Security with SIMATIC NET

Industrial Security

Overview, Security-Configurations, Background Information • March 2010

Industry Automation and Drives Technologies Service & Support Portal

This article is taken from the Service Portal of Siemens AG, Industry Automation and Drives Technologies. The following link takes you directly to the download page of this document.

http://support.automation.siemens.com/WW/view/en/27043887

If you have any questions concerning this document please e-mail us to the following address:

online-support.automation@siemens.com

S

SIMATIC
Security

Security with SIMATIC NET

Warranty and Liability

Note The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these application examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of Siemens Industry Sector.

Table of Contents

1 Problems of secure data transmission

Introduction

There are currently two major trends in industrial automation:

- wireless data transmission
- security of networks in production.

The security issue is of primary importance since industrial Ethernet solutions and numerous unsecured interfaces are on the rise. The use of standard components from information technology and the advance of Ethernet-based communication standards create vulnerabilities unknown in the physically islanded automation systems used in the past.

Aspects of data security

Data security is basically divided into three major aspects:

- **Confidentiality**
  It must be ensured that the information is not disclosed to any unauthorized third persons during the transmission.
- **Integrity**
  It must be ensured that the information can not be changed unnoticed during the transmission. The system must be laid out so as to reveal any modifications.
- **Authenticity/Authorization**
  It must be ensured that the identity of all systems involved in information transmission can be proved without doubt. It must not be possible for third persons to feign identities.

2 Explanation of terms and basic technologies

As the industrial Ethernet and PROFINET are finding their way into production, IP mechanisms and protocols, too, are advancing into the world of automation.

This chapter introduces the basics of data transmission, names the most common protocols and explains important terms.

2.1 Address assignment

Each system connected to an Ethernet network is clearly specified by a MAC address. This MAC address consists of 6 bytes. The first three bytes specify the manufacturer; the last three bytes are assigned consecutively by the manufacturers. The notation is usually hexadecimal.

$$\underbrace{\mathbf{00 \quad 08 \quad 06}}_{\text{Specifies the manufacturer (here: Siemens}} \quad \underbrace{\mathbf{FA \quad CE \quad 36}}_{\text{Assigned consecutively by the manufacturer}}$$

An IP address is assigned to each MAC address depending on the network structure. The IP address consists of 4 bytes and is represented in dotted-decimal notation (four numbers separated by dots):

157.163.232.240

2.2 Transmission protocols

The protocols used in an industrial Ethernet are from the IP protocol suite. They are divided into connection-oriented TCP protocols and connectionless UDP protocols.

The IP protocols owe their development to the fact that for a long time there were no official standards available for integrating different computers in one network. In the early 70ies, the US Department of Defense ordered one of its departments to develop and define a communication protocol for connections and data exchange in manufacturer-independent, heterogeneous computer networks.

The packet-oriented Wide Area Network ARPAnet was the experimental platform used for first tests with these communication protocols. The protocol specifications were written down and published in the form of Request for Comments (RFCs).

Once the development was finished, the US Department of Defense declared TCP/IP as its standard communication protocol in the early 80ies. Many of the RFC were taken over unchanged as military standards.

The civil breakthrough of TCP/IP came with the first implementation into the 4.2BSD UNIX system. This source code was later made publicly available as PublicDomain software by the University of Berkley. Shortly afterwards, all UNIX systems took over TCP/IP and other operating systems jumped on the bandwagon.

2.3 Firewalling

Firewalling describes the process of filtering the data traffic using information in the header of the data packet. The header includes information about the sending/receiving party, the transmission protocols used etc.; the actual data follow afterwards. Data traffic can be filtered according to:

- MAC addresses
- IP addresses
- Communication protocols
- Additionally, it can be checked whether the communication protocols used are correct syntactically.

2.4 Encryption

Encrypting the data to be transmitted ensures the confidentiality and the integrity during data transmission. The most common encryption methods are:

- IPSec
- WPA
- WEP
- SSL

This requires systems to be installed on the sending and receiving side which are capable of encrypting and decrypting the data packets. Such systems can come as hardware (e.g. SCALANCE S612/613) or as software (e.g. SOFTNET Security Client).

3 Scenarios

Content

This section presents individual security scenarios which show the relationship between what is **needed** and how this can be **solved in practice** using SIMATIC NET security components.

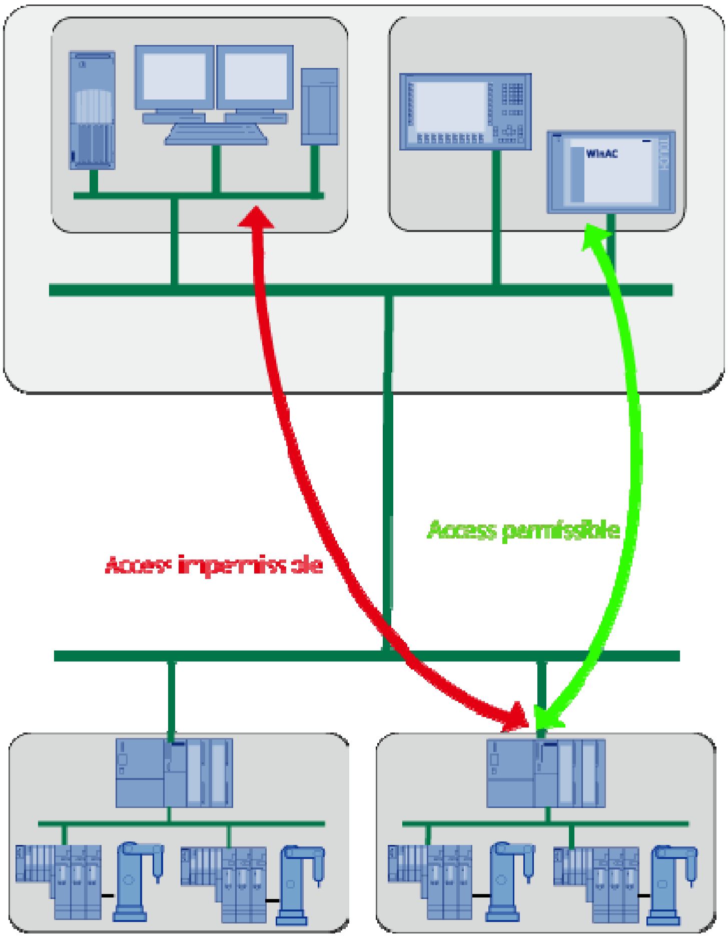
These scenarios can be divided into the following main categories:

- Restricting communication in plants
- Secure data communication over non-secure networks
- Secure communication via WLAN

3.1 Node restriction on S7 controls

Network topology

Figure 3-1



Use case

The S7 controller is connected to a network via an Ethernet CP. This network has several nodes. But only some nodes should be allowed access to the S7 controller.

Problem

The network itself does not have a protection mechanism against unauthorized access to the S7 station. Therefore, the S7 can be accessed from any configuration station using STEP 7 and its configuration can be changed. This unauthorized access could lead to the S7 being sabotaged.

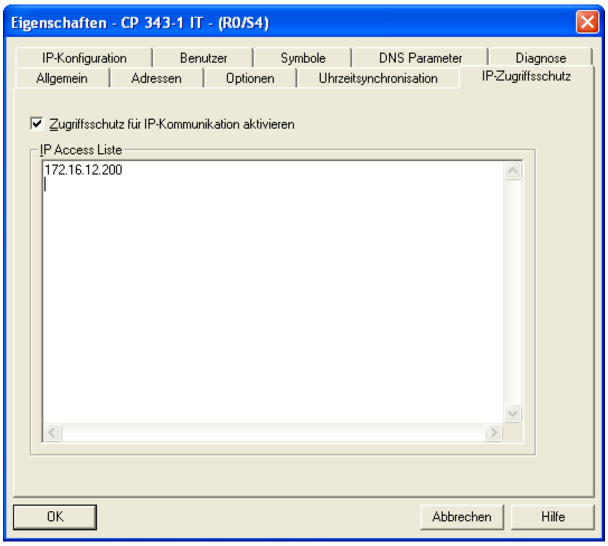
Possible solutions using SIMATIC NET components

There are two possible solutions:

- Protection in the end device through IP addresses
- Protection through segmentation using VLANs
- Protection through authentication

Protection in the end device

Figure 3-2



Eigenschaften - CP 343-1 IT - (R0/S4)

☑ Zugriffsschutz für IP-Kommunikation aktivieren

IP Access Liste

172.16.12.200

To prevent unauthorized access to a S7 station, an Ethernet communication processor (e.g. CP 443-1) is used as network connection on the S7 side. The CPs can be configured to give only selected IP addresses access to the S7 station via Ethernet.

The required configuration and settings are made via the STEP 7 HW Config in the CP properties. The IP access protection tab contains an editable list where all IP addresses can be entered which are allowed to access the S7 station.

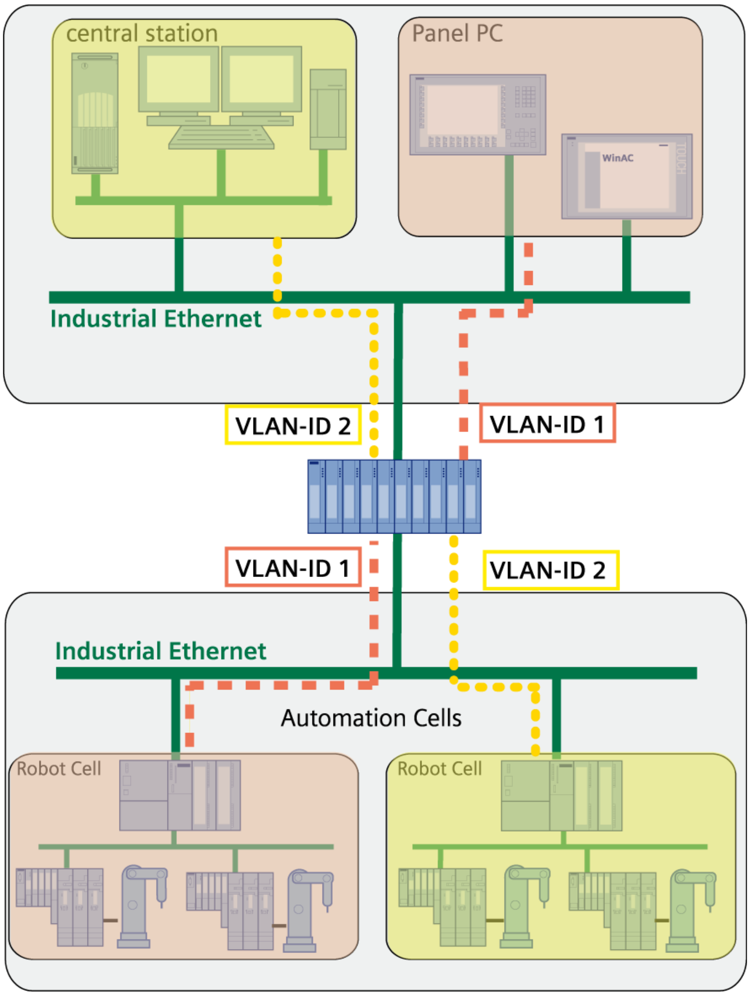
The following modules support this functionality:

Table 3-1

Module	MLFB	Firmware version
CP 343-1 IT	6GK7 343-1GX20-0XE0	V1.0 and higher
CP 343 -1 Advanced	6GK7 343-1GX21-0XE0	V1.0 and higher
CP 343-1	6GK7 343-1EX21-0XE0	V1.0 and higher
CP 343-1	6GK7 343-1EX30-0XE0	V2.0 and higher
CP 443-1	6GK7 443-1EX10-0XE0 6GK7 443-1EX11-0XE0	V2.3 and higher
CP 443 -1 Advanced	6GK7 443-1EX40-0XE0 6GK7 443-1EX41-0XE0	V1.0 and higher

Protection through “segmentation”

Figure 3-3

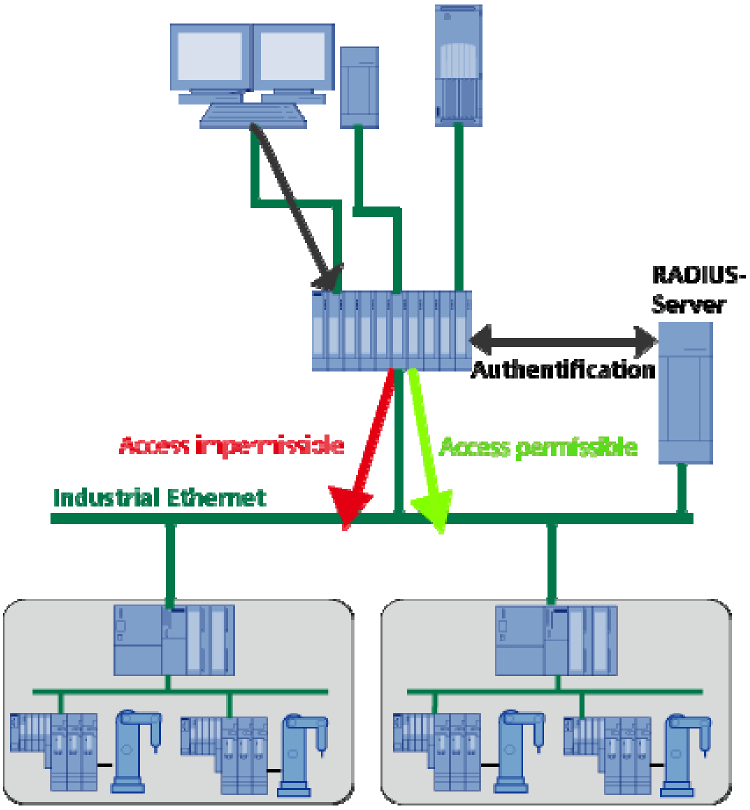


Another way of fending off unauthorized access to an S7 controller is to use a SCALANCE X-400 or X-300 switch by parameterizing VLANs.

