SIEMENS

Security with SIMATIC controllers

STEP 7 / SIMATIC WinAC/S7-1200/ S7-1500

https://support.industry.siemens.com/cs/ww/en/view/90885010

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

Increasing networking and the use of technologies traditionally associated with the "office world" in automation facilities increase the need for security. It is not enough to simply offer superficial and limited protection, because attacks from the outside can occur on several levels. Optimal protection requires a deep awareness of security.

1.1 Security strategies

Motivation

Top priority is given in automation engineering to the maintaining production and process control. Any measures taken to prevent the propagation of security risks must not have a negative impact in this context. A satisfactory security strategy implementation should ensure that only authenticated users can perform authorized (permitted) operator inputs on authenticated devices using the operator input options assigned to them. These operator inputs should use only defined and planned access paths in order to ensure reliable production or coordination during a job without endangering people, the environment, the product, the goods being coordinated, or the company's business.

Strategies

Proceeding from these principles, a security concept encompasses general defense strategies that are intended to defend against the following attacks:

- Reduction of availability (e.g. "denial of service")
- Circumvention of specific security mechanisms (e.g. "man in the middle")
- Deliberate operator error using permitted actions (e.g. following password theft)
- Maloperations as a result of non-configured user access rights
- Data espionage (e.g. to find out formulas and trade secrets or discover how plants and their security mechanisms work)
- Data tampering (e.g. to make alarm messages appear innocuous)
- Deletion of data (e.g. deletion of log files to cover up attacks)

Siemens' defense strategy uses defense-in-depth mechanisms.

Defense in depth

The concept of defense in depth implies layers of security and detection, even on single-station systems. It possesses the following characteristics:

- Attackers are faced with breaking through or bypassing each layer without being detected.
- A flaw in one layer of the architecture can be protected by capabilities in other layers.
- System security becomes a set of layers within the overall network security structure.

1.2 Implementation of strategies as solutions

1.2.1 Strengthen a sense of responsibility

Successful implementation of the security strategies in the form of security solutions in automation facilities can only be accomplished when all parties involved cooperate with a awareness of shared responsibility. These parties primarily include:

- Manufacturers (development, system testing, security testing)
- Configuration engineers and integrators (design, setup, factory acceptance test)
- Owners (operation and administration)

These strategies and their implementation must be pursued and updated across the entire lifecycle of a plant (from initial tendering, planning and design to migration and finally to eventual decommissioning of the plant).

The following aspects make it possible for the security concept to achieve its intended effect in automation facilities:

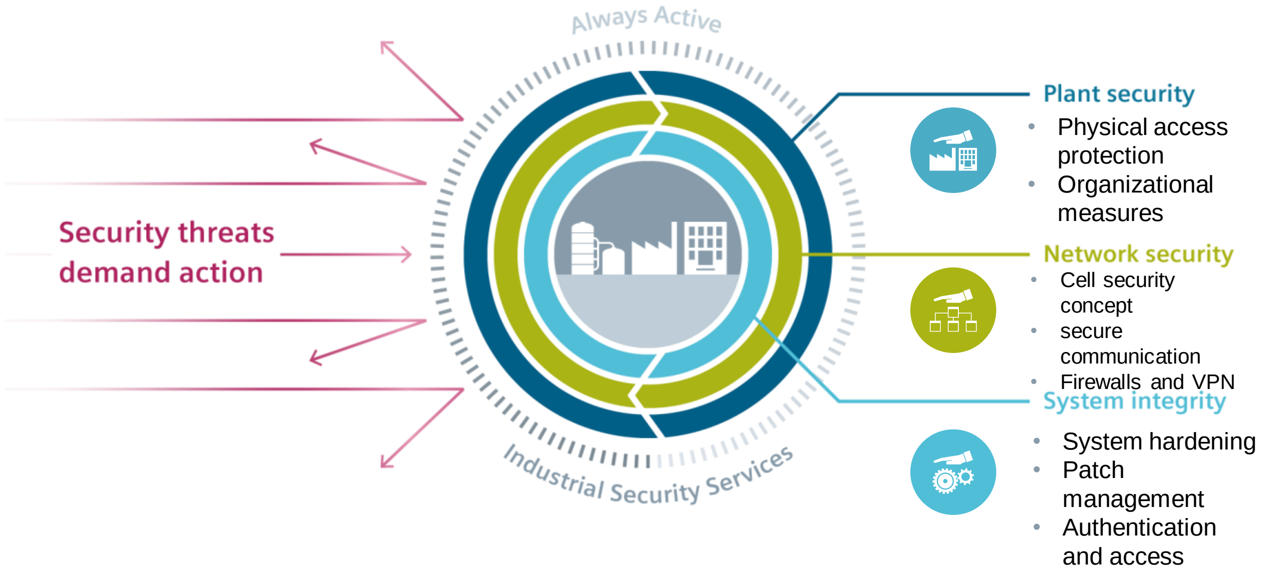
- Use of stable, fault-tolerant and system-tested products possessing baseline hardening (IP hardening) and predefined security settings, and which are specially designed for industrial use
- A cutting-edge configuration that uses current techniques and standards, allowing for a plant design that is adapted to the customer's security needs
- Careful and responsible operation of plants and components according to their potential applications as defined by the manufacturer

