhanced Mail

Security services for encrypted email traffic

**PEN conductor**

Earthed conductor that performs the functions of the protective conductor and neutral conductor at the same time

**PFS**

Perfect Forward Secrecy

Mechanism that ensures that new key negotiations are not based on previous keys. Disabling the option allows for faster but less secure encryption.

**PG operation**

Mode of the PROFIBUS/Ethernet CP in which the SIMATIC S7CPU is programmed, configured or diagnosed over PROFIBUS/Ethernet. This mode is handled by the S7 functions.

**PG/OP communication**

Programming device/operator panel communication

Allows access by the STEP 5 and STEP 7 configuration software to the SIMATIC programmable controllers.

**Piconet**

Network structure in Bluetooth, in which up to 8 nodes are organized.

**Ping**

→ *ICMP*

**PKCS**

Public Key Cryptography Standards

Collection of standards for asymmetrical cryptography systems.

**PKCS#12 format**

Standard for the transfer and backup of password-protected, personal identification information such as private keys and certificates.

**PKI**

Public Key Infrastructure

System for unencrypted data transmission with the help of key pairs. Due to the public keys to be distributed, certificates, digital signatures and chains of trust are used.

**Plastic Cladded Silica**

A fiber-optic cable construction in which quartz glass is used as the core material and silicone rubber as the cladding.

**Plastic Optical Fiber**

→ *POF*

**PLMN**

Public Land Mobile Network

Worldwide unique identifier of mobile wireless networks. The PLMN is made up of the three-digit Mobile Country Code (MCC) and the two-or three-digit Mobile Network Code (MNC) of the network provider.

### **Pluggable transceiver**

Specification of modular optical or electrical transceivers for Industrial Ethernet in different designs.

### **PNO**

PROFIBUS User Organization e. V.  
Organization for PROFIBUS users and providers

### **PoE**

Power over Ethernet  
Power supply of network devices with low power consumption via the Ethernet cable.

### **PoE+**

Power over Ethernet +  
Power supply of network devices with higher current consumption via the Ethernet cable according to the IEEE 802.3at standard.

### **POF**

Plastic Optical Fiber  
Optical fiber that can be assembled in the field and whose core and jacket are made of plastic.

### **Point to Point Protocol over Ethernet**

→ *PPPoE*

### **Polling**

→ *Polling mode*

### **Polling mode**

The polling mode is a method of data transmission in which a central instance controls the data exchange with the communication partners.

## Polling with time slots

The polling with time slots mode is used in a wireless network in which the use of the radio frequency assigned by the registration authorities must be shared with other users. Each user typically has 6 seconds per minute to exchange data with its stations. The frequency must then be released for other operators. During the allocated time slot, this pooling variant functions like a normal polling system.

## PoP

Point of Presence

Dial-in node of an Internet service provider

## Port

- **Context: Hardware**

Physical connection of an Ethernet switch, a hub, or the Ethernet interface of a device. An Ethernet interface and implemented as a switch has several ports.

- **Context: Network protocol**

Part of the addressing in IP-based networks. A port is used to specify the protocol and services to be used and the assignment of connections for received or sent frames (client/server function) for the operating system. Many port numbers such as the "Well Known Port Numbers" (e.g. port 80 for HTTP) are specified by the Internet Assigned Numbers Authority (IANA).

## Port Locking

Is used to ensure that only frames from authorized stations are forwarded by the OSM/ESM.

## Power budget

This is available between a sender and receiver on a fiberoptic link. It indicates the difference between the optical power coupled into a particular fiber by the optical transmitter and the input power required by an optical receiver for reliable signal detection.

## Power over Ethernet

→ *PoE*

## PPPoE

Point to Point Protocol over Ethernet

Use of the PPP network protocol via an Ethernet connection.

## PPTP

Point-to-Point Tunneling Protocol

Protocol for establishing a Virtual Private Network (VPN). It allows tunneling of PPP through an IP network.

### **Pre-shared Key**

→ *PSK*

### **Pretty Good Privacy**

Program for encryption and for adding a signature to data

### **Primary Setup Tool**

→ *PST*

### **Prioritized startup**

Device-internal functions of SIMATIC NET devices for speeding up the startup of IO devices in a PROFINET IO system with RT or IRT communication. Reduces the time after replacing an IO device until the next IO device is operational.

### **Process and field communication**

Mechanism for transferring process input and process output data between the controller (CPU) and actuators/sensors.

### **Process image**

Special memory area on an automation system. At the start of the cyclic program, the signal states from the process are transferred to the process input image via the input modules. At the end of the cyclic program, the process output image is transferred as a signal state to the output modules.

### **PROFIBUS**

PROcess FieLd BUS

European process and fieldbus standard specified in the PROFIBUS standard (EN 50 170, Volume 2, PROFIBUS). This specifies the functional, electrical and mechanical properties for a bit-serial fieldbus system.

### **PROFIBUS address**

Unique identifier of a node connected to PROFIBUS. To address a node, the PROFIBUS address is transferred in the frame.

**PROFIBUS device**

In PROFINET CBA: A PROFIBUS device has only one PROFIBUS attachment as a slave. The device does not take part directly in PROFINET communication but is linked using a proxy PROFINET device.

**PROFIBUS DP**

PROFIBUS bus system with the DP protocol. DP stands for the German equivalent of distributed I/O. The main task of PROFIBUSDP is the fast, cyclic data exchange between the central DP master and the distributed devices.

