Security with SIMATIC controller

SIMATIC S7-300/400/WinAC/1200/1500

https://support.industry.siemens.com/cs/ww/EN/view/77431846

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity

Table of contents

1 Minimizing Risk through Security

Increased networking and the use of proven technologies of the office world in automation systems lead to increased security requirements. It is not sufficient to offer only superficial and limited protection, since attacks from outside may occur on several levels. A deep understanding of security and how to apply it is required for optimal protection.

1.1 Security strategies

Motivation

The first priority in automation is maintaining control over the production process. Measures intended to reduce the security threats must not interfere with this priority. The use of an adequate protection concept should ensure that only authenticated users can carry out (authorized) operations, restricting access to those operation options approved for use by the authenticated user. The operation is to be carried out exclusively in clearly planned access paths to ensure that the production process will continue to operate securely during a command without any risks for people, the environment, the product, the goods to be coordinated and the business of the company.

Strategies

Based on these statements, a protection concept comprises general defense strategies which are intended to resist the following attacks:

- decrease of availability (e.g. denial of Service)
- bypassing single security mechanisms (such as “man in the middle”)
- intentional incorrect operation by authorized users (such as stealing passwords)
- incorrect operations due to misconfigured user privileges
- unauthorized monitoring of data (such as recipes and business secrets or the functioning of the machines and systems and their security mechanisms)
- modifying data (for example to alter alarm levels)
- deleting data (for example login files for covering attacks).

The Siemens defense strategy uses the mechanisms of “Defense in Depth”.

Defense in Depth

The concept of Defense in Depth contains layered structures of security and recognition measures that are superior to the security level of stand-alone systems. It has the following features:

- Capability to detect attackers that try to break through or bypass the Defense in Depth structure.
- A weak point in one layer of this architecture can be temporarily compensated for by the defensive strategies in other layers.
- The system security has its own layer structure within the overall layered structure of the networks security.

1.2 Implementation of strategies into solutions

1.2.1 Strengthening the sense of responsibility

A successful implementation of the security strategy into solutions in the automation systems can only be achieved if all the parties involved cooperate responsibly. This includes:

- manufacturers (development, system test, security test)
- systems integrator (planning, structure, factory acceptance test)
- owner/operators (operation and administration).

The strategies and their implementation must be supervised and updated throughout the complete service life of the system (from the beginning of submitting the offer, planning and design to the migration and de-installation of a system).

The following capabilities make it possible for a protection concept in automation systems to be effective:

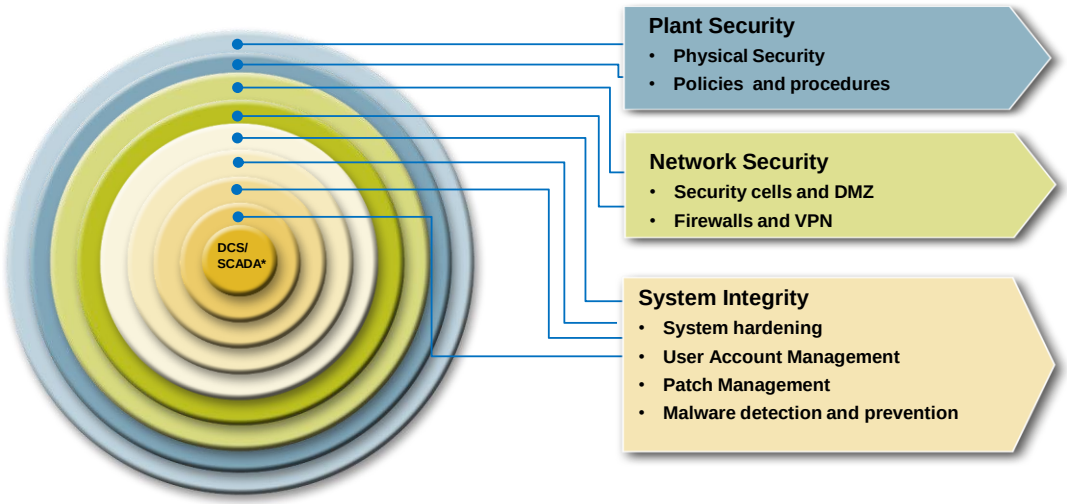
- the use of highly available and system-tested products, which have hardened and pre-defined security settings, and have been especially designed for industrial applications,
- a modern configuration, using state-of-the-art technologies and standards and allows for a system design adapted to the customer's security needs,
- the careful and responsible operation of systems and components in accordance with the uses defined by the manufacturer.