1.2.2 The Siemens protection concept: "Defense in depth"

Siemens operates on the "defense in depth" strategy to achieve its required security objectives. This strategy follows the approach of a multi-layered security model consisting of the following components:

- Plant security
- Network security
- System integrity

Figure 1-1 The "defense in depth" concept



The advantage of this strategy is that an attacker first needs to overcome multiple security mechanisms in order to cause damage. The security requirements of each of the layers can be tailored individually.

The Siemens plant security solution

Plant security prevents unauthorized persons from gaining physical access to critical components using a number of different methods. This starts with conventional building access and extends to securing sensitive areas with identity cards or access cards.

Comprehensive security monitoring leads to transparency with regard to the security status of production facilities. Thanks to continuous analyses and correlations of existing data and through comparison of these data with threat indicators, security-relevant events can be detected and classified according to risk factors.

The Siemens network security solution

If a network segment contains controllers or other intelligent devices that have little or no intrinsic protection, the only other option is to provide these devices a secure network environment. This is most easily done with special routers or gateways. These create security with integrated industrial-strength firewalls, and are themselves protected in the process. Additional security comes from segmenting individual subnets, for example by using the cell security concept or a demilitarized zone (DMZ). The security-related segmentation of the plant network into individually protected automation cells minimizes risks and increases security at the same time. The cells are divided and the devices assigned according to communication and protection requirements. Data transmission can be encrypted using "virtual private networks"

(VPN). In this way, data can be protected from espionage and manipulation. The communication partners are securely authenticated.

Readme

References

You can find an overview document on this topic in Siemens Industry Online Support (article ID: 92651441):

https://support.industry.siemens.com/cs/ww/en/view/92651441

The Siemens solution for system integrity

To safeguard system integrity, it is important to minimize weak points in PC systems and on the controller level. Siemens implements this requirement with the following solutions:

- Use of antivirus and whitelisting software
- Maintenance and update processes
- User authentication for machine or plant operators
- Access protection mechanisms are integrated into automation components
- Protection of the program code with know-how protection, copy protection and passwords

Readme

References

You can find an overview document on this topic in Siemens Industry Online Support (article ID: 92605897):

https://support.industry.siemens.com/cs/ww/en/view/92605897

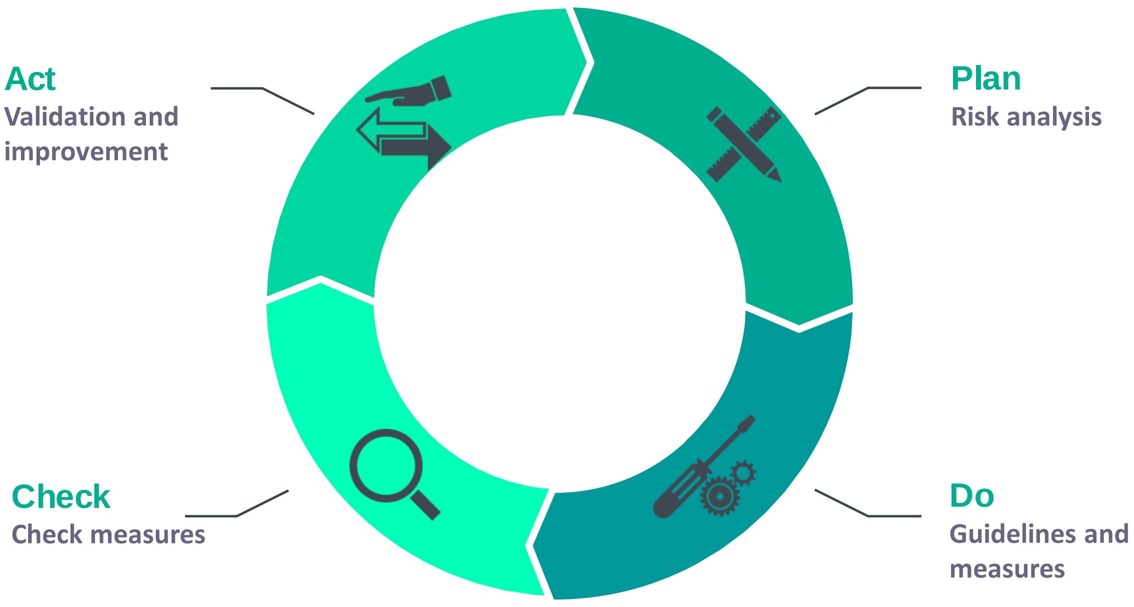
1.2.3 Security management

The basis for the design and realization of an industrial security solution is the implementation of expedient, overarching security management. Security management is a process which encompasses the following four essential steps:

- Risk analysis with definition of risk minimization measures: These measures have to be defined depending on the determined threats and risks for the plant.
- Definition of guidelines and coordination of organizational measures
- Coordination of technical measures
- Systematic security management process with regular or event-dependent repetition of a risk analysis

Security management forms an essential component of an industrial security concept for addressing security-related aspects of an automation solution – whether for a single machine, a subsystem or a complete plant. Since the risk environment of an automation solution changes over the lifecycle independent of the solution's actual function, the question at hand is rather one of a security management process. The goal of such a process is to attain and uphold the necessary security level of an automation solution. Establishing a security management process also ensures, for example, that the risk analysis entailed by the process only implements appropriate risk minimization countermeasures. Such a process could look like the following:

Figure 1-2 Security management process



1.3 Differentiation and differences

Differences between office security and industrial security

The integrated security measures of PCs and Windows operating systems generally provide a high level of security. However, these measures are typically oriented to the needs of the office environment. The objects requiring protection in the industrial security sector may be similar, but their priorities can differ greatly.

While the confidentiality and integrity of information typically has top priority in office IT, with industrial security it is plant availability and operator control that take precedence.

Therefore, when selecting suitable security measures, care should always be taken that these measures offer the necessary protection while not hindering actual operation.

Differences between functional security and industrial security

Functional security (safety) addresses the protection of the environment against malfunction of a system. On the other hand, industrial security addresses the protection of regular operation of a system against deliberate or inadvertent faults. However, even safety systems require protection against such faults.

It is the task of the machine's manufacturer to establish appropriate safety mechanisms. However, it is not permissible to make these mechanisms a primary part of the "defense in depth" concept even when they contribute to it.

While safety threats remain principally unchanged, security threats can change over the service life of a machine/plant. Therefore, regular adaptation of security is required.