**PROFIBUS FMS**

PROFIBUS bus system with the FMS protocol (Fieldbus Message Specification)

**PROFIBUS PA**

Protocol profile based on PROFIBUS DP with intrinsically safe transmission technology complying with IEC 61158-2

**PROFIBUS User Organization e. V.**

→ PNO

**PROFIdrive**

PROFIBUS protocol profile based on PROFIBUS DP, drive technology profile (version 3, isochronous mode)

**PROFIenergy**

PROFIenergy is a data interface based on PROFINET that allows consumers to be turned off during breaks in operation for the purpose of saving energy. The function is coordinated and controlled centrally irrespective of manufacturer or device. The functionality is specified in the "Common Application Profile PROFIenergy, Technical Specification for PROFINET" of the PNO.

**PROFINET**

Open Industrial Ethernet standard of the PNO for automation.

PROFINET defines a communication and engineering model with devices from different manufacturers.

## **PROFINET CBA**

Automation concept for modular system design based on ready-made components. With PROFINET CBA, communication between controllers and intelligent field devices (machine-machine communication) is implemented at the cell level.

## **PROFINET component**

In PROFINET CBA: Software view of a technological module with defined functionality. An automation system is made up of several PROFINET components.

A PROFINET component always includes one or more technological functions and the corresponding device.

## **PROFINET Component based Automation**

→ *PROFINET CBA*

## **PROFINET controller**

A controller that can be both a PROFINET component (CBA) and also supports PROFINET IO.

## **PROFINET device**

In PROFINET CBA: A device on Ethernet. A PROFINET device can also have a PROFIBUS attachment and therefore be a PROFIBUS DP master and proxy PROFINET device for PROFIBUS devices.

## **PROFINET device with proxy functionality**

Proxy for the PROFIBUS devices on Industrial Ethernet. The proxy functionality allows a PROFIBUS device to communicate not only with its DP master but also with all PROFINET communication nodes. If the device has a local (internal) PROFIBUS, it is the DP master for the local slaves.

## **PROFINET IO controller**

IO controller

Exchanges I/O signals with assigned field devices and makes them available to the user program.

## **PROFINET IO device**

IO device

Distributed field device logically assigned to a PROFINET IO controller.



**PROFINET IO supervisor**

PC/PG with commissioning and diagnostics functions in the PROFINET IO environment

**PROFINET IO system**

Consists of a PROFINET IO controller and its assigned PROFINET IO devices.

**PROFINET IO**

Heterogeneous (multiple vendors possible) communications and engineering model for the integration of distributed I/Os in Industrial Ethernet. Distributed field devices are integrated in the communication by PROFINET IO. The IO view of PROFIBUS is retained in which the field devices transfer their IO data cyclically to the process image of the controller.

**PROFIsafe**

Safety profile of PROFINET IO for transmission of standard and safety-oriented data.

**Project view**

In PROFINET CBA: Representation of the assignment between PROFINET components and their instances in the SIMATIC iMAP project.

**Protocol**

A set of rules for transferring data. Using these rules, both the formats of the frames and the data flow are specified.

**Protocol Data Unit**

→ *PDU*

**Proxy**

Representative In networks, for example, it takes on tasks as the representative of subordinate systems or devices, or it takes on tasks for another device as representative.

**Proxy server**

The security in a network can be improved by using a proxy server. Among other things, the software can be used to perform access checks or to deny or grant access to certain pages or documents as is the case with a firewall. A proxy server can also serve as a form of buffer so that Web pages called once do not need to be accessed time and time again via the host. This allows wait times to be significantly reduced in some situations.

**PRP**

Parallel Redundancy Protocol

Redundancy protocol for Ethernet networks to IEC 62439-3. With PRP, frames are sent at the same time via a two separate Ethernet networks. PRP allows bumpless path redundancy without reconfiguration times.

**PSK**

Pre-shared Key

Symmetrical encryption method in which communication partners are given a shared secret key prior to communication.

**PST**

Primary Setup Tool

Software tool with which you can assign an address (for example an IP address) to SIMATIC NET network components, Ethernet CPs and gateways.

**PSTN**

Public Switched Telephone Network

Public communications system for voice traffic between remote subscribers

**PTP**

Point-to-Point Protocol

Works at OSI layers 1 to 3.

**Public Key Infrastructure**

→ *PKI*

**Public key method**

Method that uses the components of a public key infrastructure. See also PKI.

**Publish**

→ *OPC UA PubSub*

**Publisher**

Sender in a ⇒ Publisher-Subscriber system

**Publisher-Subscriber system**

Communication model in which the sender (Publisher) does not send directly to a receiver (Subscriber), but publishes its data classified. One or more subscribers can register for reading published data or data classes.

OPC UA PubSub and some protocols of the cloud communication use Publisher-Subscriber systems.

Depending on the protocol used, communication between Publisher and Subscriber is either direct or by means of interconnected instances. In cloud applications, a broker is usually used as an intermediary instance.

**PVLAN**

Private VLAN

With a private VLAN you can divide up the layer 2 broadcast domain of a VLAN.

**QAM**

Quadrature Amplitude Modulation

Type of modulation in electronic communications engineering that combines amplitude modulation and phase modulation.

**QoS**

Quality of Service

Collective term for various qualities of services.

**QPSK**

Quadrature phase shift keying

Digital modulation technique. With QPSK, two bits can be transmitted per symbol. This doubles the usage of the available transmission speed.

**R&TTE**

Radio and Telecommunications Terminal Equipment Directive

EU directive for telecommunications end devices

**RADIUS**

Remote Authentication Dial-In User Service

Protocol for authenticating users by servers on which user data can be stored centrally. The use of RADIUS servers can increase the protection of user names, assigned roles and passwords.

### **Rapid Roaming**

Roaming with which the node can reestablish the connection so quickly without any noticeable interruption of the connection .