1.2.2 The Siemens protection concept: “Defense in Depth”

Siemens follows the “Defense in Depth” strategy in order to achieve the required security goals. The approach of this strategy is a multi-layer security model consisting of the following components:

- Plant Security
- Network security
- System integrity

Figure 1-1



The advantage of this strategy is the fact that an attacker first has to break through several security mechanisms to do any damage. The security requirements of each layer can be taken into account individually.

The Siemens solution for plant security

Implementation of an appropriate, comprehensive security management is the basis for planning and realizing an industrial security solution.

Security management is a process mainly comprising four steps:

- Risk analysis with definition of risk reduction measures: These measures must be defined for the plant, depending on the threats and risks identified.
- Determination of guidelines and coordination of organizational measures.
- Coordination of technical measures.
- A consistent security management process with regular or event-dependent repetition of risk analysis.

The Siemens solution for network security

If controllers or other intelligent devices with no or minimum self-protection are located in a network segment, a good option to consider is to create a secured network environment for these devices. One approach to achieve this is by the use of network security appliances. . Additional security can be provided by segmenting individual sub-networks, e.g. through a cell protection concept or a demilitarized zone (DMZ).

The Siemens security solution was developed particularly for the requirements of an automation environment, in order to meet the increasing demand of network

security, to reduce the susceptibility to failure of the entire production plant and thus to increase its availability.

Note Further information on this topic is available in the Siemens Industry Online Support (Entry ID: 27043887).
http://support.automation.siemens.com/WW/view/en/27043887

The Siemens solution for system integrity

In order to maintain the system integrity, it is important to minimize the vulnerabilities in PC systems and in the control level. Siemens meets this requirement with the following solutions:

- use of antivirus and whitelisting software,
- patch management,
- user authentication for machine or plant operators,
- integrated access protection mechanisms in automation components,
- protection of the program code through know-how protection, copy protection, and assignment of passwords.

1.3 Differences between office security and industrial security

The security mechanisms integrated in PCs and Windows operating systems generally provide a high level of security. However, these measures are typically designed for the requirements of office environments. In industrial security, the objects to be protected are quite similar, but, to some extent, their priorities differ significantly. While the top priorities in office IT are typically the confidentiality and integrity of information, plant availability or operability come first in industrial security. When selecting appropriate security measures, it must always be ensured that they provide the necessary level of protection without having unacceptable impact on the actual operation.

1.4 Differences between functional safety and industrial security

Functional safety addresses protection of the controlled environment against abnormal operation of the system. On the other hand security addresses protection of normal operation of a system against intentional or unintentional violations. However safety systems also need to be particularly protected against such violations.

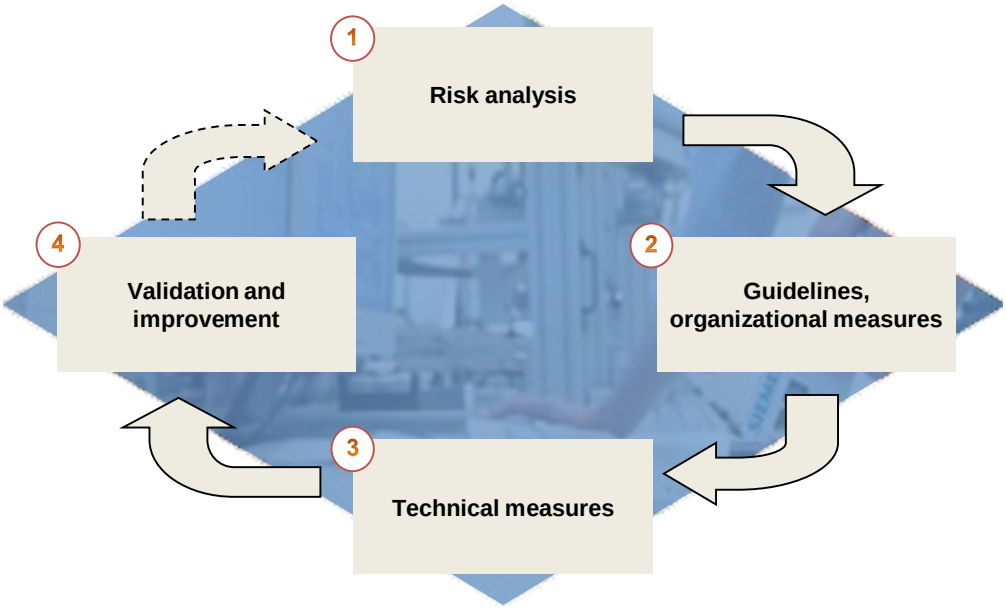
It's a machine vendor's task to establish appropriate safety mechanisms. These mechanisms must not primarily be included into the defense in depth concept, even if they can contribute.