2 Security mechanisms on the S7 CPU

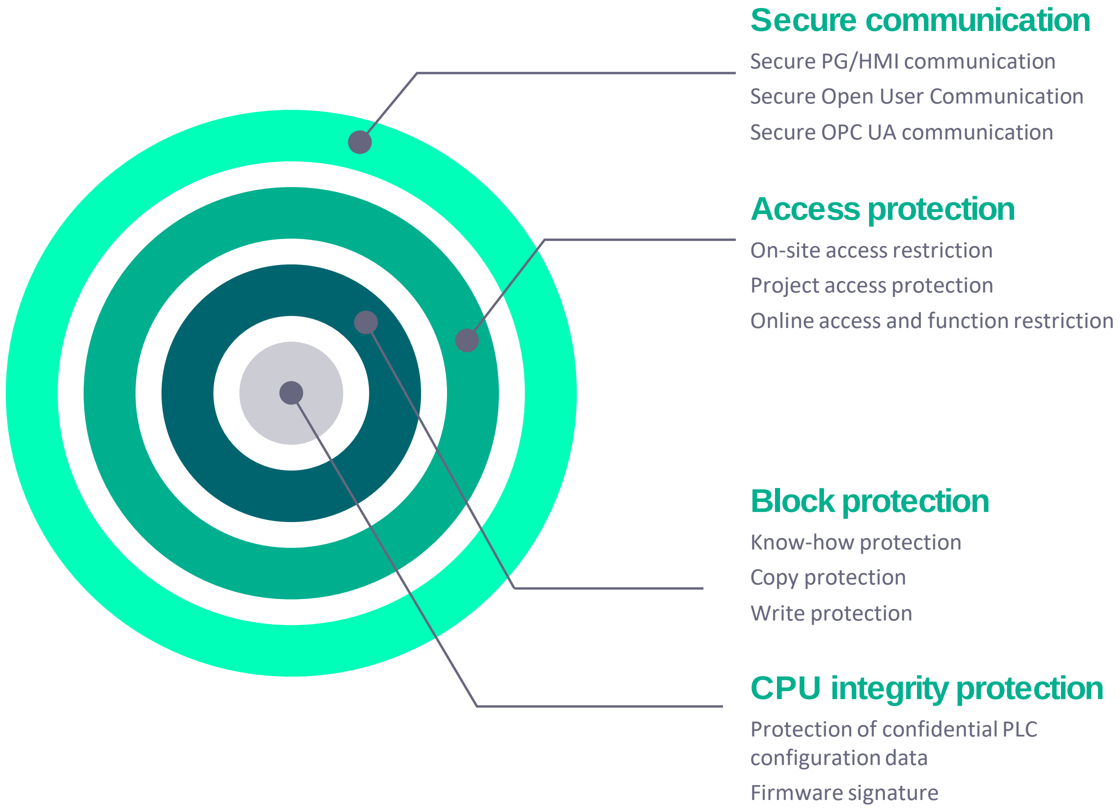
Overview

The chapters below list the integrated security mechanisms offered by SIMATIC S7 controllers.

The security mechanisms of the S7 CPU can be divided into 4 phases:

- Secure communication
- Access protection
- Block protection
- Integrity protection

Figure 2-1 S7 CPU security mechanisms


Secure communication
Secure PG/HMI communication
Secure Open User Communication
Secure OPC UA communication
Access protection
On-site access restriction
Project access protection
Online access and function restriction
Block protection
Know-how protection
Copy protection
Write protection
CPU integrity protection
Protection of confidential PLC configuration data
Firmware signature

2.1 Secure communication

Communication protection concerns the reliability and trust of data exchanged between communication partners. Data tampering by unauthorized users must be prevented.

Regardless of context, secure communication is based on the concept of public key infrastructure (PKI).

2.1.1 Overview

Public key infrastructure (PKI)

The attribute "secure" is used to describe communication mechanisms that rely on public key infrastructure (PKI). Public key infrastructure (PKI) refers to a system that can issue, distribute and verify digital certificates. Issued digital certificates are used in within the PKI to secure computer-based communication by signing and encrypting messages on the network.

Components that you have configured in STEP 7 (TIA Portal) for secure communication use an asymmetric key method with a public key and a private key. TLS (Transport Layer Security) is employed as the encryption protocol. TLS is the successor to the SSL (Secure Sockets Layer) protocol.

The essential principle of secure communication includes the following components:

- An asymmetric encryption protocol
  This protocol enables the following:
  - Encryption or decryption of messages using public or private keys
  - Verification of signatures on messages and certificates

  The messages/certificates are signed by the sender/certificate owner with that entity's private key. The recipient/verifier checks the signature with the public key of the sender/certificate owner.
- Transport and storage of public keys by means of X.509 certificates:
  - X.509 certificates are digitally signed data that make it possible to verify the veracity of public keys with respect to the associated identity.
  - X.509 certificates can contain more precise information about or restrictions on the use of public keys, for example, the date from which or until which a public key in a certificate is valid.
  - X.509 certificates contain information about the certificate issuer in secure form.

TIA Portal V17 lets the user use custom, user-specific certificates for communication partners, giving the system additional security. If one device is compromised, the other devices remain secure because they use other certificates. The certificates can be imported or, in TIA Portal, generated with the certificate manager. More information on the use of certificates in TIA Portal can be found at the following link: \3\ in chapter 4.3.

Objectives for secure communication

Secure communication is employed to achieve the following goals:

- Confidentiality, i.e. data are secret or non-readable to unauthorized eavesdroppers.
- Integrity, i.e. the message received by the recipient is the same unmodified message that was sent by the sender. The message was not modified along its transport path.
- Endpoint authentication, i.e. the communication partner as endpoint is exactly who it claims to be and is the intended destination. The identity of the communication partner is verified.

If these objectives were in the past primarily a concern for the IT world and networked computers, today machines and controllers with valuable data in the industrial environment are, because they are networked, subject to the very same dangers. They therefore pose stringent requirements for secure data exchange.

It is common practice to protect the automation cell with the cell security concept by using a firewall or a VPN connection, e.g. with the security module. However, there is increasing need to transmit data to external computers in encrypted form via an intranet or public networks.

Secure communication with STEP 7

As of V14, STEP 7 provides the PKI required for the configuration and operation of secure communication. This document describes in greater detail the following communication mechanisms:

- Secure PG/HMI communication
- Secure Open User Communication (OUC)
- Secure OPC UA communication

All of the methods listed above use the TLS (Transport Layer Security) protocol to safeguard the data in communication.

2.1.2 Secure PG/HMI communication

Overview

As of version V17, central components of TIA Portal, STEP 7 and WinCC work together with the latest controllers and HMI devices to implement innovative and standardized (secure) PG/PC communication and HMI communication, referred to as PG [programming device] / HMI communication for short.