This method uses the web-based management to assign a so-called VLAN-ID to the individual ports of a switch. Communication is then only possible within a VLAN (ports with the same VLAN ID). This means that both the configuration station and the S7 station must be on switch ports with the same VLAN ID.

Protection through authentication

Figure 3-4



The SCALANCE of the X-300 and X-400 series supports **IEEE 802.1x**. This standard is a method for authentication in networks.

The authentication of an end device is accomplished by the authenticator which can be activated or deactivated individually for **each** port via the web-based management.

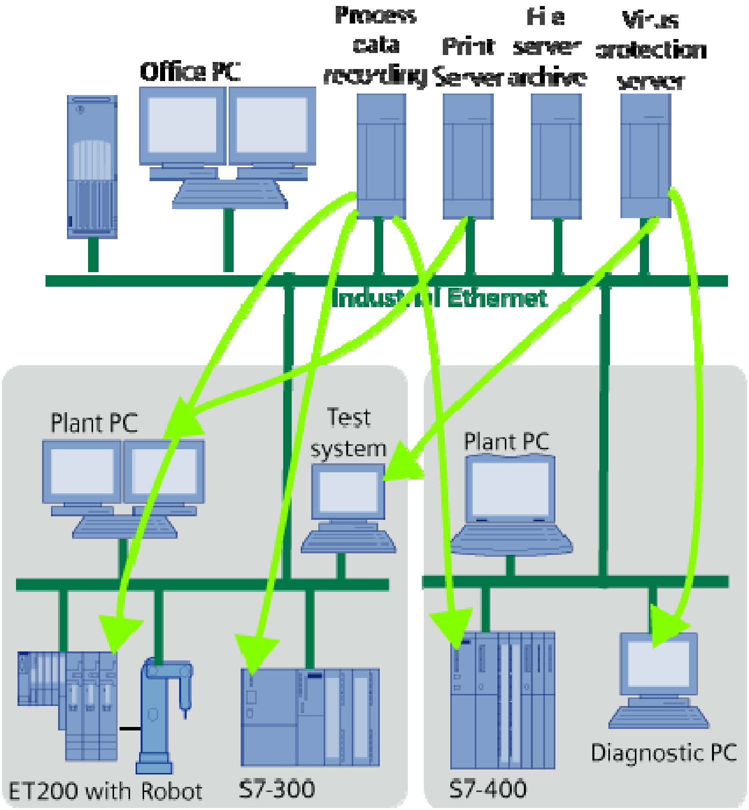
The authenticator uses an authentication server (RADIUS server) to verify the log-in data transmitted by the end device. If these data match the data stored on the RADIUS server, the end device is granted access to network behind the SCALANCE via this port; if not, access is denied.

This standard requires both the RADIUS server and the end device to support the EAP protocol (Extensive Authentication Protocol).

3.2 Function restrictions in plants / single devices

Network topology

Figure 3-5



Use case

A network often accommodates several nodes with different functions.

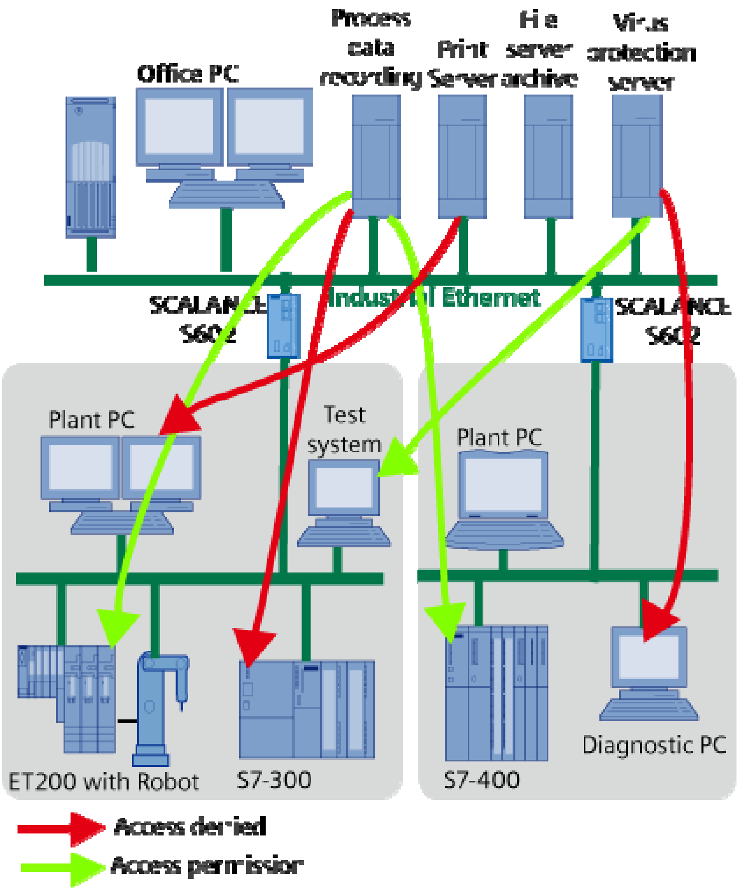
Each single device or cell is to be equipped with a fire wall to restrict access to that device or internal devices so that only certain applications are available to selected nodes.

Problem

These functionalities are often tied to specific protocols (e.g. the S7 protocol for the S7 configuration, IP address assignment with DCP, WBM via HTML). The problem is now that no filtering according to certain protocols is done within the network and therefore all nodes can access all applications.

Possible solution using SIMATIC NET components

Figure 3-6



The **SCALANCE S602** module can be used for cell protection in this case besides the SCALANCE S612/S613 security modules. It provides the same **firewall functionality** as the SCALANCE S612/S613, but it does not have a mechanism for VPN!

A SCALANCE S602 module is used to connect the cell to the remainder of the network. A filter is configured for the protocol to be blocked to prevent that certain protocols spread throughout the entire network restricting them instead to the one cell in question.

By filtering on PROFINET-DCP (for identifying all Profinet nodes), we achieve that only the nodes within the cell and not those of the entire network are displayed.

3.3 Bandwidth restriction

Use case

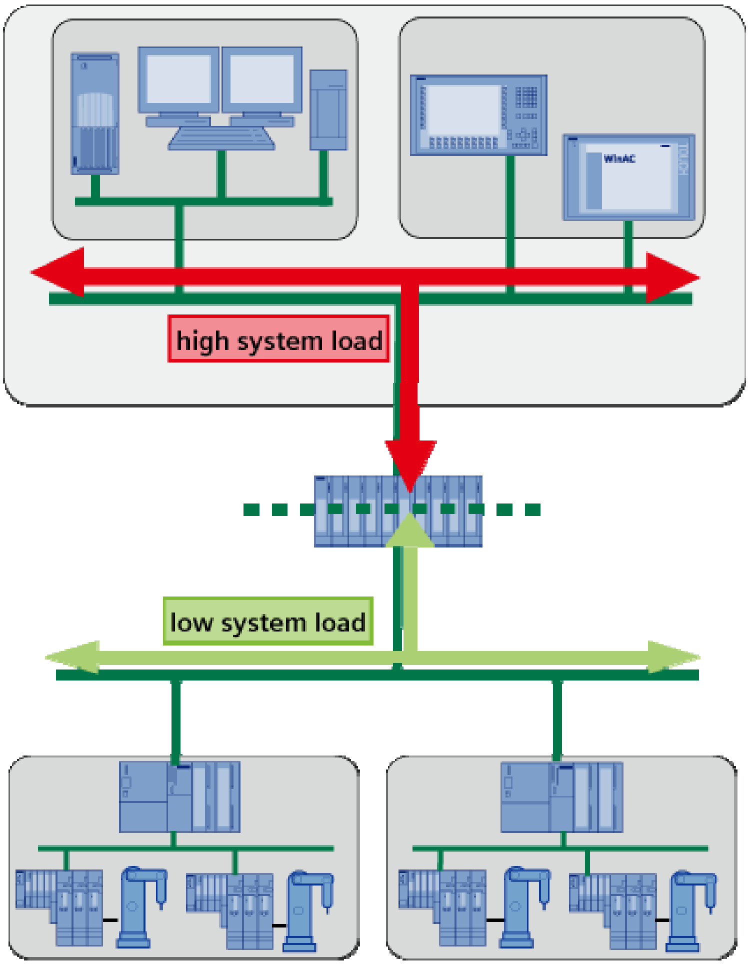
It is often the case that automation cells are connected with one another by a superior network. System load occurring in that network (e.g. broadcasting storm) must not have any impact on the single stations.

Problem

The network itself does usually not have any filter functions for such overload conditions. As a consequence, a broadcasting storm, for instance, would be forwarded into all cells causing the connection between all communication partners within that cell to be aborted. Data exchange would come to a stop.

Possible solutions using SIMATIC NET components

Figure 3-7

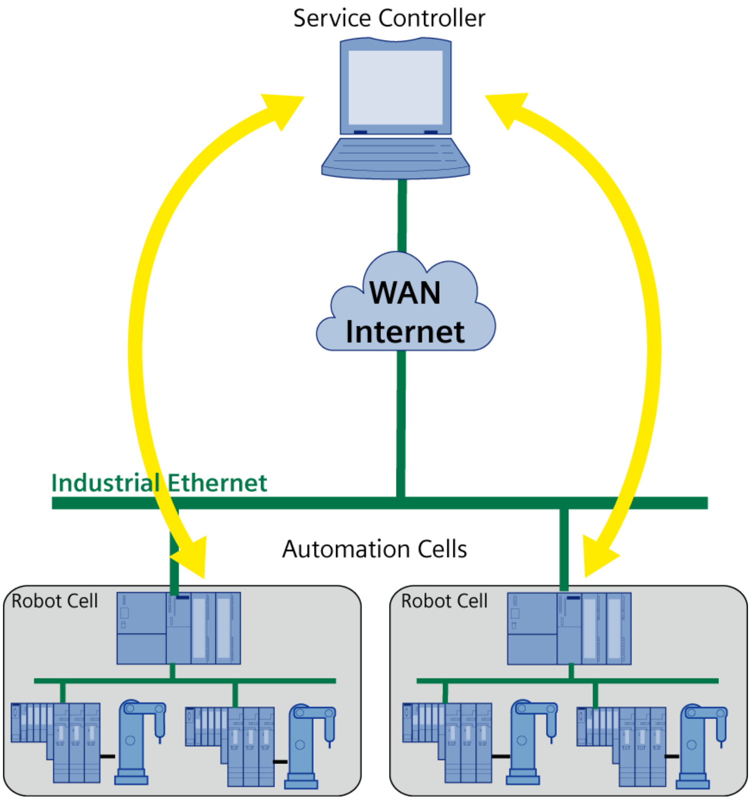


The easiest way to prevent network loads from spreading is by installing a **load limiting device** at the connecting point between a cell and the network. A load limiting device can be either a **SCALANCE X-400** or **X-300** switch or a **SCALANCE S** module in which bandwidth limitation is activated. If now a high load occurs in a network, data exchange can proceed without difficulties inside the cell.