Whereas safety threats are basically static, security threats are dynamic during lifetime of a machine / plant. Therefore the security protection needs to be continuously revised.

1.5 Security management

Security management is an integral part of an industrial security concept to address all security-relevant aspects of an automation solution – either a single machine, a plant section or an entire plant. As the potential threats to an automation solution change over its life cycle a process to monitor and detect these threats, known as security management, should be considered. The objective of this process is to achieve the necessary security level of an automation solution and to maintain it on a permanent basis. The risk analysis component contained within a security management process ensures that only appropriate countermeasures will be implemented to reduce the risks. An example of a security management process is as follows:

Figure 1-2



2 Security Mechanisms of the S7 CPU

The following chapters show which integrated access protection mechanisms the SIMATIC S7 controllers offer

2.1 Block protection

Overview

In STEP 7 V5.x and in STEP 7 (TIA Portal), there are different protection facilities - to protect the know-how of the programs in the blocks against unauthorized persons.

- Know-how protection
- S7 Block Privacy

If a block protected by this function is opened, only the block interface (IN, OUT and IN/OUT parameters) and the block comment can be read. The program code, temporary/static variables and the network comments are not displayed.
It is not possible to modify a protected block.

The following table gives an overview of the individual know-how protection facilities:

Table 2-1

Development environment:	Language	Module protection	Validity
STEP 7 V5.x	• LAD / FBD / STL • SCL • S7-GRAPH • CFC	Know-how protection (not password-protected)	S7-300/400/ WinAC
STEP 7 V5.5	• LAD / FBD / STL • S7-SCL	S7 Block Privacy (password-protected)	S7-300/400
STEP 7 (TIA Portal)	• LAD / FBD / STL • S7-SCL • S7-GRAPH	Know-how protection (password-protected)	S7-300/400
	• LAD / FBD • S7-SCL		S7-1200 (V4)
	• LAD / FBD / STL • S7-SCL		S7-1500

Overview of the blocks

S7 Block Privacy

With the S7 Block Privacy, only FBs and FCs can be protected.

Know-how protection

With the attribute KNOW_HOW_PROTECT a know-how protection mechanism for blocks of type OB, FB and FC can be activated.

Instance data blocks cannot be protected manually since they depend on the know-how protection of the assigned FB. This means that the instance data block of a password-protected FB also contains a know-how protection. This does not depend on whether the instance data block has been explicitly created or generated by a block call.

In TIA Portal are also global data blocks allowed. ARRAY-data blocks could not be protected with know-how protection.

Limitations

Blocks with a block protection cannot be further processed in STEP 7 (without correct password). Nor are testing and commissioning functions such as “Monitor blocks” or “Stops” possible. Only the interfaces of the block remain visible.

The following actions can be carried out with a protected block:

- copy and delete
- call the protected block
- online/offline comparison
- load

S7 Block Privacy

S7 Block Privacy is a STEP 7 expansion pack from V5.5 onwards for protecting functions and function blocks.

When using S7 Block Privacy, the following must be observed:

- S7 Block Privacy is operated via the context menus.
- Blocks once protected can only be unprotected with the correct password and according to the enclosed recompilation information. Therefore it is recommended to keep the password in a safe place and/or make copies of the unprotected blocks.
- Protected blocks can only be loaded to 400 CPUs from version 6.0 onwards, on 300 CPUs only from version 3.2.
- If there are sources in the project, the protected blocks can be restored by means of the sources by compilation. The sources can be completely removed from the S7 Block Privacy.