Components

We refer in particular to the following CPU families:

- S7-1500 controller family with firmware version V2.9 or later
- S7-1200 controller family with firmware version V4.5 or later
- Software controller with firmware version V21.9 or later
- SIMATIC Drive Controller with firmware version V2.9 or later
- PLCSim and PLCSim Advanced version V4.0

In addition, HMI components have been updated to provide support for secure PG/HMI communication:

- Panels or PCs configured with WinCC Basic, Comfort and Advanced
- PCs with WinCC RT Professional
- WinCC Unified PCs and Comfort Panels

SINAMICS RT SW version V6.1 onward and STARTDRIVE version V17 onward have also been updated.

Properties of PG/HMI communication

The main feature of PG/HMI communication is its simplicity: Establishing an online connection from a programming device (with TIA Portal installed) to a CPU (for example to download a program) requires minimal effort. Here, the online connection also meets criteria such as confidentiality and integrity on the basis of an established SIMATIC communication standard.

In the process of integrating machines and plants into an open IT environment, however, it is also necessary to set up switches for communication between the programming device / HMI device and the CPU. Communication must not only be secure with respect to integrity and confidentiality of sensitive data, rather, communication security also needs to measure up to widely accepted security standards and thereby meet the requirements for the future.

As of TIA Portal version V17, PG/HMI communication has been upgraded: The TLS protocol (Transport Layer Security) is available to secure PG/HMI communication by means of standardized security mechanisms.