3.4 Secure remote access via Internet

Network topology

Figure 3-8



Use case

It is often desired that a service technician connects to a production network from a remote location in order to obtain access to the stations (e.g. S7 etc.) connected in the network. Once connected to the network, he can, for instance, load new programs into an S7 controller or update firmware.

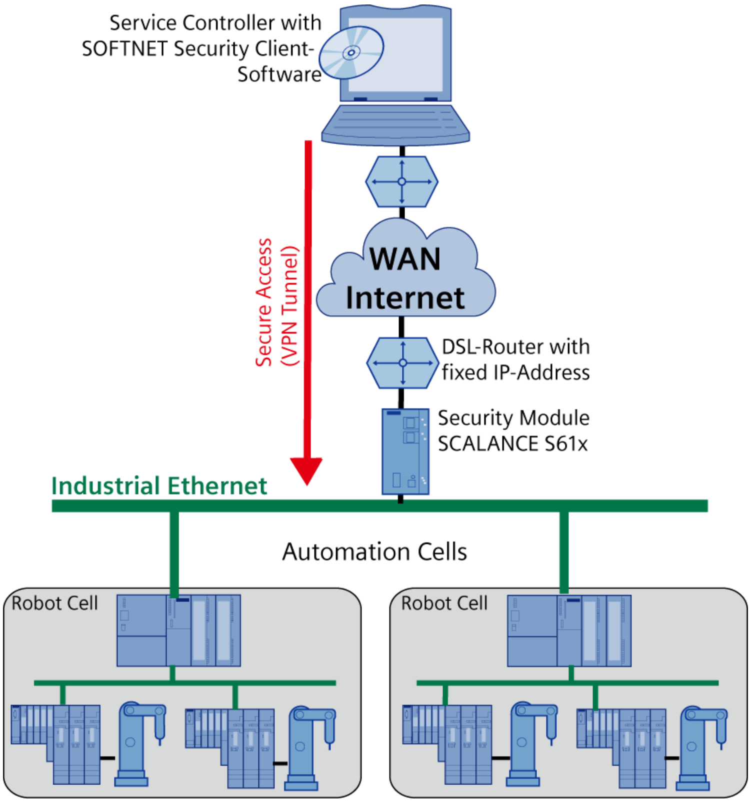
Since a higher performance is expected today, an Internet connection is preferred to a modem solution. This has the additional advantage that technicians around the world can connect to a network at lower costs than with the modem solution.

Problem

Two aspects related to data security are of major interest in this scenario. Firstly, it is important that data transmitted over the Internet are encrypted to prevent their being read by third persons. Secondly, it is essential that only the service staff is given access to the system.

Possible solutions using SIMATIC NET components

Figure 3-9



When considering the two data security aspects, remote access of a service technician to an automation network requires a **software solution** to be implemented on the technician’s side and a **hardware** approach on the network side.

A configuration tool is used to configure the SIMATIC NET **Softnet Security Client** software installed on a service PC and the **SCALANCE S61x** module on the network side so that each constitutes an end point of a joint VPN (Virtual Private Network) tunnel.

The Softnet Security Client is the active node in this configuration, i.e. it initiates that the tunnel to the SCALANCE S module is opened on the network side. This has the advantage that a service technician can log on to the Internet from any location in the world without his current IP address being known (**dynamic IP address**).

The automation network comprises a SCALANCE S612 or SCALANCE S613 which protects and terminates the IPSec tunnel. These modules are connected to the Internet. In contrast to the service technician side, the access point here must have a static official address, i.e. an IP address routed in the Internet (**fixed IP address**). This IP address enables the Softnet Security Client to find the SCALANCE S in the Internet.

After a service technician has established a VPN connection to the SCALANCE S612/613 on the automation side by means of the Softnet Security Client, he can access all devices in the automation network, for instance, to load a new parameterization into an S7 using STEP7.

Note

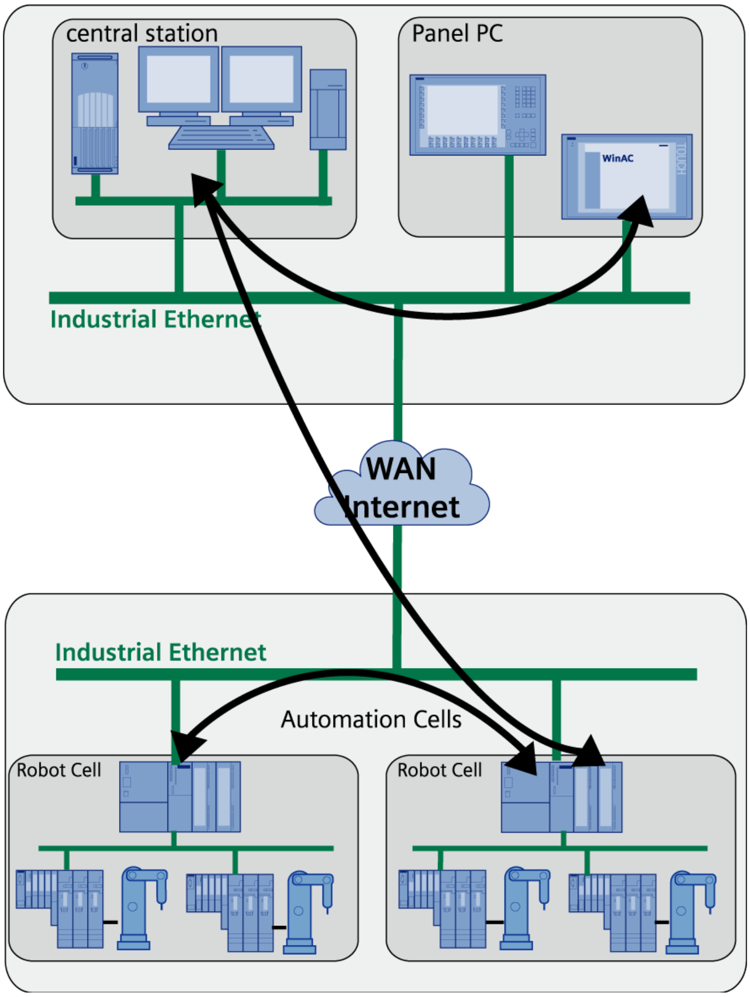
The document titled “Possible constellations using security components” provides additional information about this configuration. It is located on the same html page as this document.

3.5 Secure data communication between cells

3.5.1 Data communication via Internet

Network topology

Figure 3-10



Use case

Plant components networked around the globe or remote access via WAN to single devices from a central station, e.g. for diagnosis are quite common today. Exchanging sensitive manufacturing data, important production data or confidential data etc. among plant components and/or with the central station are everyday usage scenarios. A secure communication is therefore essential.

Problem

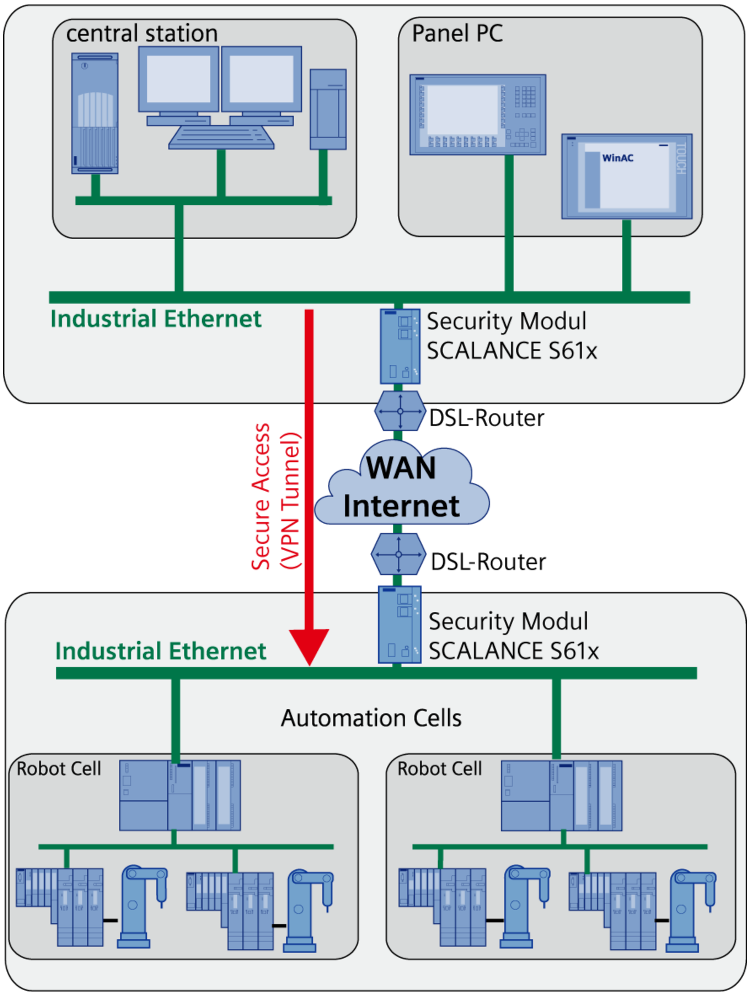
There are numerous risks associated with the Internet:

- Incorrect PC settings cause vulnerabilities and open up the way for viruses, trojans or worms.
- Non-encrypted data can easily be intercepted, manipulated or wiretapped.
- Intermediate storage of data
- Unnoticed hacker attacks from outside etc.

An unprotected internet connection can cause entire plant parts to be sabotaged.

Possible solution using SIMATIC NET components

Figure 3-11



Static VPN connections are established to enable a secure communication between distributed plants. To this end, each distributed plant component has one SCALANCE S module with internet access.

A configuration tool is used to configure all **SCALANCE S61x modules** so that they form the end points of a joint VPN (Virtual Private Network) tunnel.

One module in this configuration assumes the active part, i.e. it initiates that the tunnel to the other SCALANCE S modules is established. The active module only needs a **dynamic IP address**.

The other modules are passive and terminate the IPSec tunnel for the automation network in which they are located. In contrast to the active module, the access points here must have a static official address, i.e. an IP address routed in the Internet (**fixed IP address**).

As the connection is being established, the active side now opens a VPN connection to all SCALANCE S modules configured passive. Afterwards, the individual networks/cells behave as though they were part of a common network.

This means that S7 connections, for instance, can be parameterized and operated as usual. Furthermore, it is possible for a service technician to connect to one of the cells on the network in order to access all devices in the single networks/cells (e.g. diagnosing devices using NCM).

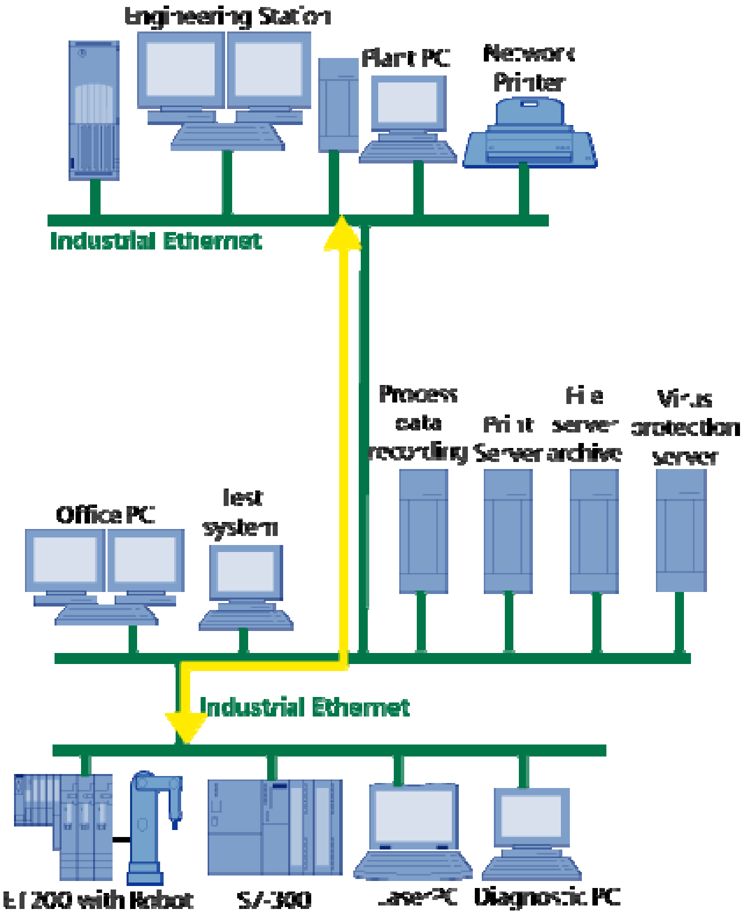
Note

The document titled “Possible constellations using security components” provides additional information about this configuration. It is located on the same html page as this document.