Note Further information for setting the block protection with the S7 Block Privacy can be found in the FAQ “How can the improved block protection for FBs and FCs be set up in STEP 7 V5.5? (Entry ID: 45632073).
http://support.automation.siemens.com/WW/view/en/45632073

Know-how protection (STEP 7 V5.x)

Blocks in STEP7 V5.x can be protected by adding a block attribute. The code word KNOW_HOW_PROTECT is indicated during programming of the block in the source.

The block protection can only be revoked with the STL source. If the STL sources are no longer available to the program or the project, the protection for the blocks cannot be removed.

It is recommended to use S7-Block Privacy instead as an improved know-how protection mechanism.

Note Further information on setting up the block protection can be found in the KNOW_HOW_PROTECT FAQ “How can a block protection be installed for blocks I created myself?” (Entry ID: 10025431).

http://support.automation.siemens.com/WW/view/en/10025431

Know-how protection (TIA Portal)

In the TIA Portal, the block protection is set via the context menu by indicating a password.

The following must be observed:

- In the comparison between the offline and the online version of know-how-protected blocks, only the data that are not protected will be compared.
- No type of a know-how-protected block can be created in the library. If such a block is added to a library, the new copying template also contains the know-how protection. There, you need the correct password of the know-how-protected block for using the copies.
  If a know-how-protected block is to be used in a library without disclosing the password, the following items have to be observed for programming these blocks:
  - During compilation all the code and data blocks called must be known. So it is not possible to make any indirect calls.
  - For programming the blocks, the use of PLC variables and global data blocks should be avoided.

Note

Further information can be found in the STEP 7 (TIA Portal) online help at:

- Set up know-how protection for blocks
- Open know-how-protected blocks
- Remove know-how protection for blocks

For S7-1200 (V4) and S7-1500-PLCs an additional copy protection can be set up which binds execution of the block to the PLC to the memory card with the defined serial number.

2.2 Online access and function restrictions

CPU protection levels

The S7 CPU offers three (S7-300/S7-400/WinAC) or four (S7-1200(V4)/S7-1500) access levels to limit the access to certain functions.
Setting the access level and the passwords restricts the functions and memory areas that are accessible without a password.
The individual access levels and the respective passwords are defined in the object properties of the CPU.

Table 2-2

Access levels	Access restriction
Level 1 (no protection)	The hardware configuration and the blocks can be read and modified by anyone.
Level 2 (write protection)	With this access level, only read access is allowed without a password, which means that the following functions can be carried out: • reading the hardware configuration and the blocks • reading diagnostic data • loading the hardware configuration and the blocks into the programming device. • changing the operating state (RUN/STOP) (not for S7-300 / S7-400 / WinAC) Without the password the following functions cannot be carried out: • loading the blocks and hardware configuration into the CPU • writing test functions • firmware update (online)
Level 3 (write/read protection)	At this access level, only • HMI access and • reading diagnostic data is possible without a password. Without the password the following functions cannot be carried out: • loading the blocks and hardware configuration into or from the CPU, • writing test functions • changing the operating state (RUN/STOP) (not for S7-300 / S7-400 / WinAC) • firmware update (online).
Level 4 (complete protection) S7-1200 (v4) S7-1500	With a complete protection, the CPU forbids: • read and write access to the hardware configuration and the blocks, • HMI access, • modifications in the server function for PUT/GET communication, • read and write access in the area “Accessible devices” and in the project for devices that are switched online.

Operating behavior with activated protection level

A password-protected CPU has the following behavior during operation:

- The protection of the CPU becomes effective when the settings have been loaded into the CPU and a new connection is established.
- Before an online function can be carried out, it is first checked whether it is admissible, and if there is a password protection, the user is asked to enter the password.
- The functions protected by a password can only be carried out by a single PG/PC at a time. No other PG/PC can login with the same password.
- The access rights to the protected data applies only for the duration of the online connection or until the access authorization has been removed manually with “Online > Remove access rights”

Note The configuration of an access level does not replace the know-how protection. This prevents unauthorized modifications in the CPU by restricting the download rights. The blocks on the SIMATIC memory card, however, are not write or read-protected. For protecting the program code, the know-how protection must be used.