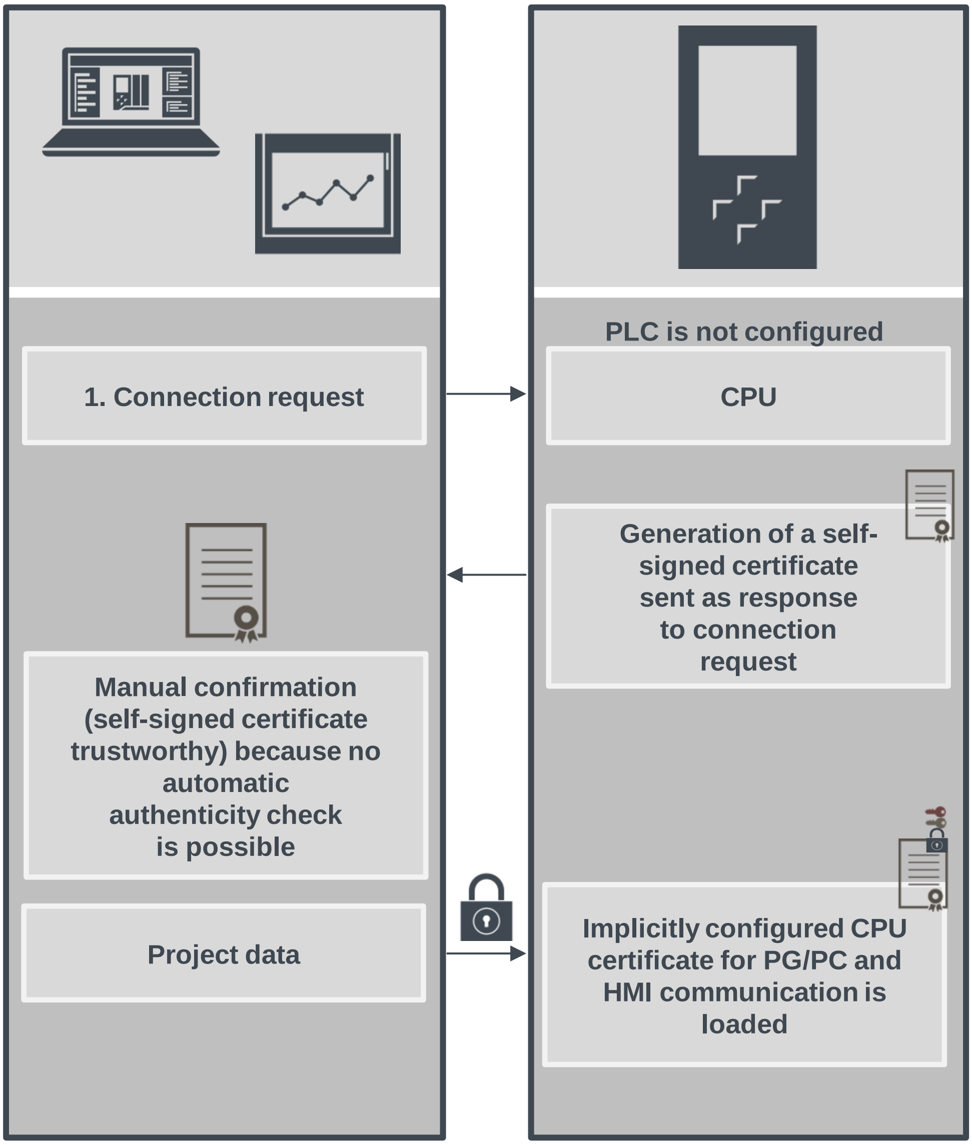
Process

Secure PG/HMI communication relies on the programming device and HMI panel verifying the authenticity of the CPU by means of the communication certificate (sent by the CPU when the connection is established) and recognizing the CPU as "trustworthy". Secure PG/HMI communication is only possible when the PG/HMI panel trust the CPU. When the connection is being established, the CPU transmits the communication certificate to the communication partner (programming device or HMI panel). To ensure that communication between the CPU and a programming device / HMI panel is secure, the CPU must possess a certificate. However, this certificate is only issued once the project is downloaded to the CPU. Secure communication between the programming device / HMI panel and CPU is described below.

Initial connection setup to the CPU – Preparation phase

The Figure below explains the initial connection setup sequence from a programming device or HMI panel to the CPU. This is known as the "preparation phase".

Figure 2-2 TLS connection setup


PLC is not configured
1. Connection request
CPU
Generation of a self-signed certificate sent as response to connection request
Manual confirmation (self-signed certificate trustworthy) because no automatic authenticity check is possible
Project data
Implicitly configured CPU certificate for PG/PC and HMI communication is loaded

Even the initial connection setup for downloading to the CPU is secured with the TLS protocol in the model of secure PG/HMI communication.

However, for this connection setup step, the CPU uses its manufacturer device certificate (if present) or a self-signed certificate. Use of the CPU is restricted in this phase. In this phase, the CPU waits for the provision of password-based key information. In simple terms: It is waiting for the password for sensitive PLC configuration data. See chapter 2.4.1. This phase is referred to below as the "preparation phase". The CPU indicates that it is in the preparation phase through a corresponding message in the diagnostic buffer.

Downloading a project to the CPU provides the CPU with the project data:

- Hardware configuration, including configured certificates for secure communication (OPC UA, HTTPS, secure OUC, secure PG/HMI communication)
- User program

Exiting the preparation phase

The password for confidential PLC configuration data and/or the key information generated from the password are not saved in the project by TIA Portal.

Therefore, the password will be requested in a series of dialogs during the initial download (or when a new project is downloaded), then transferred to the CPU. Only through this step is the

CPU able to use the protected PLC configuration data. This concludes the preparation phase and the CPU can go into RUN.

Note

> If you do not protect confidential PLC configuration data with a password, the password will not need to be entered during the initial download. While this does not affect the PG/HMI communication sequence, you must bear in mind that confidential PLC configuration data (e.g. private keys) have virtually no protection against unauthorized access. See chapter 2.4.1.

PG/HMI communication startup

When the CPU is loaded and it has received the CPU certificate for secure PG/HMI communication, the programming device will reconnect – this time on the basis of the downloaded CPU certificate.

2.1.3 Secure Open User Communication (OUC)

TCP/IP-based Open User Communication (OUC) has become the standard for communication with SIMATIC S7 CPUs. In the S7 CPU, OUC is implemented on the basis of instructions (e.g. TCON, TSEND, TRCV und TDISCON). To establish secure TCP communication with the S7 CPU, the data block with system data type TCON_IP_V4_SEC must be used.

S7-1500 CPUs with firmware version V2 or later support secure communication with addressing via a domain name server (DNS).

To set up secure TCP communication with a domain name, you must create your own data block with the system data type TCON_QDN_SEC, assign parameters and call the system data type right at the instruction. The TCON instruction supports the TCON_QDN_SEC and TCON_IP_V4_SEC system data type. As of firmware version V2.5, the TSEND_C and TRCV_C instructions also support the system data types TCON_QDN_SEC and TCON_IP_V4_SEC. Additional information on the structure of secure OUC and on the S7 CPU can be found at the following link: \4\ in chapter 4.3.

2.1.4 Secure OPC UA communication

OPC UA allows data exchange between different systems, both within the process and production level as well as with systems on the control and enterprise levels.

This option also contains security risks. For this reason, OPC UA offers a range of security mechanisms:

- Identify verification of OPC UA server and OPC UA clients,
- User identity verification, and
- Signed/encrypted data exchange between OPC UA server and OPC UA clients.

The security settings should only be circumvented when there is good reason to do so:

- During commissioning, or
- With island projects without an Ethernet connection to the outside world.