### **Rapid Spanning Tree Protocol**

→ *RSTP*

### **RAS**

Remote Access Service

With the Remote Access Service, you have the option of connecting clients via a modem, ISDN, or X.25 connection to the local area network. Not only different clients are supported but there is also great flexibility in the selection and possible combinations of the network protocols used.

### **RCoax cable**

Coax cable in which the inner conductor is separated from the outer conductor by a dielectric. The outer conductor is interrupted by slits at regular intervals. At these points, a high-frequency signal in the cable is also emitted into the environment of the cable or a high-frequency signal in the environment of the cable is received on the cable, similar to an antenna.

### **Ready Time**

→ *TRDY*

### **Real Time**

→ *RT*

### **Real-Time communication**

→ *RT communication*

### **Received Signal Strength Indication**

→ *RSSI*

### **Reconfiguration time**

Context: OSM

The time required by a device in the redundancy manager mode (or with OSM "Standby") to restore a functional configuration if a device fails or a network cable is interrupted.

**Redundancy client**

Device in a ring topology that reacts to the test and reconfiguration frames of the redundancy manager.

**Redundancy domain**

Group of devices that support the "media redundancy" function in a ring topology. All devices in a ring topology with media redundancy must belong to the same redundancy domain.

**Redundancy manager**

Device in a ring network section with media redundancy that monitors the ring topology. Only one of the two ring ports of the redundancy manager forwards data frames when the ring is closed.

If the ring is interrupted, the redundancy manager triggers a reconfiguration of the network by forwarding data frames via both ring ports. This means that all remaining devices can be reached again (redundancy clients) in the ring over a linear bus.

**Redundant Network Access**

→ *RNA*

**RegTP**

Regulatory authority for telecommunication in Germany

**Remote Access Service**

→ *RAS*

**Remote Monitoring**

→ *RMON*

**Remote status**

Status of the IO data on the communications partner (GOOD or BAD) transferred by the communications partner. Both the output data to be written as well as the input data to be read have a remote status.

Context: PROFINET IO

**Reorganization**

Mechanism with which the logical token ring is reorganized in PROFIBUS.

All the masters on PROFIBUS form a logical token ring. Within this token ring, the token is passed on from node to node. If the transmission of the token is incorrect or if a master is

removed from the ring, this leads to an error when the token is passed on (the token is not accepted by this station). As a result, the station is excluded from the ring. The number of exclusions is counted in the internal token error counter. If this counter reaches an upper limit value, the logical token ring is then reorganized.

### **Repeater rule**

So-called "5-4-3 rule"

Rule that says that on an Ethernet network with shared access in a star topology (10Base2, 10Base5, 10BaseT), a maximum of 5 segments with 4 repeaters can be used and active end devices can only be connected to 3 segments. The repeater also counts as an active end device.

### **RFC**

Request for Comment

Standardization document of the research and development group of the Internet, for example, for definition of protocols, procedures and services.

### **RFC1006**

Request for comment no. 1006

Document of the Internet Engineering Task Force (IETF) to specify the ISO transport service on TCP

### **RFC1213**

Specifies the MIB II that must be supported by all devices that can be managed using SNMP.

### **Ring buffer**

Memory organization so that when the end of the buffer is reached, the recording continues at the start by overwriting the oldest entries.

### **Ring port**

Port of a device that establishes the connection to a neighboring device in a ring topology. A device has exactly two ring ports for the connection within a ring.

### **RIPv2**

Routing Information Protocol version 2

Dynamic, cost-based routing protocol that is specified in RFC 2453. Unlike RIPv1, RIPv2 also supports VLSMs (Variable-Length-Subnet-Mask) and uses broadcast instead of multicast as well as authentication. RIPv2 supports flat networks, there is no way of subdividing them.

**RMON**

Remote Monitoring

RMON-compliant devices allow diagnostic data to be collected on the device and read out by a network management station. This means that network problems are detected early and can be eliminated. The particular advantage of RMON is that it is independent of location. The acquired data can be analyzed at any point in the network with suitable reporting software.

**RMON Agent**

Remote Monitoring Agent

Context: OSM

The RMON agent of the OSM/ESM collects data, for example on network load that can be called up by a network management station when necessary. The OSM/ESM supports the RMON groups Statistics, History, Alarm, Event.

**RNA**

Redundant Network Access

In Siemens Industry, RNA stands for devices and software that support the redundancy protocol "Parallel Redundancy Protocol" (PRP). RNA allows the connection of devices to redundant Ethernet network structures. Some devices of the SCALANCE X-200RNA product line also support the redundancy protocol "High-availability Seamless Redundancy" (HSR).

**Roaming**

Free movement of wireless LAN nodes even beyond the boundaries of the wireless cell of an access point. The node can change from one wireless cell to the next without any noticeable interruption.

**Router**

Active network component that controls the data traffic based on the IP address. Routers have a wide range of filter and security functions.

**Routing Information Protocol version 2**

→ *RIPv2*

**RPC**

Remote Procedure Call

Protocol intended to simplify the implementation of distributed applications. Allows a user program to use a function of a program running on a different computer without needing to bother about the basic network functions. RPC works according to the client-server model.

**RP-SMA**

→ *R-SMA*

**RS-485 repeater**

Device for amplifying bus signals and for linking segments over long distances.

**RSA**

Rivest, Shamir & Adleman Algorithm

Public key method

**R-SMA**

Antenna connector with reversed polarity

**RSSI**

Received Signal Strength Indication

Indicator for specification of the relative device-related received field strength. The value is specified without unit.

See also "CSQ".

**RSTP**

Rapid Spanning Tree Protocol

Layer 2 protocol that allows redundant transmission paths. This prevents circulating frames and, if a fault develops, provides an alternative path within one second (reconfiguration time).