3.5.2 Data communication via LAN

Network topology

Figure 3-12



Use case

A modern network in a company links office and automation areas via one industrial Ethernet.

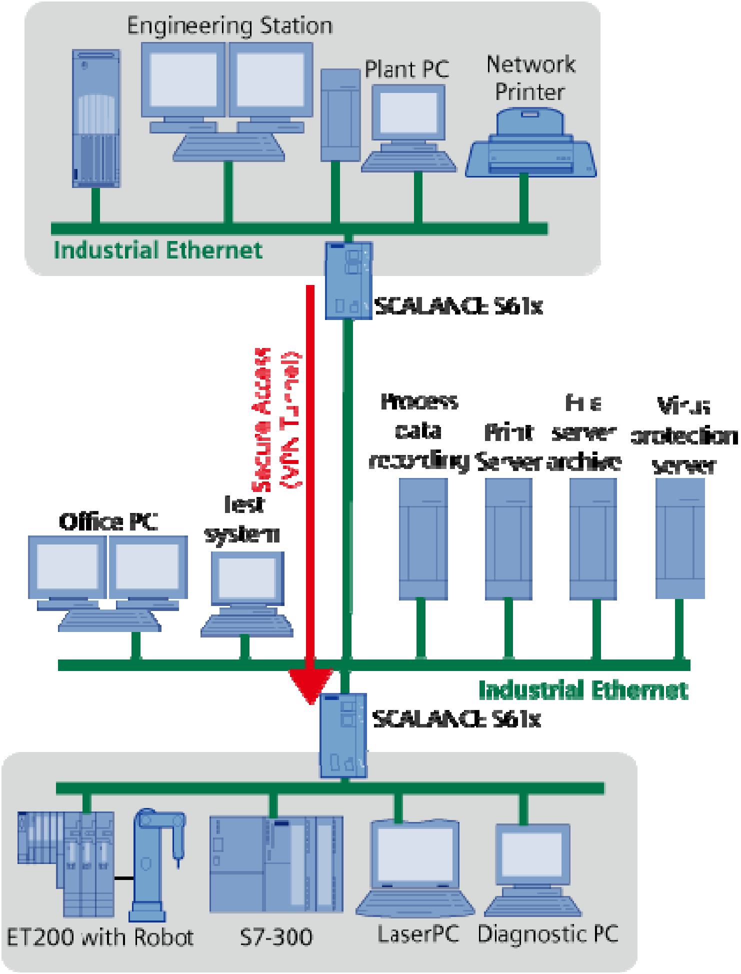
In large sites production is often distributed over several buildings. Exchanging sensitive manufacturing data, important production data or confidential data etc. among plant components and/or with the central station are everyday usage scenarios here.

Problem

Since uniform access mechanisms are used in office and automation networks, confidential production data become accessible to third persons who can view or even modify them if the network is unprotected.

Possible solution using SIMATIC NET components

Figure 3-13



Communication among automation cells is accomplished via an exclusive corporate network. Therefore, this scenario focuses less on secure data transmission (encryption) but more on the **restriction of the permitted communication among the automation cells**.

A configuration tool is used to configure all **SCALANCE S61x modules** so that they form the end points of a joint VPN (Virtual Private Network) tunnel.

One module in this configuration assumes the active part, i.e. it initiates that the tunnel to the other SCALANCE S module is established.

The other modules are passive and terminate the IPSec tunnel for the automation network in which they are located. Unlike the active component, these must have a static IP address within the corporate network (**fixed IP address**).

As the connection is being established, the active side now opens a VPN connection to all SCALANCE S modules configured passive. Afterwards, the individual networks/cells behave as though they were part of a common network.

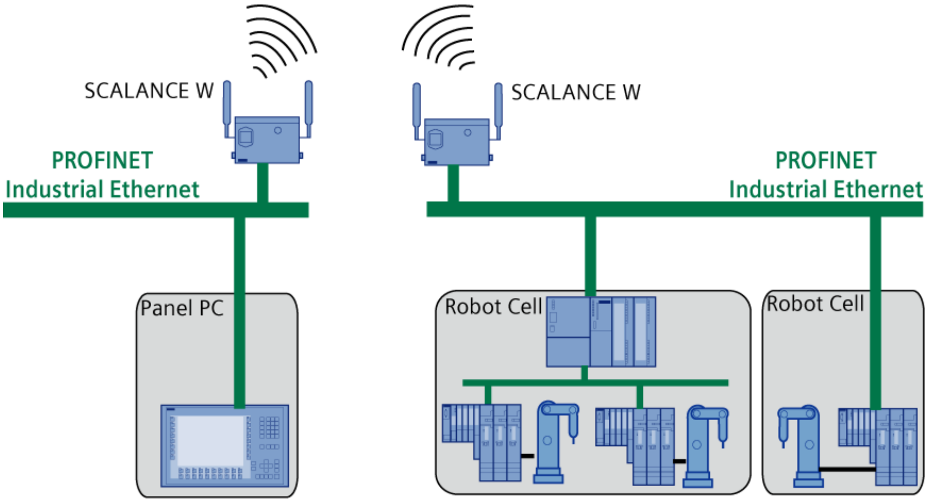
This means that S7 connections, for instance, can be parameterized and operated as usual. Furthermore, it is possible for a service technician to connect to one of the cells on the network in order to access all devices in the single networks/cells (e.g. diagnosing devices using NCM).

The difference to scenario 3 "Node restriction on S7 controllers" is that the VPN tunnel protects an entire automation cell against unauthorized access and not only one S7 controller via the CP. The data sent over the tunnel are encrypted.

3.6 WLAN scenarios with SCALANCE W

Network topology

Figure 3-14



Use case

Plant components which are difficult to access or areas where extreme conditions prevail (high temperature, rough environment etc.) are connected via a WLAN field. Secret, sensitive data are exchanged via industrial wireless LAN. Data security considerations should also apply for this type of transmission.

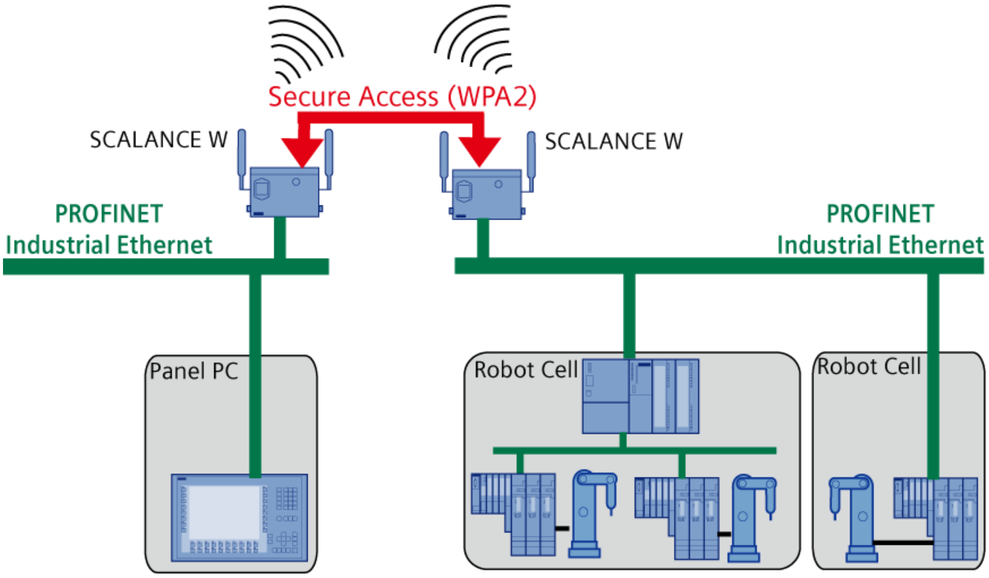
Problem

The radio network does not provide any protection features against unauthorized access. An unprotected radio network bears the risk that unauthorized person can log on to the WLAN and sabotage other terminal equipment.

To ensure data security, the WLAN components must have certain protection features.

Possible solution using SIMATIC NET components

Figure 3-15



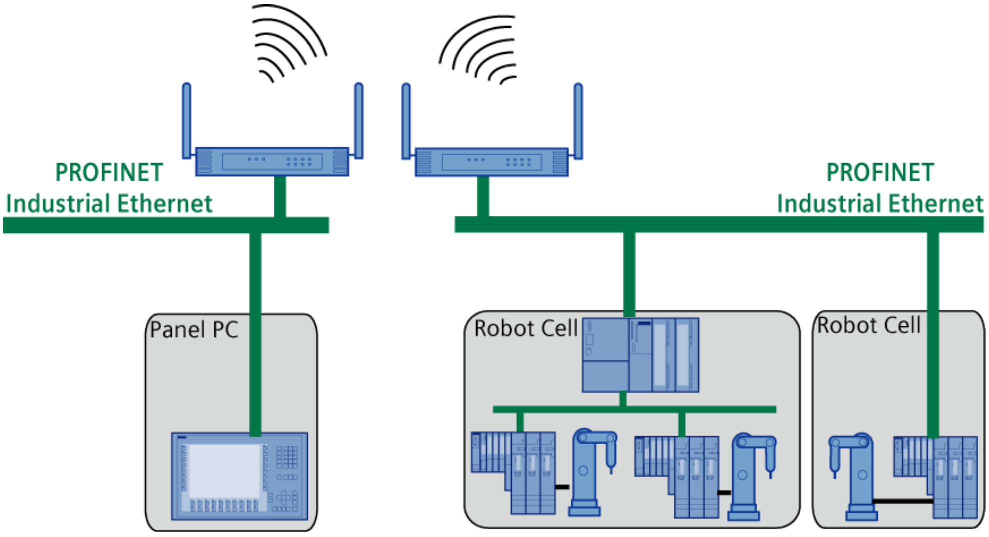
Besides their rugged design, the **SCALANCE W** products also offer **effective means for securing data**. All data to be sent are encrypted so that can not be spied, eavesdropped and tampered with.

The configuration of the access points and clients can be done easily via the web-based management.

3.7 WLAN scenario with non-secure components

Network topology

Figure 3-16



Use case

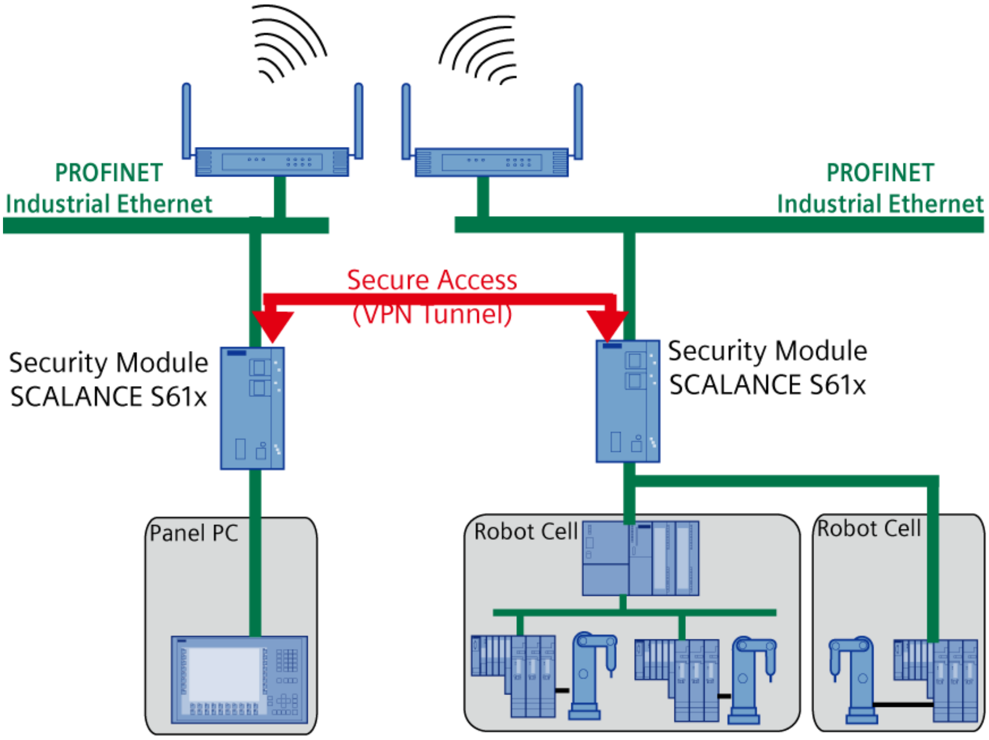
Not every WLAN infrastructure has the necessary security mechanisms. For economic reasons, it is desirable to keep the existing system and expand it to obtain a secure and protected network. Data security aspects must also be observed when operating an existing radio network.