A secure connection between the OPC UA server and an OPC UA client is only established when the server can identify itself to the client. This is the purpose of the server certificate. Link \5\ in chapter 4.3 provides more information on working with the OPC UA server/client certificate in TIA Portal.

Automated certificate management with Global Discovery Server (GDS)

As of firmware V2.9, the OPC UA server of the S7-1500 CPU supports certificate management services which can be used by a Global Discovery Server (GDS), for example.

Using GDS push management functions, OPC UA certificates, trusted lists and Certificate Revocation Lists (CRLs) can be updated for the OPC UA server of the S7-1500 CPU on an automated basis. Automation of certificate management saves manual effort in giving the CPU a new configuration, for instance, after a certificate's validity period expires and the CPU is redownloaded. In addition, you can use the GDS push management functions to transfer updated certificates and lists in the CPU's STOP and RUN states. More information on OPC UA certificate management with GDS can be found at link \6\ in chapter 4.3.

2.2 Access protection

Access to the CPU should only be granted to authorized persons, processes and devices. This entails an on-site access restriction and system access to the CPU.

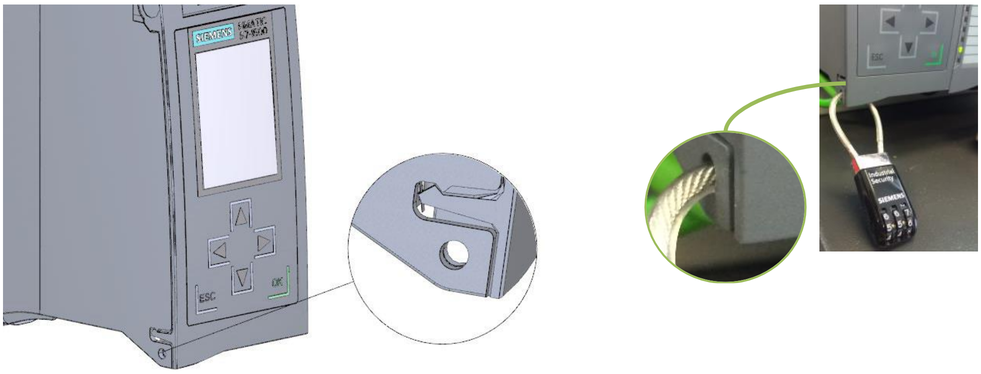
2.2.1 On-site access restriction (S7-1500)

CPU lock

The SIMATIC S7-1500 has a hinged front cover with a display and control keys. It must be opened in order to insert or remove the SIMATIC Memory Card, or to manually change the CPU operating state. To protect the CPU against unauthorized access, this front cover can be adequately secured with the locking tab. Your options include:

- Securing the front cover with a padlock, or
- Attaching a seal

Figure 2-3 CPU lock



Display lock

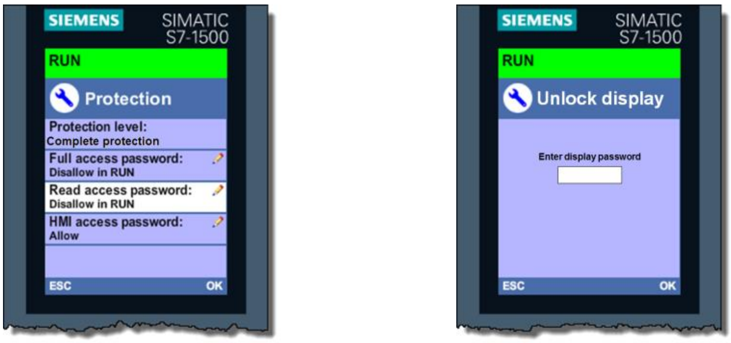
The SIMATIC S7-1500 additionally offers a password authentication function on the display. It is possible to configure a CPU access password for each access level. If access is disabled, the user receives a message in TIA Portal that the password is currently invalid. This on-site deactivation can, for example, offer additional protection against undesired, invalid configurations. The legitimation setting for the password is only active when the CPU is in RUN mode. If the CPU is in STOP mode, access with the passwords remains possible.

To protect the CPU functions that can be operated from the display, a display password can be defined in TIA Portal. This is accomplished in the CPU properties under "Display > Password". Due to the restricted character set and the difficulty of entering characters with the display keys, the password in this case is limited to uppercase letters and numbers.

Note

> If the CPU is in STOP mode, access with the appropriate password is possible regardless of the setting on the display.