**RT**

Real Time

Real-time communication with PROFINET IO

**RT class**

Group of PROFINET devices with the same real-time properties. Two RT classes are distinguished: RT and IRT.

**RT communication**

Real-Time communication

Transmission mechanism for cyclic exchange of IO data between PROFINET devices. The transmission mechanism guarantees that IO data is transferred at deterministic intervals.



**RTS**

Request to send / Clear to send

Method for avoiding collisions

**S/STP**

Cable design of twisted pair cables with twisted wire pairs that are each wrapped individually with a foil shield. Both individually screened pairs are also shielded with a common braided copper shield.

**S0 interface**

Basic interface of ISDN for connecting end devices

**S5-compatible communication**

→ *Open communication services*

**S7 programming interface for PG/PC - extended for optimized data blocks**

Programming interface for setup of an Ethernet connection that is not configured between PC and S7-1200 (V4 and higher) or S7-1500 over the SIMATIC NET OPC server. The API uses S7 communication over OPC UA and supports access to optimized data blocks (S7OPT-API).

**S7 protocol**

Protocol used for communication with SIMATIC S7 automation systems. It supports both communication between PG/PC and programmable controllers as well as between programmable controllers of the SIMATIC S7 system.

**S7 routing**

PG/OP communication via different networks

**S7 subnet ID**

→ *Subnet ID*

**SAP**

Service Access Point

Service access point

Identification characteristic on the interface between a calling application and the layer providing the service in the OSI layer model. There are specific versions of the term depending on the service that is called.

Example: TSAP (Transport Service Access Point) which identifies a transport service and the calling application.

**SC connectors**

Standardized connectors for glass FO cables

**SC RJ connectors**

Standardized plug-in connector for fiber-optic cable, for example for POF and PCF FO cable

**SCADA**

Supervisory Control and Data Acquisition

Supervisory control system for operator control and monitoring of plants

**SCALANCE**

Scalable Performance

Name of the SIMATIC NET product generation for active Industrial Ethernet network infrastructure components

**Scatternet**

Network structure in Bluetooth in which several piconets are organized.

**SCP**

→ *Pluggable transceiver*

**Screened shielded twisted pair**

→ *S/STP*

**SCT**

Security Configuration Tool

Configuration tool for security products

**SDA service**

Send Data with Acknowledge

Sending of acknowledged services at layer 2 of the OSI layer model.

**SDN service**

Send Data with No Acknowledge

Sending of unacknowledged services at layer 2 of the OSI layer model. (broadcast, multicast).

**Secure Hash Algorithm**

→ *SHA*

**Security**

→ *Industrial Security*

**Security Configuration Tool**

→ *SCT*

**Segment**

TCP frame on the transport layer (OSI layer 4)

**Segmentation**

Disconnection of a faulty segment from an Ethernet network. With this function, network components such as OLMs, ELMs, ASGEs are capable of limiting long-lasting faults to a segment.

**Send buffer**

Memory area in a telecontrol module for triggered frames.

Each value of a data point that is intended for the transmission is stored in a separate frame in the send buffer.

Compare Image memory

Context: TeleControl

**Send Data with Acknowledge**

→ *SDA service*

**Send Data with No Acknowledge**

→ *SDN service*

**SEND/ RECEIVE**

→ *SEND/RECEIVE protocol*

### **SEND/RECEIVE protocol**

Group of protocols that allow simple communications services based on Industrial Ethernet and PROFIBUS for data exchange with SIMATIC S5 and SIMATIC S7 devices.

See also "Open communication services"

### **Serial Baud Rate**

Context: OSM

Transmission speed of the serial interface of the OSM/ESM.

### **Server**

→ *Client-server model*

### **Service Access Point**

→ *SAP*

### **Services**

Services provided by a communication protocol

### **Setup time**

→ *TSET*

### **SFP**

Small Form-factor Pluggable

Small standardized modules for network connections.

### **SFP media module**

Special media module that can be fitted with SFP transceivers.

### **SHA**

Secure Hash Algorithm

Groups of cryptologic hash functions to check the integrity of data:

SHA-0, SHA-1, SHA-2, SHA-3

### **Shared Device**

The "shared device" functionality allows submodules of one IO device to be distributed among different IO controllers to save one or more head modules. To be able to use the

"shared device" function, the IO controller and the shared device must be in the same Ethernet subnet.

### **Shared LAN**

All components in a shared LAN share the nominal bandwidth. Shared LANs are structured with repeaters/hubs.

### **Shield impedance**

Resistance to alternating current of the cable shield. Shield impedance is a characteristic of the cable used and is normally specified by the manufacturer.

### **SIG**

Special Interest Group

User organization for Bluetooth

### **Signal Propagation Delay**

The time required by a data packet on its way through the network.

### **SIM card**

SIM: Subscriber Identity Module

Chip card for identification and authorization of a mobile wireless node in the mobile wireless network

### **SIMATIC iMap**

Engineering tool from Siemens for PROFINET CBA. Allows the configuration, commissioning, and monitoring of modular, distributed automation systems based on the PROFINET standard.

### **SIMATIC iMap - STEP 7 Add-on**

Software for the SIMATIC iMap interface to STEP 7.

### **SIMATIC NCM PC**

Configuration software that allows STEP 7-compatible configuration for SIMATIC NET PC components. Replaces the earlier PC configuration tools COML S7 and COM PROFIBUS PC Edition. The common database with STEP 7 < V10.0 ensures integrated project engineering including all protocols for PC stations.

## **SIMATIC NET**

Siemens SIMATIC Network and Communication. Product name for networks and network components from Siemens.