Problem

It is not trivial to expand an existing radio network. It must be ensured that the new modules are integrated without difficulty and without causing any disturbances. If this is not the case, the system can become instable as a consequence or all existing modules may have to be reconfigured which involves additional costs and expenses.

Possible solution using SIMATIC NET components

Figure 3-17



In order to create a protected and secure data link, a static VPN connection is established between distributed plants. For this purpose, a SCALANCE S61x module is integrated into each plant component.

This has the advantage that the already existing WLAN access points do not have to be configured anew.

Only the SCALANCE S modules are configured so that they form the end points of a common VPN tunnel.

4 Basics and principles

This chapter gives an overview of the important terms, mechanisms, concepts and implementations associated with the security mechanisms.

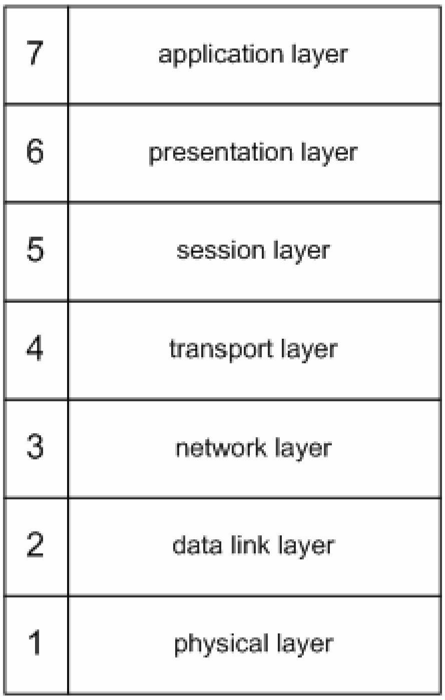
4.1 Basics of Ethernet and the IP protocol suite

4.1.1 OSI model (7-layer model)

The OSI model was developed by the International Standards Organization (ISO) forms the theoretical basis for data transmission in networks.

The model describes the way data is transmitted between two computer systems. There are seven layers and each layer assumes a certain function autonomously.

Figure 4-1



7	application layer
6	presentation layer
5	session layer
4	transport layer
3	network layer
2	data link layer
1	physical layer

The modular design enables specific program parts of single layers to be exchanged as desired. Thus it becomes possible to develop programs which are independent of the hardware used. This offers a considerable advantage over a monolithic solution.

For instance, using one TELENET application it is possible to communicate with another computer via LAN, a modem connection, via the serial interface or via industrial Ethernet.

The TELNET program works independently of the physical line. It merely passes the data packets on to the TCP layer (OSI layer 4) or receives data packets from this layer.

4.1.2 System addressing (MAC and IP address)

Each node in an IP-based Ethernet network is characterized by

- its unique MAC address specified by its hardware and
- an IP address assigned to it.

Additionally, a so-called subnet masks provides the information which address range its IP subnet encompasses.

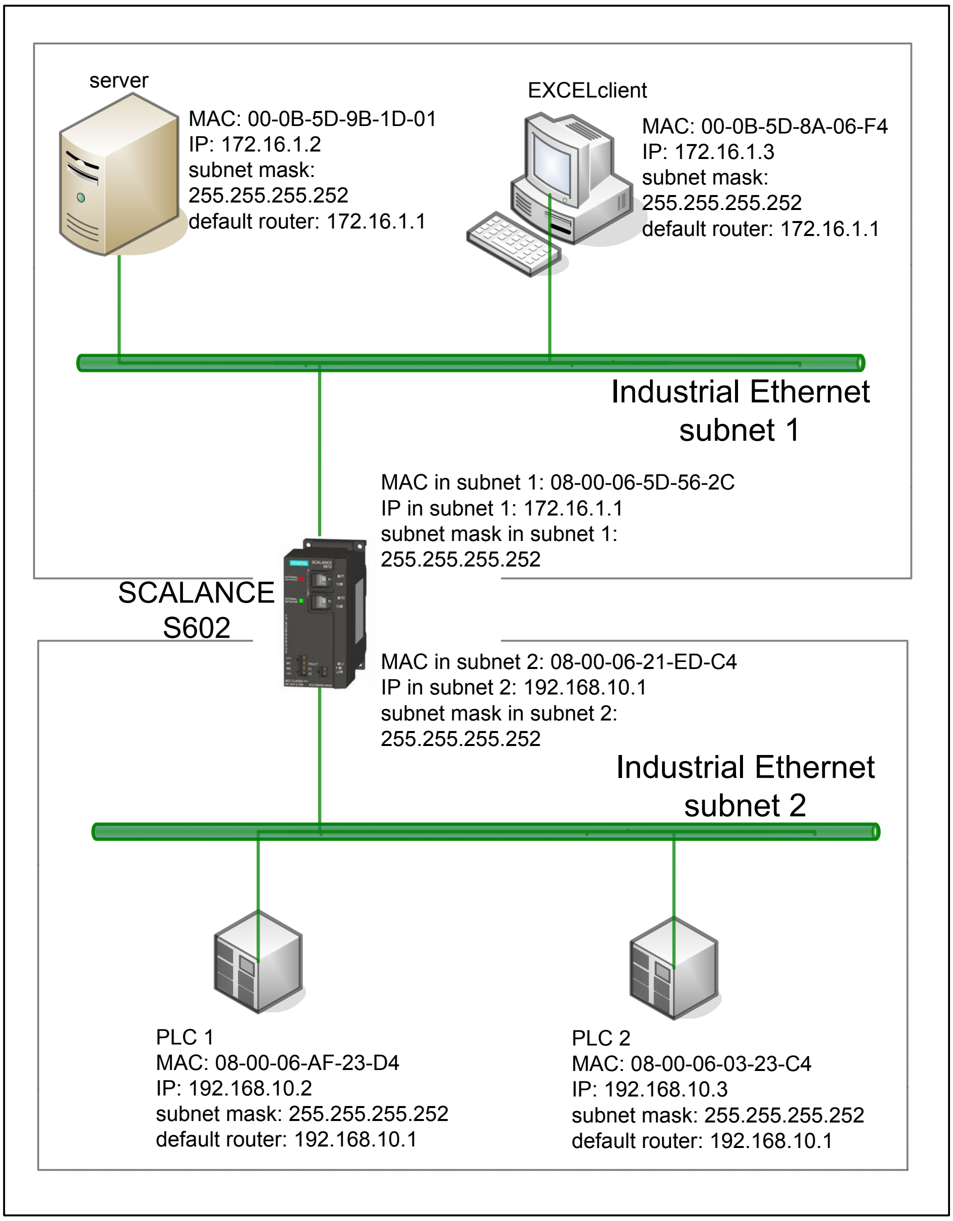
If several subnets are defined in a network, it is also informed about the addresses (systems) of the nodes in other subnets.

These systems located at the subnet transitions are called routers.

The following products from the SCALANCE range can be used as router:

- SCALANCE S module (S602, S612, S613)
- SCALANCE X 414-3E as layer 3 router

Figure 4-2


server
MAC: 00-0B-5D-9B-1D-01
IP: 172.16.1.2
subnet mask:
255.255.255.252
default router: 172.16.1.1
EXCELclient
MAC: 00-0B-5D-8A-06-F4
IP: 172.16.1.3
subnet mask:
255.255.255.252
default router: 172.16.1.1
Industrial Ethernet
subnet 1
MAC in subnet 1: 08-00-06-5D-56-2C
IP in subnet 1: 172.16.1.1
subnet mask in subnet 1:
255.255.255.252
SCALANCE
S602
MAC in subnet 2: 08-00-06-21-ED-C4
IP in subnet 2: 192.168.10.1
subnet mask in subnet 2:
255.255.255.252
Industrial Ethernet
subnet 2
PLC 1
MAC: 08-00-06-AF-23-D4
IP: 192.168.10.2
subnet mask: 255.255.255.252
default router: 192.168.10.1
PLC 2
MAC: 08-00-06-03-23-C4
IP: 192.168.10.3
subnet mask: 255.255.255.252
default router: 192.168.10.1

4.1.3 ARP

The Address Resolution Protocol (ARP) maps a MAC address to an IP address. Each network node keeps its own table with this mapping:

Table 4-1

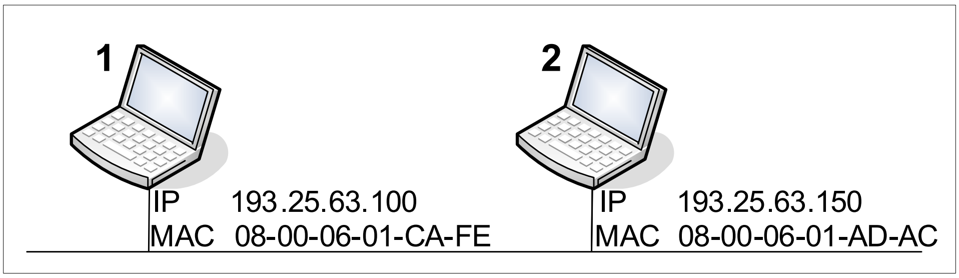
IP address	MAC address	Type
146.254.249.1	00-07-b4-00-00-02	dynamic
146.254.249.2	00-09-7b-9e-f1-8a	dynamic
146.254.249.3	00-09-7b-e0-a0-0a	dynamic

All assignments learnt via the ARP are saved as ‘dynamic’. It is also possible to generate ‘static’ entries manually.

Example 1: Address resolution in the same subnet:

Node 1 wants to send data to node 2:

Figure 4-3



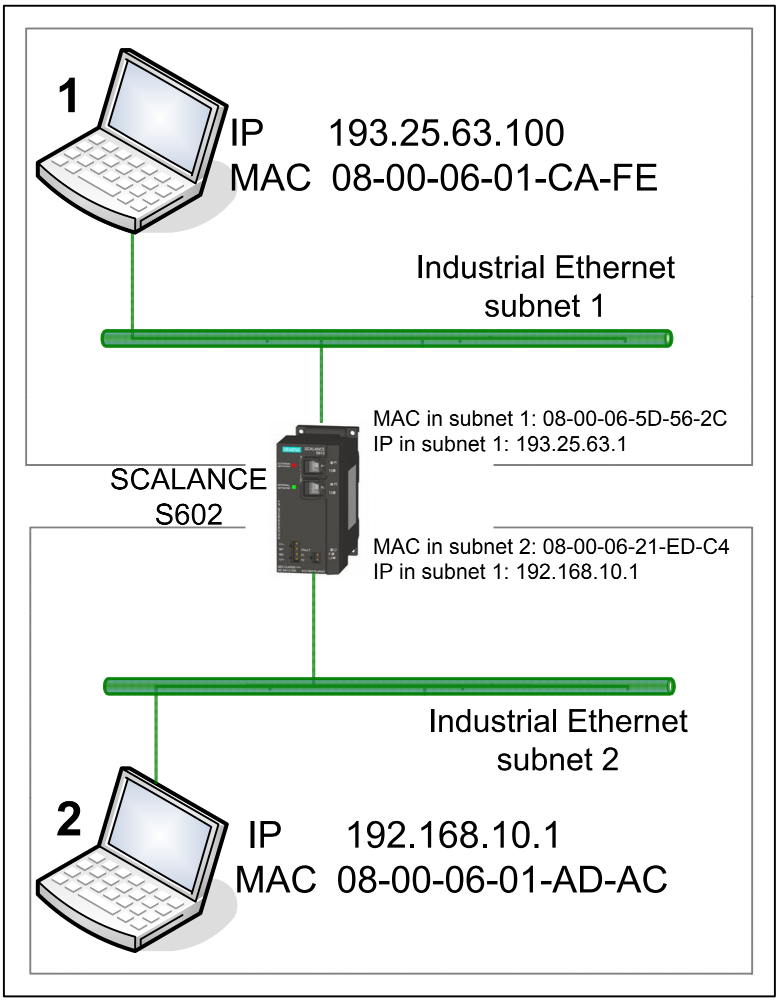
Process:

- Node 1 sends the following to all others in the subnet (via the broadcast address): “Who has the IP address 193.25.63.150?“.
- Computer 2 recognizes that this is its IP address and responds: “The MAC address to 193.25.63.150 is 08-00-06-01-AD-AC.“
- A connection between node 1 and 2 can now be established.