2.3 Copy protection (S7-1200 (V4) / S7-1500)

Copy protection makes it possible to associate the entire program or the individual block with a specific SIMATIC memory card or CPU. By associating the program elements with a serial number of a SIMATIC memory card or a CPU, it is only possible to use this program or this block in combination with this defined SIMATIC memory card or CPU.

If a block with a copy protection is loaded into a device that does not correspond to the serial number defined, the complete loading process is rejected. This also means that even blocks without copy protection cannot be loaded.

The copy protection and the entries of the respective serial numbers are made in the block properties.

Note If such a copy protection is installed for a block, it is important that this block also contain block know-how protection. Without know-how protection, anyone would be able to remove the copy protection.

However, the copy protection must be installed first, since the settings for the copy protection are write-protected if the block has know-how protection.

2.4 Local access protection (S7-1500)

Locking the CPU

The SIMATIC S7-1500 has a front flap with a display and operating buttons. For inserting and removing the SIMATIC memory card and for manual changes of the CPU operating state, it must be opened.

For the protection of the CPU against unauthorized access, this front flap can be secured with the locking hatch. Two options are available:

- securing the front flap with a lock
- securing the front flap with a seal

Figure 2-1

Locking the display

In the display you can block the access to a password-protected CPU (local locking). The access protection is only effective when the operating mode switch is in the RUN position. The access protection is effective independent of the password protection, i.e. even if somebody accesses the CPU through a connected programming device and enters the correct password, the access to the CPU will still be denied. The access protection can be set separately for every access level in the display, which means that for example read access is locally permitted, but write access is not permitted locally. You can configure a password for the display in STEP 7 in the properties of the CPU in such a way that the local access protection is ensured by a local password.

2.5 Further measures for protecting the CPU

The following measures additionally increase the protection against unauthorized access to the functions and data of the S7 CPU from outside and within the network:

- deactivate or restrict the web server
- deactivate the time synchronization via NTP server
- deactivate the PUT/GET communication (S7-1200(V4)/ S7-1500)

Note In the default configuration of the modules, these functions are deactivated.

Security functions for the web server

With the web server you can remote control and monitor the CPU via the company Intranet. Evaluations and diagnostics are therefore possible over great distances.

However, the risk of unauthorized accesses to the CPU can increase by activating the web server.

If you wish to activate the web server, we recommend the following measures:

- do not connect the CPU web server directly to the internet
- protect access to the web server via the use of appropriate network segmentation, DMZ, and security appliances.
- access the web server via the secure transmission protocol “https”,
- configure the user and functions rights via the user list
  - create a user
  - define execution rights
  - assign passwords.

Users can only perform the functions that have been established as part of the user administration configuration. Once a user has been configured he can log in with his password and access the websites according to his access rights. By default, a user with the name “Everybody” has been set. This user has minimum access rights (read access to the intro and start page). The user “Everybody” has been set without a password and cannot be modified.

Deactivate the PUT/GET communication (S7-1200(V4)/ S7-1500)

The CPU can be the server for a number of communication services. In this mode, other communication devices can access the CPU data without having been configured or programmed explicitly for the CPU. In the same way the local CPU does not have the possibility of controlling the communication to the clients. Whether this type of communication is admissible for the local CPU or not, is defined in the object properties of the CPU.

In the default configuration, the option “Access via the PUT/GET communication…” is deactivated. In this case, read and write access to the CPU data is only possible for those communication connections which require programming for the local CPU and for the communication partner (e.g. Access via BSEND / BRECV instructions, is possible even in the default configuration).

Communications, for which the local CPU is only server (that means, that there is no configuration / programming of the communication to the communication partner), are not possible in the operation of the CPU.

This includes:

- PUT/GET, FETCH/WRITE or FTP access via communication modules
- PUT/GET access by other S7-CPUs
- HMI access via PUT/GET communication

3 Security Mechanisms of the S7-CPs

The following chapters show which security mechanisms the SIMATIC S7-CPs (CP x43-1 Advanced V3 and CP 1x43-1) offer.