## **SIMATIC NET Industrial Ethernet**

SIMATIC NET bus system for industrial applications based on Ethernet

## **Simple Network Time Protocol**

→ *SNTP*

## **Simple Object Access Protocol**

→ *SOAP*

## **SINAUT**

Siemens Network Automation

Station control system or telecontrol system based on SIMATIC S7. It works with the SINAUT ST7 telecontrol protocol.

## **SINAUT ST7**

Proprietary telecontrol protocol for SIMATIC NET telecontrol modules

## **SINAUT TD7**

Software for control of ST7 communication of telecontrol modules. TD7 is available in two alternative versions:

- TD7onCPU: Program blocks in the CPU user program
- TD7onTIM: Configurable part of the firmware of the communication module

## **SINEC**

Previous product name for networks and network components from Siemens. New name: SIMATIC NET

## **Single mode**

Transmission form in fiber-optic cables in which transmission takes place by means of a straight mode (wave). Attenuation is mainly caused by physical absorption and dispersion as well as by mechanical bending. The amount of attenuation depends, among other things, on the wavelength of the input light.

**SMI**

Structure of Management Information

A definition for the presentation of the data transferred using SNMP based on Abstract Syntax Notation One (ASN1). SMI describes the syntax of the managed objects and their names and coding.

**SMSC**

Short Message Service Center - SMS center

When sending an SMS message, the message is first sent to the SMSC, buffered there and then forwarded to the recipient.

**SMTP**

Simple Mail Transfer Protocol

Transmission protocol Email

**SMTP server**

Device that received sent E-mails and forwards them to the recipient.

**SNAP**

Subnetwork Access Protocol

Mechanism for multiplexing protocols in networks that use IEEE 802.2 LLC.

**SNMP**

UDP-based open network management protocol for monitoring, diagnostics, control and administration of networks.

**SNMP agent**

Software installed on a managed device that can detect and signal the status of the device. At the request of a manager, the software can also change values on the device.

**SNMP manager**

Requests information about the connected network components and manages it. The SNMP manager can change some values on SNMP agents with write access (SET datagram).

**SNTP**

Simple Network Time Protocol

Standardized protocol for synchronizing clocks in computer systems via communications networks

## **SOAP**

Simple Object Access Protocol

XML-based mechanism for exchanging structured information and rules relating to the data type between computers in a distributed environment.

## **Socket interface**

Interface allowing data communication with computers via TCP/IP. On this interface which is commonly found in the PC and UNIX world, users can program their own protocols.

## **SOFTNET**

Software component for handling communications protocols on SIMATIC NET PC modules.

## **SOFTNET module**

In contrast to HARDNET modules, SOFTNET modules are communications processors with which the major part of protocol processing is performed on the PC.

## **SOHO**

Small Office, Home Office

Private and small business IT users

## **Source NAT**

NAT method in which a source IP address in the source network is replaced with a different source IP address in the destination network.

## **Spanning Tree Protocol**

→ STP

## **Spoofing**

Methods for undermining authentication and identification procedures based on trustworthy addresses or host names. In IP spoofing, for example, a falsified source IP address is used.

Anti-spoofing describes mechanisms to discover or prevent spoofing.

## **Squelch function**

Squelch



Squelch reduces the interfering noise in communications during breaks in transmission. This increases the signal-to-noise ratio.

**SRS**

Siemens Remote Services

Service portfolio of Siemens AG for establishing secure connections between customer networks and the Siemens Remote Service platform.

See: (Page )

**SSH**

Secure Shell

Network protocol or corresponding computer program for secure creation of an encrypted, interactive network connection with a remote device. It provides the user with the same options as a direct connection to the device via a terminal.

**SSID**

Service Set Identifier

Name of a WLAN network that must be known to all network nodes at the same time and that forms part of every transferred message. Hiding the SSIDs alone provides only very weak access protection against third parties and must always be supplemented by other encryption methods (WPA2).

**SSL**

Secure Sockets Layer

Protocol for encrypted data transfer on the Internet.

As of SSL version 3.0: "TLS" (Transport Layer Security), see also TLS.

**SSL certificate**

Certificate according to the X.509 standard with the enhancement "Server authentication"

**SSL connection**

Secure Sockets Layer (SSL) - former name of Transport Layer Security (TLS)

The SSL protocol is located at the transport layer (OSI layer 4) above TCP and is used for a secure transaction. With SSL, the user is sure that it is connected to the required server (authentication) and that the sensitive data is transferred over a secure (encrypted) connection.

## **SSN = DMZ**

Secure Server Net = Demilitarized Zone

## **ST connector (ST = Straight Tip)**

→ *BFOC*

## **Standard mounting rail**

Metal rail standardized in compliance with EN 50 022. The standard mounting rail is used for fast snap-on mounting of suitably equipped devices.

## **Standby**

Context: OSM

Procedure for redundant linking of multiple subnets with a fast reconfiguration time < 300 ms

## **Standby Cable**

Context: OSM

Connecting cable (ITP XP standard cable 9/9) for linking the standby master and standby slave in the redundant link.

## **Standby sync port**

Context: OSM

Port of an OSM/ESM via which two OSMs or ESMs are connected together in the redundant ring link so that they can inform each other of their operating states (does not exist on the OSM TP22 and ESM TP40).

## **Stateful packet inspection**

Firewall technology that generates firewall states for permitted frames. Firewall states automatically permit the responses to permitted frames.

## **Station**

Station in an automation system usually a SIMATIC station with CPU, I/O modules and often with communications modules.

## **Station Configuration Editor**

Denotes the accessible user interface of the software for PC stations known as the station manager; the Station Configuration Editor allows access to the component management of

the PC station. Here, components are the modules and the applications of a PC station involved in communications.