Example 2: Address resolution beyond subnet limits:

If node 1 wants to establish a connection to a system outside its own subnet, address resolution becomes a bit more difficult since there is a router installed at the transition between the subnets.

Figure 4-4


1
IP 193.25.63.100
MAC 08-00-06-01-CA-FE
Industrial Ethernet subnet 1
MAC in subnet 1: 08-00-06-5D-56-2C
IP in subnet 1: 193.25.63.1
SCALANCE S602
MAC in subnet 2: 08-00-06-21-ED-C4
IP in subnet 1: 192.168.10.1
Industrial Ethernet subnet 2
2
IP 192.168.10.1
MAC 08-00-06-01-AD-AC

Process:

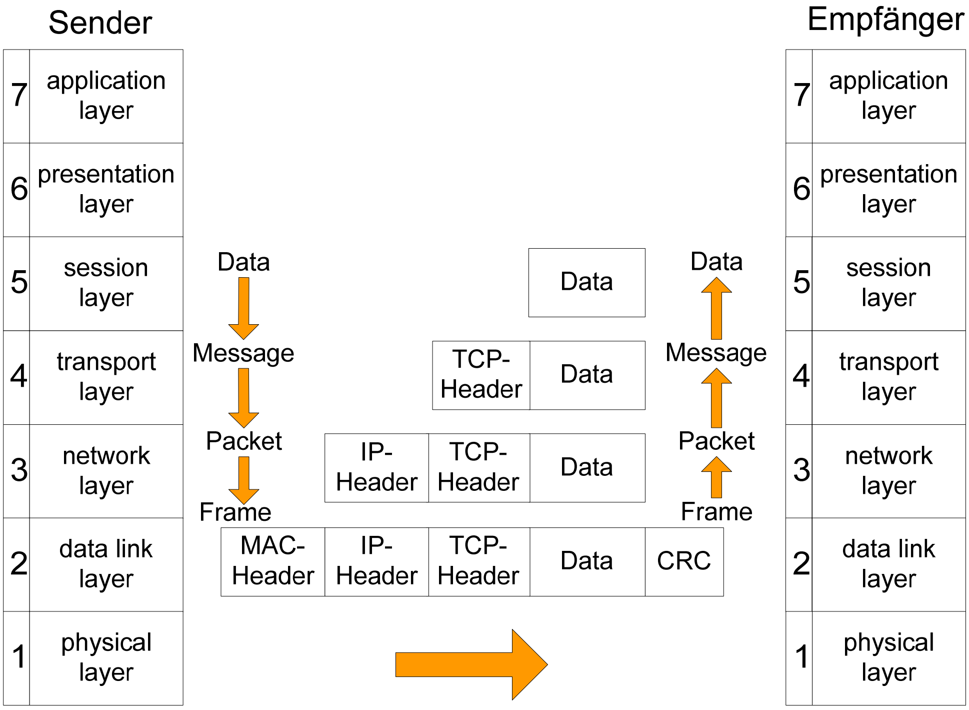
Table 4-2

Step	Function procedure
1.	Node 1 recognizes that node 2 is located in another subnet because of its own IP address and the subnet mask.
2.	The routing table of node 1 contains an entry that the subnet in which node 2 is located can be reached via the IP address 193.25.63.1.
3.	Node 1 therefore sends the following ARP request to 193.25.63.1: “Which MAC address does 193.25.63.1 have?”
4.	SCALANCE S602 sends the following response to node 1: “The MAC address to 193.25.63.1 is 08-00-06-5D56-2C.“
5.	Node 1 then sends the first packet intended for node 2 to SCALANCE S602.
6.	The header of the data packet enables the router to recognize that the packet is intended for node 2. Its routing table shows that it is directly connected to the desired subnet.
7.	It therefore sends an ARP request to 192.168.10.1: “Which MAC address does 192.168.10.1 have?”
8.	Node 2 responds: “The MAC address to 192.168.10.1 is 08-00-06-01-AD-AC.“
9.	The address resolution in the reverse direction is accordingly. To this end, node 2 requires an entry in its routing table that it can reach subnet 1, where node 1 is located, via the address 192.168.10.1.

4.1.4 Structure of a data packet

Data are transmitted in packets. These packets are formed by the protocols in the individual OSI layers adding transmission-related information to the actual data to be transmitted. The additional information is found in headers:

Figure 4-5



The individual headers which the sending side adds when sending the data are evaluated step by step on the receiving end until the data are available to the application on the top layers.

4.1.5 Formation of subnets and routing

The formation of subnets, routing and data forwarding across subnet limits are part of **OSI layer 3**.

The creation of subnets requires a subnet ID and a subnet mask. The lowest IP address is used as subnet ID. In the subnet mask it is defined how many IP addresses are contained in the subnet from the subnet ID on.

Example:

A company consists of four manufacturing units with 30 controllers each. These units are mapped as subnets in one main network. The main network is assigned the address range 192.168.1.0 – 192.168.1.255:

Table 4-3

	Subnet ID	Address range network nodes	Corresponding subnet mask
Unit 1	192.168.1.0	192.168.1.1 to 192.168.1.30	255.255.255.224
Unit 2	192.168.1.32	192.168.1.33 to 192.168.1.62	255.255.255.224
Unit 3	192.168.1.64	192.168.1.65 to 192.168.1.94	255.255.255.224
Unit 4	192.168.1.96	192.168.1.97 to 192.168.1.126	255.255.255.224

The highest IP address in a subnet (**192.168.1.31** for unit 1) must not be assigned to any network node. This address is referred to as **broadcast address** and is used as collective address for all IP addresses in the subnet. If data is sent to this highest IP address, then all nodes on the subnet are the recipients.

4.1.6 TCP

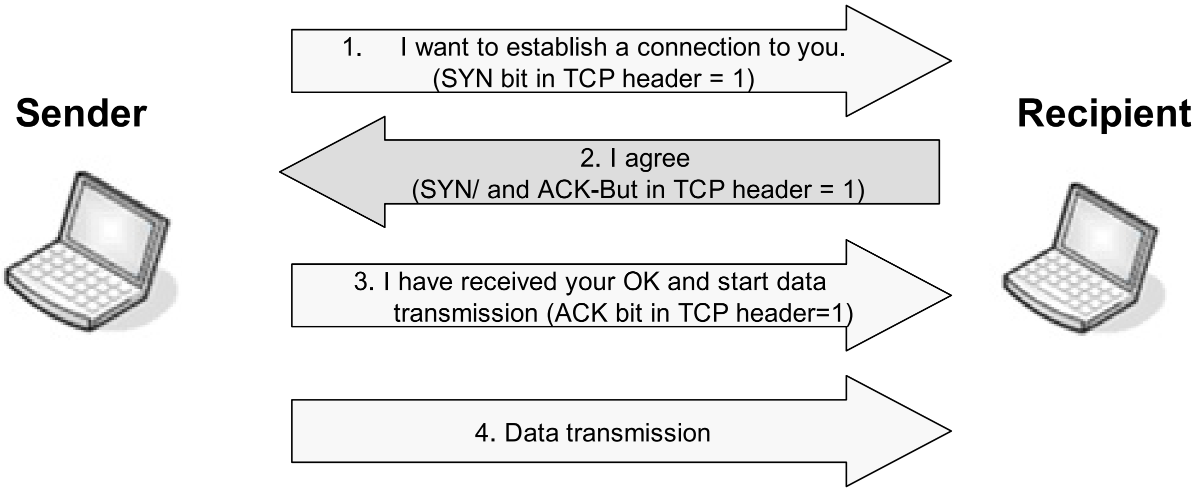
TCP is a part of the IP protocol suite and is assigned to **OSI layer 4** (transport layer). Each TCP/IP data link has a sender and a receiver. In the IP protocol suite, TCP is a connection-oriented protocol that controls the data traffic and takes measures in the event of data loss.

The TCP's task is to distribute the data from different application processes, add a header and forward it for transmission to the Internet Protocol (IP) on OSI layer 3 (network layer). On the receiving side, TCP sorts the data and puts it back together to a data flow. TCP recognizes lost packets and requests them again. On the transport layer, sending and receiving side are in permanent contact to each other. Although it is rather a virtual connection, control messages are exchanged continuously during the data transmission. With the SEND/RECEIVE interface via TCP connections the Ethernet CP supports the socket interface (e.g. Winsock.dll) to TCP/IP that is available on virtually every end system (PC or external system).

A TCP connection is established and closed using the so-called 3-way handshake:

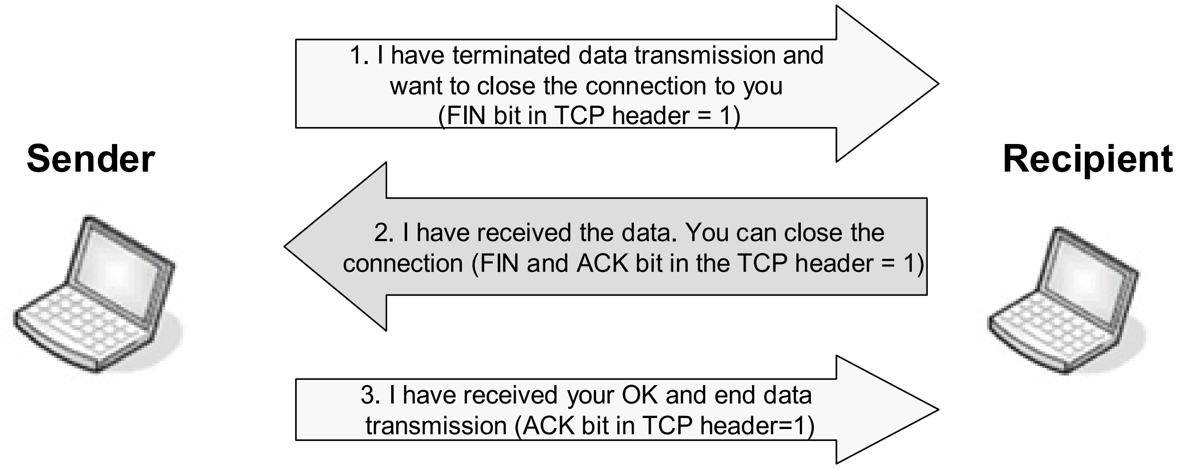
Establishing a TCP connection:

Figure 4-6


Sender
Recipient
1. I want to establish a connection to you. (SYN bit in TCP header = 1)
2. I agree (SYN/ and ACK-But in TCP header = 1)
3. I have received your OK and start data transmission (ACK bit in TCP header=1)
4. Data transmission

Closing a TCP connection:

Figure 4-7


Sender
Recipient
1. I have terminated data transmission and want to close the connection to you (FIN bit in TCP header = 1)
2. I have received the data. You can close the connection (FIN and ACK bit in the TCP header = 1)
3. I have received your OK and end data transmission (ACK bit in TCP header=1)

4.1.7 UDP

UDP also belongs to **OSI layer 4** (transport layer). Unlike TCP, UDP is a **connectionless** protocol; it does not send acknowledgements for packets that have arrived. Avoiding some features such as data flow control, protocol-controlled requesting of lost data packets makes UDP faster. Therefore, UDP is better suited for data transmission such as video streaming where lost data packets do not matter. Furthermore, UDP is used as a simple transport protocol if higher-layer protocols (in OSI layers 5-7) carry out error-checking.