Note The functions in CP 1543-1 can be configured from STEP 7 Professional V12 including update 1 onwards.
The CP 1243-1 needs STEP 7 Professional V13 Update 3 or higher..

Figure 3-1

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

3.1 Stateful Inspection Firewall

Description

Firewalls make it possible to filter the incoming and outgoing traffic that flows through a system. A firewall can use one or more sets of “rules” to inspect network packets as they come in or go out of network connections and either allows the traffic through or blocks it. The rules of a firewall can inspect one or more characteristics of the packets such as the protocol type, source or destination host address, and source or destination port.

The filter capabilities of a package filter can be improved considerably if the IP packages are checked in their proper context. For instance, a UDP package arriving from an external computer should only be forwarded internally if another UDP package has been sent to that computer shortly before from within the network (e.g. in case of a DNS request of a client in the internal network to an external DNS server). To enable this, the package filter must maintain records of all states to all current connections. Package filters that are able to do this are therefore referred to as **Stateful**.

Properties

Stateful Inspection Firewalls have the following properties:

- with TCP connections: Imitation of the status monitoring of a complete TCP/IP protocol stack
- with UDP connections: simulation of virtual connections
- creation and deletion of dynamic filter rules.

3.2 Data encoding via VPN

Description

A VPN (virtual private network) is a private network that uses a public network (like the Internet) for the transmission of private data to a private target network. The networks need not be compatible with one another.

Although VPN uses the addressing mechanisms of the carrier network it still uses its own network packages to separate the transport of private data packages from the others. Due to this fact, the private networks appear as a shared logical (virtual) network.

IPSec

An important aspect for the communication of data across network boundaries is IPSec (IP security). It is a standardized protocol suite and provides for manufacturer-independent, secure, and protected data exchange via IP networks. The main object of IPSec is protecting and securing the data during a transmission via an insecure network. Known weaknesses such as the intercepting and changing of data packages can be prevented by this security standard, due to encrypted data packages and authentication of the devices.

3.3 NAT/NAPT (address translation)

Description

Network Address Translation (NAT) / Network Address Port Translation (NAPT) are methods for converting private IP addresses into public IP addresses.

Address conversion with NAT

NAT is a protocol for address conversion between two address spaces. The main task is the conversion of public addresses, i.e. IP addresses used and routed on the Internet into private IP addresses and vice versa.

Through the use of this technology the addresses of the internal network are not visible in the external network. In the external network, the internal nodes are only visible via external IP addresses defined in the address conversion list (NAT table).

The typical NAT is a 1:1 conversion, i.e. a private IP address is converted to a public one.

The target address for the internal nodes is therefore an external IP address.

The NAT table contains the assignment of private and public IP addresses and is configured and managed in the gateway or router.

Address conversion with NAPT

NAPT is a variant of NAT and is often considered to be identical. The difference to NAT is the fact that ports can be converted too with this protocol.

The IP address is no longer converted 1:1. Instead, there is only one public IP address which is converted to a number of private IP addresses by adding port numbers.

The target address for the internal nodes is an external IP address with a port number.

The NAPT table contains the assignment of external ports to private IP addresses including port numbers and is configured and managed in the gateway or router.

3.4 Secure IT functions

3.4.1 File Transfer Protocol (FTP)

Description

The File Transfer Protocol is a specified network protocol for data transmission between an FTP server and an FTP client, or between two FTP servers.

FTP allows for exchanging data, creating and renaming directories, and also deleting them. The communication between FTP client and FTP server is an exchange of text-based commands. Each command sent by the FTP client results in a feedback by the FTP server in the form of a status code and a message in plain text.

For this, FTP creates two logical connections: a control channel via port 21 for the transmission of FTP commands and their responses as well as a data channel via port 20 for data transmission.

With a passive FTP, the two channels are initiated by the FTP client, whereas with active FTP the server initiates one of the channels to the client.

Solution for a secure FTP is FTPS

Secure data transmission with FTP is achieved with a combination of FTP and the SSL protocol and uses the same ports as in the normal FTP mode (port 20/21).

A certificate which is generated and delivered with the configuration of the security CP is used as the key for SSL.