### **Stationmanager**

PC application that allows a PC to be configured in a similar way to an S7 station and to download this via a network. The station manager is the basic component for the configuration and runtime of OPC applications of SIMATIC PC stations.

### **STEP 7 project**

Set of data containing the configuration data that can be downloaded to S7 stations, switches, PC stations etc.

### **Store and forward**

Context: OSM

In this switching technique, used by the OSM/ESM, the entire frame is read in before it is forwarded by the switch. A frame is only passed on if it is error-free.

### **STP**

Spanning Tree Protocol

The spanning tree method allows network structures to be created in which there are several connections between two IE switches/bridges. Spanning tree prevents loops being formed in the network by allowing only one path and disabling the other (redundant) ports for data traffic. If there is an interruption, the data can be sent over an alternative path. The functionality of the spanning tree algorithm is based on the exchange of configuration and topology change frames.

### **STP**

→ *Pluggable transceiver*

### **Strict Queueing**

Processing scheme which specifies the order in which the frames are processed in a queue. As long as there are frames with high priority in the queue, only the high-priority frames are processed.

### **Structured cabling**

Application-neutral cabling of building complexes for IT purposes. The European standard EN 50173 "Generic cabling systems" divides up a location into areas as follows:

- Primary area (interconnection of buildings of a campus)
- Secondary area (interconnection between floors of a building)
- Tertiary area (information technology connections for the end devices)

EN 50173 recommends cabling systems suited to these areas that can also meet the communication requirements of the future flexibly and independent of any specific application.

## Subnet

Part of a network delineated from the total network by suitable devices, for example gateways. The subnet includes bus components and all the attached stations. Parameters within a subnet (for example with PROFIBUS) must normally be matched up.

A system usually consists of several subnets with unique subnet numbers. A subnet consists of several nodes with unique PROFIBUS or MAC addresses (Industrial Ethernet).

## Subnet ID

Address parameters of an S7 subnet

Based on the S7 subnet ID, a node can be uniquely assigned to a subnet. Based on the subnet ID, a router recognizes whether a target address is inside or outside the subnet. The subnet ID is still an address parameter of S7 connections.

The S7 subnet ID consists of two parts: Project number - subnet ID

## Subnet mask

The subnet mask specifies which part of the IP address is used as the subnet address. With a class B network (subnet mask 255.255.0.0), the first two fields of an IP address (e.g. 192.168 of the IP address 192.168.017.009) represent the subnet.

## Subnet number

→ *Subnet ID*

## Subscribe

→ *OPC UA PubSub*

## Subscriber

Receiver in a ⇒ Publisher-Subscriber system

## Suppressor

Component for reducing induced voltages. Induced voltages occur when circuits with inductances are turned off.

**Switch**

Network component that basically has the same properties as a bridge. In contrast to the bridge, the switch can, however, establish several connections between the ports at the same time. These connections are established dynamically and temporarily depending on the data traffic.

**Switching**

Simultaneous establishment of several connections between the ports. These connections are established dynamically and temporarily depending on the data traffic.

**SWR**

Standing Wave Ratio

Ratio between the energy radiated by the antenna to the energy that the antenna reflects to the wireless module

**SYNC mode**

The SYNC mode is a DP mode in which one, several (group) or all DP slaves transfer data to their process outputs at a certain time. The time at which the data is transferred is indicated in the SYNC command (a control command for synchronization).

**Syslog**

Service on a server (Syslog server) that receives system messages and, for example, records them in log files.

**TACACS**

Terminal Access Controller Access Control System

AAA protocol used for client-server communication between AAA servers and a Network Access Server (NAS). TACACS servers provide a central authentication instance for remote users that want to establish an IP connection to an NAS.

**Target Rotation Time**

→ *TTR*

**TCP**

Transmission Control Protocol

Protocol for connection-oriented data transmission in networks; it belongs to the family of Internet protocols. In the OSI layer model, the protocol operates at layer 4.

## **TCP/IP**

Transmission Control Protocol / Internet Protocol

The name of a collection of protocols that due to their great significance for data transmission in heterogeneous networks are also known as the Internet protocol family. In the OSI layer model, these protocols operate at layer 3 (IP) and layer 4 (TCP).

## **TCSB**

→ *Telecontrol server*

## **TD7onCPU / TD7onTIM**

→ *SINAUT TD7*

## **TDMA**

Time Division Multiplex Access

Time slot-controlled access method

## **Technological Functions**

→ *TF*

## **Telecontrol server**

PC for monitoring and control of remote S7 stations linked via Internet or a mobile wireless network. The telecontrol server is normally a centrally deployed PC with a connection to the Internet on which the "TELECONTROL SERVER BASIC" (TCSB) application is installed. The telecontrol server is not configured in STEP 7.

## **TeleService**

TeleService enables central management, control and monitoring of distributed plants through remote connections. Setup of a remote connection with TeleService requires a TS Adapter or a telecontrol CP.

## **TeleService gateway**

PC in the network as intermediary between the engineering station and remote S7-1200 with mobile wireless CP. The "TS Gateway" software is installed on the PC. TS Gateway is used only for the "TeleService" function via mobile wireless. No process data can be transferred with TS Gateway. The TeleService gateway is not configured in STEP 7.

## **TeleService server**

Switching station for data transmission between the engineering station and remote S7 station. This can be a telecontrol server or a TeleService gateway.

**TELNET**

Protocol with which an interactive connection can be established to another device in the LAN or on the Internet. The user then has the same options as when directly connected to this device with a terminal.

**Termination**

→ *Terminator, active*

**Terminator, active**

Terminating resistor for bus segments at transmission rates of 9.6 kbps to 12 Mbps (PROFIBUS). The power supply is separate from the bus nodes.