4.1.8 Port addressing

Each TCP or UDP data packet contains a port number associated with an application or a service that polls this port and receives the data from TCP. The port numbers start at 1 and up to port number 1024 they are assigned to a specific application, e.g. port 80 for HTTP. All higher port numbers are free to be used by other programs. When configuring the connection in STEP 7, ports from 2000 on are available. This port structure enables several applications to establish connections to several communication partners simultaneously via the network.

4.1.9 Application Examples

Table 4-4

Application	Transport protocol	Port number
FTP (data exchange)	TCP	20
FTP (control data)	TCP	21
SSH	TCP	22
TELNET	TCP	23
SMTP (e-mail)	TCP	25
DNS (name resolution)	UDP	53
HTTP	TCP	80
ISO_TSAP (SIMATIC Manager)	TCP	102
HTTPS (SSL)	TCP	443

4.2 Firewalls

This chapter presents the most important firewall types and their properties.

4.2.1 Packet filter

From a historical point of view, packet filter firewalls are an expansion of network routers. Each router has two or more interfaces to connected networks and maintains tables about which networks are connected or available via which interfaces (routing tables). It is quite easy to expand the routers by certain sets of rules that specify whether the existing routers can be used by different IP packets or not. Routers make their routing decisions only on the link layer (layer 3) of the OSI model. This requires only the IP header of the packets to be analysed so that the router can achieve sufficiently high transfer rates even with a moderate hardware equipment. The filter mechanisms of a classical packet filter are kept comparably simple to be able to guarantee persistent transfer rates. This is why these packet filters only use information in the headers of the packets; they do not consider the data contents of the IP packets on higher protocol levels. A well equipped packet filter in a TCP/IP environment therefore makes its decisions based on the following parameters:

- IP addresses of sender and receiver
- IP protocol used
- TCP or UDP ports provided that the IP packet transports one of these protocols
- IP and TCP flags, ICMP types
- the network interfaces via which the IP packet reaches the packet filter and may leave it again

Not all packet filter implementations use all these parameters. The administrator determines a set of filter rules that remains static during operation. Each rule defines for a combination of the above parameters whether an IP packet is forwarded or not. When a certain IP packet is processed, a comparison with the existing filter rules yields whether a rule applies to the packet parameters. If yes, the action defined in the rule is executed (forward or block). If no filter rule matches the packet, a default setting becomes active (which should block the packet for security reasons).

A classical packet filter processes each IP packet individually. The decision about forwarding or blocking does not depend on which IP packets were processed previously.

Many packet filters are implemented on the basis of routers. The so-called bridging firewalls are an alternative to this. Their filter rules control the data traffic over a network bridge, i.e. on OSI layer 2. In terms of security, they are nearly identical to the packet filters on the routing level. A slight advantage could be that they are configured without their own IP address so that they are not visible on IP level. They are advantageous from a network point of view if the connected network segments should not or can not form autonomous subnets or backlash-free integration is required. The SCALANCE S modules S612 and S613 are such bridging firewalls.

4.2.2 Stateful packet filters

The filter properties of packet filter can be improved considerably if the IP packets are checked in their context. For instance, a UDP datagram arriving from an external computer should only be forwarded inside if another UDP datagram was sent to that computer shortly before from within (e.g. in case of a DNS request of a client in the internal network to an external DNS server). To enable this, the packet filter must maintain records of all states to all current connections. Such packet filters are therefore referred to as **stateful**. In case of TCP connections, they imitate the status monitoring of a complete TCP/IP protocol stack, and in case of UDP, they simulate virtual connections. Another important feature of a stateful packet filter is its capability to dynamically generate and delete filter rules. In the above case, a rule must be activated for a limited period which accepts the “response packet” and forwards it to the client after the first UDP data packet has passed from inside to outside. After the time window for the response has expired, this rule has to be deleted again. The configuration is thus facilitated for the firewall administrator since some rule definitions do not have to be entered explicitly anymore. On the other hand, the firewall behavior is no longer fully under the administrator’s control. Stateful packet filters thus offer additional security in so far that many ports for IP packets arriving from outside do not have to be kept open permanently but are only opened if required. External ports which are permanently open are now only required for such connections initiated from outside.

4.2.3 Stateful inspection firewalls

The word **inspection** in the name of this firewall type indicates in which direction the inspection possibilities are expanded here. Stateful inspection firewalls also have access to the contents of the data packets. They so pave they way for checking the contents of the data traffic and other higher-ranking control functions such as user authentications. The prerequisite for this is given by the other keyword **stateful**. Only by tracking the status is it possible to assign the individual IP packets to the different simultaneous connections thus enabling a sensible contents check. It can hardly be concluded from the contents of a single IP packet whether it belongs e.g. to a certain e-mail - and it is even more difficult to verify whether this e-mail contains a virus, trojan or worm. This check is only possible if the entire data stream from all IP packets of that connection is put together. Usually, stateful inspection firewalls do not perform the check themselves, but rather they forward the data stream to separate security servers which then check the data. But security servers are only available for very few protocols. For these protocols, the stateful inspection firewalls work similarly to the application level gateways described in the next section. For all other protocols, they function as a stateful packet filter. Stateful inspection firewalls can therefore be regarded as hybrid systems.

4.2.4 Application gateways

This firewall type concentrates its monitoring functions on the application layer (OSI layer 7). There is a special **proxy** test program for each processed application protocol. It analyses the full data stream of that application. This firewall type is therefore referred to as **proxy firewall**. In any case, a proxy verifies only compliance with the application protocol for which it was written. The following protocol-specific and configuration-dependent options add to this:

- **Filtering protocol elements**

  Not everything defined in the application protocol may be allowed in the real application case. A possible example is e.g. the filtering of the PUT command in the ftp protocol if the addressed ftp server is not allowed to receive uploads.

- **Searching for malware**

  On the application layer, the data is in a format that allows checking it for viruses, trojans, worms and other malware using a custom virus scanner.

- **User authentication**

  In case the application protocol itself provides for a user authentication, it may already be requested by the proxy before addressing the originally addressed server. An unauthorized user can not reach the server in this case.

4.3 IPSec-based encryption

The use of IPSec-based encryption eliminates those weak points in IP communication that are potentially most dangerous:

- **Espionage**
  It is possible to **read the contents of the data packets** as they are transmitted (e.g. via the Internet)
- **Manipulation**
  The data in the packets can be **manipulated** during transmission either concerning the contents or the addresses of recipient or sender.

This is achieved by using **ESP** (see Encryption via ESP protocol) to coordinate and perform the data encryption and **AH** (see Integrity check via AH protocol) to coordinate and perform the integrity check. This guarantees that confidentiality and/or integrity are ensured depending on the requirements or application.

4.3.1 Security Associations (SAs)

To be able to perform IPSec-based protected communication between 2 partners in the first place, the so-called **security associations** must be determined. They are specified by:

- an unambiguous SPI (Security Parameter Index)
- an IP address of the communication partner
- the security protocol to be used (ESP or AH)
- the key to be used
- the validity period
- the protocol mode (tunnel mode or transport mode)

These security associations describe a unidirectional relation between sender and receiver. Hence, two opposite security associations have to be defined for bidirectional communication.

4.3.2 Integrity check via AH protocol

The **authentication header** is basically used to calculate a **cryptographic checksum** over each single data packet. The data are not changed during this process.

This process is also referred to as hashing. The standard procedure is the hashed message authentication code with the algorithms MD5 or SHA-1.

A modification of the data packet during transmission would require the cryptographic checksum calculated previously to be adapted in order to remain undiscovered. An outsider would not be able to do that. The recipient of the packet would recognize that the cryptographic checksum no longer matches the data field and that integrity is no longer guaranteed.

4.3.3 Encryption via ESP protocol

With **Encapsulating Security Payload**, the content of each data packet is **encrypted**, i.e. the data are modified cryptographically for the transfer. Moreover, ESP offers several optional security functions:

- an integrity check of the data packet
- anti-replay (to prevent e.g. DoS attacks)
  Anti-replay is the concept of not allowing an intercepted packet to be sent to the recipient multiple times and so causing overload. Such packets are no longer considered by the recipient.

Usual standard methods with ESP are:

- DES
- RC4
- 3DES
- AES

4.3.4 IPSec modes (tunnel vs. transport)

IPSec encryption is possible in two different modes:

Transport mode

In transport mode, the encryption encompasses “only” the data field. The packet headers remain untouched. The transport mode is nearly always used in special environments only where an address conversion via NAT/NAPT is required due to external circumstances.

Tunnel mode

In the tunnel mode, the encryption and thus confidentiality encompasses the entire data packet including header. Since this mode also protects against modifications in the header, it is used far more often than the transport mode.

4.3.5 Methods of key management (negotiating and exchanging)

Concepts

There are presently three standard concepts for exchanging or negotiating IPSec key information and for setting up the SAs:

- Manual Key Management (manual IPSec)
- Simple Key Management for Internal Protocols (SKIP)
- Internet Security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE) as its subset.

ISAKMP

ISAKMP between sender and recipient comprises two phases:

- **First phase:** Establishing an SA to
  - negotiate, generate and distribute the used keys
  - authenticate the communication partners
  - exchange the integrity and/or confidentiality algorithms to be used
- **Second phase:**
  - Establishing one or more SA for user data communication

IKE

IKE as a partial implementation of ISAKMP is integrated into the SCALANCE S series and equally comprises two phases. Key management in phase 1 is limited to the Diffie-Helman procedure where the communication partners are authenticated via:

- **Pre-shared keys**
  - The key material has been negotiated, generated and distributed offline.
- **Public-key procedure**

  The key material has been negotiated online using certificates (e.g. via the RSA algorithm).

4.3.6 Key exchange techniques

Asymmetric techniques

The basic idea with asymmetric algorithms is to use a pair of keys. One of the two keys is for encrypting the message. This public key is accessible to everybody. The second key is for decrypting the message. This key must remain secret (private key). This technique is also referred to as public key algorithms. It is essential that the private key can not be derived or calculated from the public key.

Symmetric techniques

With symmetric algorithms, the same key is used for encrypting and decrypting on both sides or keys are used for encrypting and decrypting that can be derived from each other. Symmetric algorithms have the advantage of being very fast and relatively easy to implement. The drawback is the encryption of the key material. The symmetry requires the key to be known to both the sender and the recipient. Since an algorithm is only secure if the information required for the encryption, i.e. the key, remains secret, that key has to be exchanged or negotiated previously on a secure channel. If the key is revealed during this exchange, the entire encryption process is endangered.

Diffie-Hellman algorithm

The Diffie-Hellman algorithm is probably the best known method of exchanging key information online. Named after the inventors Whitfield Diffie and Martin Hellman, it was first used in 1976. This technique aims to generate a common key for sender and recipient for each security association. Both encryption parties agree on:

- a large prime number p
- a basis g for which 1<g<p holds

The common key is generated by means of this piece of information.

Summary

Symmetric and asymmetric techniques are often combined in practice to compensate for their disadvantages. For the actual encryption of the data a symmetric key is often used because it is very fast. An asymmetric procedure is then adopted to distribute this symmetric key to all communication partners.

4.4 Wireless LAN – Security basics

4.4.1 WEP (Wired Equivalent Privacy)

WEP is the oldest and at the same time the least secure encryption method for protecting WLAN transmissions against unauthorized intruders according to the 802.11 standard.

In this method, a user password is used as a fixed key to generate a sequence of pseudo random numbers. Each character of the message to be transmitted is then encrypted or decrypted with the next number from this sequence on the receiving side.

The method is relatively simple and rather easy to compromise in two ways: On the one hand, the key must be exchanged between sender and receiver while the connection is established; this exchange is unencrypted.

On the other hand, statistical methods can be used to determine characteristics from the transmitted message traffic, which again enable to draw conclusions about the used key as long as there is an adequate number of messages for the analysis.

For these reasons WEP is generally no longer considered to be adequately secure.

4.4.2 WPA (Wi-Fi Protected Access)

WPA is the development of WEP and still considered as standard despite several shortcomings. Aside from technical changes of the actual encryption algorithm, the execution of the protocol was also adapted and additional functions were integrated:

- Passwords for the network access (authentication) can be stored on a central server (“RADIUS”)
- The key for the message transmission changes dynamically and thus makes statistical attacks more difficult,
- The MAC address (i.e. the unique hardware identification) of the sender is incorporated into the key, which makes it even more difficult to falsify the sender of messages.