Secure FTP data transfer with CPx43-1 Advanced V3 is only possible if the security function is enabled and is explicitly permitted in the configuration of the CP.

3.4.2 Network Time Protocol (NTP)

Description

The Network Time Protocol (NTP) is a standardized protocol for synchronizing the time on several computers / components across the network. The precision is within the millisecond range.

An NTP server makes the time available to the NTP clients.

NTP (secured)

NTP (secure) allows for secure and authenticated time synchronization by means of authentication methods and a joint encryption code. Both the NTP server and the NTP clients must support this function.

A secure time synchronization is supported by CP x43-1 Advanced V3 and CP 1x43-1, if the Security Function is activated and the expanded NTP configuration has been explicitly activated in the configuration.

3.4.3 Hypertext Transfer Protocol (HTTP)

Description

The Hypertext Transfer Protocol (HTTP) is part of the family of Internet protocols and is a standardized procedure for transferring data within a network. HTTP is primarily used for loading websites from a web server to a web browser.

HTTPS

Data transported via HTTP are readable as plain text and can be intercepted by third parties.
Today particularly – in the age of online banking, online shopping, and social networks – it is important that the transmission of confidential and personal data is secure and protected against unauthorized access.
The Hypertext Transfer Protocol Secure (HTTPS) is the easiest way of securely transmitting data.
HTTPS has the same structure as the HTTP protocol, but in addition it uses the Secure Socket Layer Protocol for encryption.
Many of the latest models of SIMATIC CPU's and CP's support HTTPS, and can be configured to use HTTPS exclusively, providing an increased level of security for data transmission.

3.4.4 Simple Network Management Protocol (SNMP)

Description

SNMP – Simple Network Management Protocol – is a UDP-based protocol that was specified particularly for the administration of data networks and in the meantime has established itself also as a de facto standard for TCP/IP devices.
The individual nodes in the network – network components or terminals – feature a SNMP agent that provides information in a structured form. This structure is referred to as MIB (Management Information Base). In the network node, the agent is usually implemented as firmware functionality.

Management Information Base – MIB

An MIB (Management Information Base) is a standardized data structure consisting of different SNMP variables, which are described by a language independent of the target system. Due to the cross-vendor standardization of MIBs and access mechanisms, even a heterogeneous network with components from different manufacturers can be monitored and controlled. If component-specific, non-standardized data is necessary for network monitoring, this data can be described by the manufacturers in “private MIBs”.

Secure SNMP (SNMPv3)

There are several versions of SNMP: SNMPv1, SNMPv2, and SNMPv3. The original version SNMPv1 and SNMPv2 are sometimes still used. However, it is recommendable not to use SNMPv1 and SNMPv2 since security mechanisms have not been implemented in these versions, or only in a restricted way.
From version 3, SNMP additionally offers user administration with authentication and optional encryption of data packages. Security with SNMP was substantially improved by these aspects.
The secure SNMP is supported by CP x43-1 Advanced V3 and CP 1x43-1, if the Security Function is activated and SNMPv3 has been explicitly activated in the configuration.

4 The Achilles Certification Program

Motivation

Security in industrial automation can only be achieved if manufacturers, suppliers, users and operators cooperate. An important part of the cooperation is the creation of international standards that are to be applied universally as a basis for future-oriented security concepts and solutions.

Creating uniform standards

The standards

- ISA 99 “Manufacturing and Control Systems Security”,
- the IEC 62443 “Security for Industrial Process Measurement and Control – Network and System Security”,
- the German guideline VDI/VDE 2182 “Informationssicherheit in der industriellen Automatisierung” (information security in industrial automation),

are of particular importance for the creation of uniform standards that are to be used universally.

While the latter deals with the procedures and mechanisms for securing automation components and systems, the ISA Security Compliance Institute (ISCI) meets the challenge of creating a uniform certification framework.

The Achilles certification program

The Achilles certification program by Wurldtech is considered an international standard for cyber security.