**TF**

Technological Functions

Application layer 7 in Industrial Ethernet (contains user services)

**TFTP**

Trivial File Transfer Protocol

Simple, UDP-based protocol for transferring files.

**TIM**

Telecontrol Interface Module

Communication module that handles all data transmission functions provided by the SINAUT system independently.

**TKIP**

Temporal Key Integrity Protocol

Security protocol for cyclic key changing in wireless LAN.

**TLS**

Transport Layer Security

Protocol for encrypted data transfer on the Internet. TLS is used, among other things, during data transfer using HTTPS.

**Token**

Frame that represents the right to transmit in a network. It signals the two states "occupied" or "free". The token is passed from active node to active node.

### **Token passing**

Collision-free access method: the right to send (token) circulates between the nodes forming a logical ring

### **Token ring**

Logical arrangement of masters in a bus system. All masters physically connected to a bus receive the token and pass it on to the next master in the token ring.

### **Token rotation time**

Time that elapses between receiving the token and receiving the next token.

### **Topology**

Structure of the networking of multiple devices in a network. The most important basic forms are linear bus, tree and star. Combinations of all basic types are possible.

### **TP**

Twisted Pair

Data cables with pairs of twisted wires. By twisting the pairs of wires, electromagnetic interference has opposing effects in the individual twists and cancels itself out in the difference signal. Twisted-pair cables are available in a variety of qualities for different transmission speeds.

### **TP Cord**

Twisted-pair cable for short connections that complies with category 5. Used in a cabinet or in an office environment with low EMC interference levels.

### **TP port**

Port with a TP connector (RJ45 jack)

### **TPC**

Transmit Power Control

Function for control system of the transmit power according to IEEE 802.11h. The transmit power of nodes is reduced until the minimum for reliable transmission with the configured transmission speed has been reached.

### **Transmission Control Protocol**

→ *TCP*



**Transmission Control Protocol / Internet Protocol**

→ *TCP/IP*

**Transmission rate**

Number of frames transferred per second

**Transport interface**

Access to the connection-oriented services of the transport layer, layer 4 in the ISO/OSI reference model.

**Transport layer**

Layer 4 of the ISO/OSI reference model for open system interconnection. The purpose of the transport layer is to transfer data (raw information) reliably from device to device.

**Transport Service Access Point**

→ *TSAP*

**Trap**

SNMP datagram that is formed due to an event.

**TRDY**

Ready Time

Bus parameter for PROFIBUS. Indicates readiness to acknowledge or respond.

**Triaxial cable**

The SIMATIC NET LAN cable 7270 is based on the coaxial cable specified in the IEEE 802.3: 10BASE5 standard but with a solid aluminum shield and outer sheath making it more suitable for industrial application.

**Triple A concept**

→ *AAA*

**Trivial File Transfer Protocol**

→ *TFTP*

**TS Gateway**

Application on a TeleService gateway

**TSAP**

Transport Service Access Point

Access point of a communications connection on ISO layer 4 (transport connection)

**TSET**

TSET

Setup time

Bus parameter for PROFIBUS. Minimum interval on the sender between receiving an acknowledgment and sending a new call frame.

**TSL**

Slot Time

Slot time, bus parameter for PROFIBUS.

Time during which the sender of a frame waits for the acknowledgment from the receiver.

**TTR**

Target Rotation Time

Target rotation time

Bus parameter for PROFIBUS. Each master compares the target rotation time with the actual token rotation time. The difference between the two decides how much time the DP master took to send its own data frames to the slaves.

**Tunnel**

Connection over a protocol that embeds the data of another protocol.

**Twisted Pair**

→ *TP*

**UDP**

User Datagram Protocol

Datagram service for simple and data transfer beyond the boundaries of a network without acknowledgment.

**UDP connection**

Connection type that can be configured in STEP 7

To be able to transfer SIMATIC S7 UDP datagrams, UDP connections need to be configured. This provides the address information and system resources required for the transfer. However, as UDP is a connectionless service, no explicit connections are established between the communication partners during operation. The datagrams are sent without any prior connection establishment based on the configured information.

**UL**

Underwriters Laboratories

Accredited test laboratory for certification

**UMTS**

Universal Mobile Telecommunication System

Mobile wireless standard of the 3rd generation (3G). UMTS allows significantly higher data transmission rates than the GSM networks of the 2nd generation so that, for example, video applications can also be transferred.

**Undersize telegram**

Context: OSM

Frames with a length less than 64 bytes.

**Underwriters Laboratories**

→ *UL*

**UNFREEZE**

Job for resetting the FREEZE mode.

**Unicast address**

A frame with a unicast destination address is intended for precisely one node with the corresponding MAC address.

**Uniform Resource Identifier**

→ *URI*

**UNII**

Unlicensed National Information Infrastructure

Name of the 5 GHz band in U.S. literature.

**Universal Time Coordinated**

→ *UTC*

**UNSYNC**

Job for resetting the SYNC mode.

**Upstream**

Communication from node (client) to access point.

**URI**

Uniform Resource Identifier  
Address of a document on the Internet

**URL**

Uniform Resource Locator  
Address of a document on the Internet

**UTC**

Universal Time Coordinated  
A reference time with worldwide validity based on international atomic time.

**UTRAN**

UMTS Terrestrial Radio Access Network  
Wireless access networks to the mobile wireless network according to the UMTS standard.

**VACM**

Viewbased Access Control Model  
Defines views with access rights to the object tree that can be assigned to users.  
The SNMPv1/v2 read/write community represents 2 views with read or write permission.

**Variable**

Context: OPC  
Placeholder for a value obtained at the time required.

This might be the value of a sensor, control parameter, status information, or the status of the network connection. Examples of variables: The value of a sensor, control parameter, status information, or the status of a network connection.