The development of an encryption algorithm which was supposed to replace WEP by the IEEE task group 802.11i was delayed so that the Wi-Fi Alliance recommended the application of WPA as a subset of the 802.11i standards as interim solution. In the meantime, this has been rendered invalid with the adoption of the 802.11is standard and WPA2 or AES are available as methods of first choice.

4.4.3 WPA2 und AES (Advanced Encryption Standard)

After adopting the complete 802.11i standard, this standard was applied by the Wi-Fi Alliance as WPA2. The essential difference between WPA2 and WPA is the encryption method: The shortcomings which were identified in the meantime in WPA no longer exist in the AES method used in WPA2.

Like WEP, “Advanced Encryption Standard” exercises the “adding up” of a key to the message. One block of the raw data is processed with the corresponding identical key but several processing sequences with respectively varying block boundaries take place.

When selecting “reasonable” passwords with adequate length which cannot be guessed, AES-encrypted messages are considered to impossible to crack according to the present state of the art (2006).

4.4.4 EAP (Extensible Authentication Protocol)

EAP is a widely used framework for different authentication methods for network access. In other words, EAP itself is not an authentication method but describes the mechanism according to which client and server can agree on a method.

One of the methods which can be used under EAP is “EAP-TLS” (“EAP-Transport Layer Security”), in which the network nodes have to be “certified” before they are authorized for the network communication, i.e. they must e authenticated at a central server. This method is comparable to SSL familiar from the internet.

4.4.5 MAC filter

MAC addresses (Media Access Control) are codes that enable hardware elements (e.g. network cards, modules, motherboards, etc.) to be clearly identified world wide.

The addresses normally comprise 6 bytes (48 bits) and are “hard-wired” in the corresponding components; upon request the components identify themselves by returning their MAC address.

In the network management, filter tables with MAC addresses can be created which allow or forbid the access to specific addresses. This enables to implement a simple, albeit comparatively insecure access protection for the network.

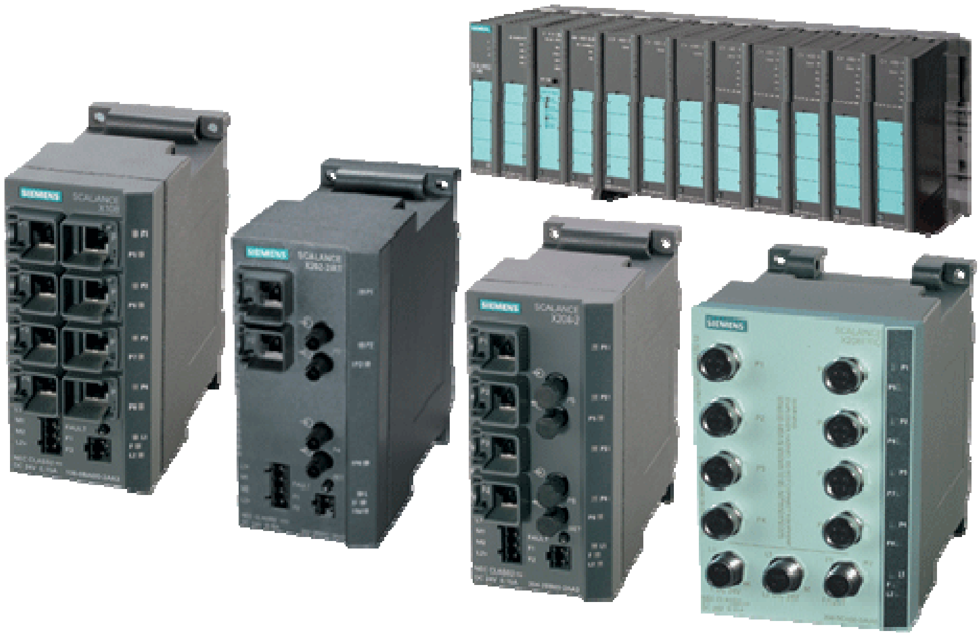
It cannot be excluded that MAC addresses are manipulated (“spoofing”) so that MAC filters only offer adequate protection for a network in connection with other measures.

5 SIMATIC NET products

The SCALANCE product range comprises the SIMATIC NET products. The postfix after the “family name” stands for the application field. An "**X**" stands for "**switching**", the "**W**" for "**wireless**" and the "**S**" for "**Security**".

5.1 Industrial Switching – SCALANCE X

Figure 5-1



The **SCALANCE X** product range offers switches for industrial use. They are available in different performance categories with an expanded performance spectrum for each stage. These devices offer the advantage that they were developed to match the specific requirements of automation environments. This shows e.g. in the temperature ranges for which the switches can be used. The rugged housing, too, is adapted to the more demanding application environment. The devices are mounted either directly to a surface or via a top-hat rail.

The individual function stages are indicated by the number affixed to the “family name”. This number always has three digits. The hundreds digit indicates the performance class. It can be between 0 (lowest performance class) and 4 (highest performance class). The tens digit and ones digit reflects the number of electrical ports. The designation SCALANCE X224 therefore describes a switch of performance class 2 with 24 electrical ports.

Only switches of performance class 3 and 4 are suited for safety-relevant functions. The difference between the 300 and 400 switches is that the 400 series has a modular design whereas the 300 products have a compact design.

5.2 Industrial Wireless LAN - SCALANCE W

Figure 5-2

The Industrial Wireless LAN (IWLAN) components are a mobile solution for new applications up to and including field level. The products offer a unique combination of reliability, ruggedness and safety.

The industrial use of wireless technology requires particularly reliable connections. A modulation that is disturbance-tolerant is taken into account in standard 802.11 b/g and a. The data rate can be reduced in defined steps to maintain the wireless connection even over greater distances or reflections at metallic objects. This is all part of the IEEE 802.11 standard with data rates up to 54 Mbit/s and frequencies from 2.4 GHz and 5GHz. A turbo mode function with a transmission rate of up to 108 Mbit/s is also supported where two adjacent channels are bundled. The turbo mode is, however, not conformant to IEEE.

Besides this standard, Industrial Wireless LAN from SIMATIC NET offers an expansion of the standard which provides selected nodes a defined data rate. This enables deterministic data traffic on the basis of the shared medium wireless LAN. IWLAN supports the selected monitoring of the connection of a node to the access point in order to initiate immediate counter-measures in the event of connection being cancelled or the radio cell being left.

Everyday use in a harsh industrial environment requires **rugged** products, especially when they are not installed inside control cabinets. IWLAN components from SIMATIC NET are designed for **protection class IP65** and operating temperatures between -20°C and +60°C with dewing and meet the high requirements of SIMATIC concerning shock and vibrations. The connector design is **shake-proof and vibration-proof**.

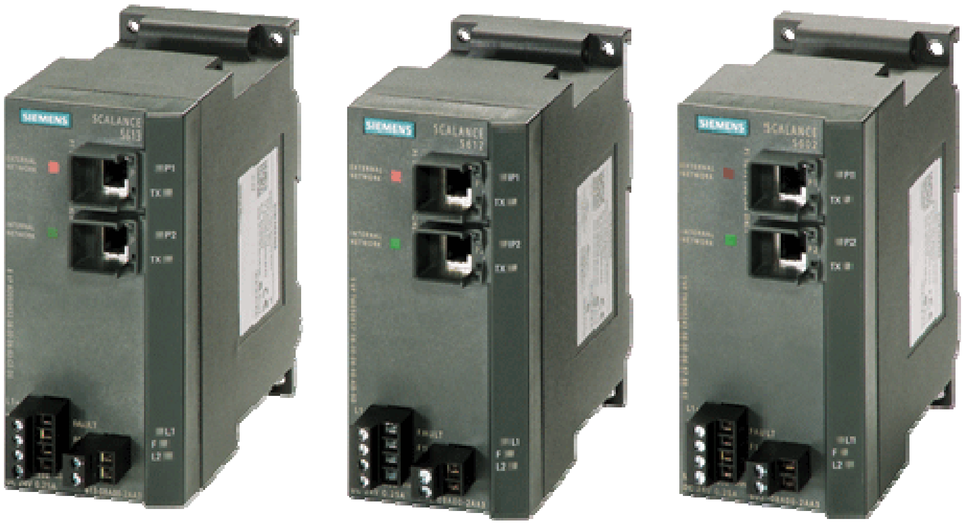
Protection against unauthorized access and data encryption are requirements which are not only important when transmitting secret formulations. Industrial

Wireless LAN exactly follows the specifications defined by IEEE and WiFi in the 802.11 standard to enable a high level of interoperability. The new mechanisms from **WPA and an AES-based encryption** have eliminated the known security gaps of wireless LAN and WEP.

Downtimes of network segments and connected industrial Ethernet nodes are eliminated by using the C-PLUG in the event of a fault. The C-PLUG enables SIMATIC NET components to be exchanged quickly and easily without reconfiguration of the spare part.

5.3 Industrial Security - SCALANCE S

Figure 5-3



The hardware and software of the SCALANCE S product range form a security system that is sophisticated down to the smallest detail. It is tailored to the high demands of industrial communication.

The protection functions of SCALANCE S ensure that the entire **data traffic** from and to the cell is **controlled**. The security modules are simply placed in front of the devices to be protected just like a network component.

The protection of subnets or automation cells with security modules ensures that automation devices are secured although they do not have own security functions. Equipping all automation devices with their own security functionality does not make sense, neither from a technical nor from an economic point of view. The concept using cells, however, is an efficient means of securing existing networks.

Security modules are capable of protecting **several devices simultaneously**. For users the means lower costs and significantly less configuration effort.

Real-time capability and security are contrary requirements in principle. Each security mechanism must check whether certain connections or accesses are allowed or not by relying on rules or configurations. This also costs time and performance. Inside the cell, however, real-time data traffic can flow entirely unaffected by security mechanisms.

The **encryption** of device communication is another important pillar of security in data transmission. The SCALANCE S612 and SCALANCE S613 security modules offer IPSec-based encryption algorithms in connection with the software-based SOFTNET Security Client.

The S61x security modules

The **SCALANCE S61x** security modules provide an integrated firewall and utmost data security by means of IPSec VPN tunneling of incoming and outgoing data. Both modules are also routing-capable from version 2.0 on.

The SCALANCE **S61x** security module is available in the following versions:

Table 5-1

Property	S612	S613
Stateful Inspection Firewall	yes	yes
Number of protected device on the internal network per VPN tunnel	32	64
Number of simultaneously manageable VPN tunnels	64	128
Interfaces	2 RJ45 10/100 Mbit/s	2 RJ45 10/100 Mbit/s

The S602 security module

The SCALANCE **S602** security module offers a routing functionality on layer 3 and is equipped with two RJ45 10/100 Mbit/s Ethernet ports in addition to the integrated firewall that is standard for all SCALANCE S products. Integration of the TCP/IP protocols DHCP, DNS, NTP, Syslog make the offer complete.

C-Plug

The configuration data are saved automatically on a configuration plug (C-PLUG). In case a device has to be exchanged, merely the C-PLUG has to be taken over into the replacement device. This enables the replacement component to start up with the same device configuration although it was not configured separately.

6 List of abbreviations

Table 6-1

Abbreviation	Description
AES	Advanced Encryption Standard
AH	Authentication Header
ARP	Address Resolution Protocol
C-PLUG	Configuration Plug
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
EAP	Extensible Authentication Protocol
ERTEC	Enhanced Realtime Controller
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GHz	gigahertz
GPRS	General Packet Radio Services
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IRT	Industrial Real Time
ISAKMP	Internet Security Association and Key Management Protocol
IWLAN	Industrial Wireless Local Area Network
LAN	Local Area Network
LED	Light Emitting Diode
Optical fiber	Optical fiber
MAC	Media Access Control
Mbit/s	Megabits per second
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OSI	Open System Interconnection
PSTN	
RADIUS	Remote Authentication Dial-In User Service
RSA algorithm	Rivest-Shamir-Adleman algorithm
RSTP	Rapid Spanning Tree Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WEP	Wireless Encryption Standard
Wi-Fi	Wireless Fidelity
WPA	Wireless Fidelity Protected Access

7 History

Table 7-1 History

Version	Date	Change
V1.0	31.10.2007	First edition
V1.1	02.03.2010	New Layout