The certificate confirms that the automation systems have the necessary communications robustness to improve the security and stability of industrial plants. Achilles certification serves as an important criterion for the selection of products with robust communication systems. The Achilles certification program confirms that the Siemens control systems are resistant to network attacks. The certification program is divided in two levels:

- Achilles Communications Certification Level 1: The first level of the certification program confirms the robustness of the Ethernet, IP, ARP, ACMO, TCP and UDP in the modules with a special test program. If they meet all the test requirements, the modules get the Achilles Level 1 certification.
- Achilles Level 2 Certification: This second level comprises the same protocols as Level 1. However, every protocol is tested more intensively. In addition, Level 2 contains more tests, Denial-of-Service (DoS) tests with a higher link rate and more requirements.
  The tested Siemens Industry modules all have the Achilles Level 2 certification.

5 Literature

Bibliography

This list is by no means complete and only presents a selection of related references.

Table 5-1

	Subject	Title
/1/	STEP7 SIMATIC S7-300/400	Automating with STEP7 in AWL and SCL Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-397-5
/2/	STEP7 SIMATIC S7-300/400	Automating with STEP 7 in KOP and FUP Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-296-1
/3/	STEP7 SIMATIC S7-300	Automating with SIMATIC S7-300 inside TIA Portal Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-357-9
/4/	STEP7 SIMATIC S7-400	Automating with SIMATIC S7-400 inside TIA Portal Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-372-2
/5/	STEP7 SIMATIC S7-1200	Automating with SIMATIC S7-1200 Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-355-5
/6/	STEP7 SIMATIC S7-1500	Automating with SIMATIC S7-1200 Author: Hans Berger Publicis MCD Verlag ISBN: 978-3895784033
/7/	SIMATIC NET security	SIMATIC NET Industrial Ethernet Security Basic Principles and Application Configuration Manual http://support.automation.siemens.com/WW/view/en/56577508
/8/	S7-1500 Manual	SIMATIC S7-1500 Automation system http://support.automation.siemens.com/WW/view/en/59191792
/9/	S7-1200 Manual	SIMATIC S7-1200 Automation system http://support.automation.siemens.com/WW/view/en/36932465
/10/	S7-400 Manual	SIMATIC S7-400 Automating System S7-400 CPU-Data http://support.automation.siemens.com/WW/view/en/53385241
/11/	S7-300 Manual	SIMATIC S7-300, CPU 31xC and CPU 31x: Technical Data http://support.automation.siemens.com/WW/view/en/12996906
/12/	CP343-1 Advanced	System Manual Part B CP343-1 Advanced http://support.automation.siemens.com/WW/view/en/62046619
/13/	CP443-1 Advanced	System Manual Part B CP443-1 Advanced http://support.automation.siemens.com/WW/view/en/59187252
/14/	Manual CP1543-1	SIMATIC NET S7-1500 - Industrial Ethernet CP 1543-1 http://support.automation.siemens.com/WW/view/en/76476576

Internet link specifications

This list is not complete and only represents a selection of relevant information

Table 5-2

	Subject	Title
\1\	Reference to the entry	http://support.automation.siemens.com/WW/view/en/77431846
\2\	Siemens Industry Online Support	http://support.automation.siemens.com
\3\	Industrial Ethernet Security	http://support.automation.siemens.com/WW/view/en/18701555/130000
\4\	Getting Started S7-1500	http://support.automation.siemens.com/WW/view/en/71704272
\5\	Overview pages „All-round protection with Industrial Security”	https://support.industry.siemens.com/cs/de/en/view/50203404
\6\	Overview pages „Industrial Remote Communication“	https://support.industry.siemens.com/cs/de/en/view/64721753
\7\	Overview possible constellation with IP-based Remote Networks	https://support.industry.siemens.com/cs/de/en/view/26662448
\8\	SIMATIC NET Industrial Ethernet Security, Setting up security in STEP 7 Professional	https://support.industry.siemens.com/cs/de/en/view/109477192
\9\	SIMATIC NET Industrial Ethernet Security – setting up Security - Getting Started	https://support.industry.siemens.com/cs/de/en/view/109474411
\10\	SIMATIC NET - Industrial Ethernet Security - Security basics and application - Configuration Manual	https://support.industry.siemens.com/cs/de/en/view/109474417

6 History

Table 6-1

Version	Date	Modifications
V1.0	09/2013	First version
V2.0	03/2016	Add CP 1243-1, add futher links