**Variable services**

Application service group, it provides services for processing variables

**VFD**

Virtual Field Device

Substitute object for a device at the field level

**Virtual Private Network**

→ *VPN*

**VLAN**

Virtual Local Area Network

A virtual network structure that can connect distributed LANs and the nodes connected to them. The nodes communicate with each other as if they were in the same physical LAN. Switches with VLAN capability handle the distribution and delivery of the data frames.

**VLAN identifier**

An Ethernet packet has a VLAN identifier if a field in the Ethernet packet header (EtherType) has a certain value. In this case, the Ethernet packet header contains information on a virtual LAN and possibly also a packet priority.

**VNS**

Virtual Network Services

The organization of logical networks within one or more physical networks.

**VoIP**

Voice over IP

Transmission of telephone calls via IP-based networks.

**VPN**

Virtual Private Network

Technology for secure transportation of confidential data in public IP networks, for example the Internet.

## **VRID**

ID of a virtual router.

## **VRID tracking**

With this function all interfaces of a VRID are monitored.

When the status of an interface changes from "connected" to "not connected", the priority of all VRRP interfaces with the same VRID is reduced to the value "0".

When the status of an interface changes back from "not connected" to "connected", the original priority of the VRRP interfaces is restored.

## **VRRP**

Virtual Router Redundancy Protocol

Mechanism for increasing the availability of important gateways in local area networks by using redundant routers.

## **VSWR**

Voltage Standing Wave Ratio

Ratio of the effective voltages of the outgoing and returning waves in a electrical cable, a measure of transmission losses. Under ideal conditions the entire power from the source is transmitted to the receiver without loss. Incorrect termination leads to reflection of the electromagnetic waves and therefore to losses. An unsuitable termination may be a resistor that does not correspond to the cable impedance or a second connected cable with a different impedance, for example an antenna.

VSWR = 1 means no losses (but also practically no radiation of power of an antenna).

VSWR =  $\infty$  means total reflection.

## **WAN**

Wide Area Network

Network covering a wide area.

## **WAN, classic**

Includes SINAUT communication via dedicated lines (private or leased), private wireless networks, analog telephone network, digital ISDN network and mobile wireless networks (without Internet).

## **WAN, IP-based**

Includes IP-based telecontrol communication via wireless, fiber-optic cables, public networks and the Internet using services such as DSL, GPRS or UMTS or via broadband systems such as OTN and PCM30.

**Watchdog**

Mechanism for monitoring whether or not a function can be used

**Watchdog time**

A monitoring time that can be set on a DP slave to detect failure of the assigned DP master

**WBM**

Web Based Management

Web pages integrated in SIMATIC NET devices for configuration and diagnostics using a Web browser. Entries are sent to the device using HTTP or HTTPS and passed on to the user by the device.

**WCDMA**

Wideband CDMA

Multiplex method for high transmission speeds.

**WDS**

Wireless Distribution System

Directional radio links for connecting access points for an extended service set (ESS).

**Web Based Management**

→ *WBM*

**Web browser**

Program for displaying Web pages

**Web pad**

Portable device in A4 size with touch screen for Internet use.

**Web server**

Program that provides information using HTTP.

**WECA**

See WiFi Alliance.

## Weighted Fair Queueing

Processing scheme which specifies the order in which the frames are processed in queues. Even if there are frames with high priority in the queue, frames with a lower priority are also processed during queueing.

## WEP

Wired Equivalence Privacy

Optional part of the IEEE 802.11 standard. WEP specifies a mechanism for authentication and encryption, whereby both partners use a fixed key stored on the device. All devices that want to access the network in which WEP is used, must therefore first be supplied with the same keys. WEP works with key lengths between 40 and 128 bits. Key lengths that differ from this size are occasionally found (for example 256 bits) but these are not included in the vendor-independent WLAN standards IEEE 802.11b and 802.11g. The key can only be renewed manually.

## WHART

→ *HART Version 7*

## Wi-Fi

→ *Wireless Fidelity*

## Wi-Fi Alliance

Alliance of manufacturers of wireless LAN products (formerly WECA) that guarantees compatibility of its devices.

Compatible devices are identified by the WiFi seal.

## Wi-Fi seal

→ *Wi-Fi Alliance*

## Wired LAN

Wired local area network

## Wireless Fidelity

Wireless Fidelity

Product certificate for wireless power supply; see also Wi-Fi Alliance.

## Wireless LAN

→ *WLAN*



**Wireless Sensor Network**

→ *WSN*

**WirelessHART**

→ *HART Version 7*

**WLAN**

Wireless LAN

Wireless network

**WLANA**

Wireless LAN Association

Company consortium of wireless LAN providers to promote wireless LAN technology in the network market.

**WMM**

Wireless Multimedia Extensions

Part of the IEEE 802.11e standard

**WPA**

Wireless Protected Access

A temporary security mechanism from WECA that closes existing security gaps in WEP. Here the AES encryption method is used. It will be superseded by IEEE 802.11i.

**WPA2**

Wireless Protected Access 2

Improved and expanded WPA method

**WSN**

Wireless Sensor Network

Wireless sensor network with WirelessHART devices.

**X.25**

Interface between end device and data transmission equipment for any devices operating in packet mode in public data networks and via permanently switched cables.

**X.509 certificate**

International standard for the creation of digital certificates for public key infrastructures.

**XTI**

UNIX Transport Layer Interface

Layer 4 transport layer, standardized in UNIX.

**Yellow Cable**

Coaxial cable type PG 8 with an impedance of 50 ohms. The Ethernet standard specifies a yellow color, hence "yellow cable". The ends must be terminated with terminating resistors.