Figure 2-4 Display lock



SIEMENS SIMATIC S7-1500

RUN

Protection

Protection level: Complete protection

Full access password: Disallow in RUN

Read access password: Disallow in RUN

HMI access password: Allow

ESC OK

SIEMENS SIMATIC S7-1500

RUN

Unlock display

Enter display password

ESC OK

2.2.2 Project access protection

TIA Portal provides a user management function (UMAC – User Management and Access Control) for projects. It allows you to create and manage users and roles in your project. You can also protect your project and define which user is allowed to perform which functions. When you set up project protection, you are created as the project administrator. Then you can create additional users and assign them roles with certain rights. After project protection is enabled, the project can only be opened and modified by authorized users.

Note Note that project protection cannot be removed once set up.

The project administrator can add the following users and user groups to a project:

- Local project users:
  Local project users are users who are defined and managed in a TIA Portal project. These user accounts are valid only for this one project. Using project user accounts is a good idea when the entire automation solution is created within one project.
  The system additionally creates the local project user "Anonymous". This user does not need to authenticate itself with a password. You can use roles to grant this user certain rights. Note that your project's security will be greatly diminished if you assign this user too many rights. The anonymous user "Anonymous" is disabled by default. It cannot be deleted.
- Global users and user groups:
  These user accounts are defined and managed outside of TIA Portal in UMC (User Management Component). You can import global users and user groups into the various TIA Portal projects that these users will be working on. Adding users and user groups from UMC requires the corresponding rights in UMC. Global users can also use the single sign-on method to authenticate themselves.

UMC – User Management Component

Additionally, you can install the "User Management Component UMC" software package on one or more computers. It provides central user management. This creates a system of interconnected UMC installations (UMC ring server, UMC server). In this UMC system, you can define users and user groups, or import them from a Windows Active Directory. When UMC is installed, you can access the UMC server from TIA Portal in order to add users and user groups (defined on the UMC server) to the TIA Portal user management. In this way you can also assign users and user groups the necessary function rights to a TIA Portal project via roles.

Within TIA Portal, however, you cannot modify the data of the users and user groups that were added from UMC. As a result, for example, you cannot change passwords or other data of UMC users or UMC user groups even if you are an administrator in the project. This is only possible in UMC. You nevertheless have the option of synchronizing the user management in TIA Portal with UMC, and you can check the synchronization status. This allows you to fix inconsistencies between the global users and user groups in UMC and the UMC users/user groups that have already been imported into TIA Portal.

2.2.3 Online access and function restriction

The S7 CPU has four access levels, in order to limit access to specific functions. Setting up the access level and password will limit the functions and memory ranges that are accessible without a password. The individual access levels and the associated passwords are defined in the object properties of the CPU. Legitimating oneself with a configured password grants access according to the associated protection level.

Table 2-1

Access levels	Restriction of access
Full access (no protection)	Hardware configuration and blocks can be read and changed by anyone.
Read access for F blocks (only with F-CPUs)	F blocks in the safety program cannot be modified without legitimation with the password associated with this access level or a higher access level.
Read access	This access level grants only write-protected access to the hardware configuration and the blocks unless the password is entered. Without the password, the following functions can be utilized: • Read the hardware configuration and blocks • Download the hardware configuration and blocks to the programming device • Read diagnostic data • Display online/offline comparison results • Set the time • Change operating mode (RUN/STOP) The following functions **cannot** be run without entering the password: • Download the blocks and hardware configuration to the CPU • Write-based test functions • Firmware update (online)
HMI access	This access level only allows the following when the password has not been entered: • HMI access • Read diagnostic data Example: With the "HMI access" access level, you can go online and display diagnostic icons for the states of objects. Tags can be read and written via an HMI device. The following functions **cannot** be run without entering the password: • Download the blocks and hardware configuration to/from the CPU • Display online/offline comparison results • Change operating mode (RUN/STOP) • Write-based test functions • Firmware update (online)

Access levels	Restriction of access
No access (complete protection)	Only identification data can be read, e.g. via "Accessible subscribers". With complete protection, the CPU forbids: • Read and write access to the hardware configuration and blocks • HMI access • Modification in the server function for PUT/GET communication

Operational performance with protection level activated

A password-protected CPU behaves as follows when in operation:

- The CPU protection takes effect once the settings are downloaded to the CPU and a new connection has been established.
- Before an online function is executed, the necessary permission is checked and, if password-protected, the user is prompted to enter a password.
- The password-protected functions can only be executed from a programming device or PC at any given time. Another programming device or PC cannot sign in with a password.
- Access permissions to the protected data apply while the online connection is active, or until the access protection is removed manually via "Online > Delete access permissions".

Going online with a password-protected CPU

Going online with a password-protected CPU requires read access as of STEP 7 V14. Therefore, you must enter the password for read access when you go online or, if no password was configured for this, you must enter the password for full access.

If you have a fully protected CPU and you only have a password for HMI access on hand, cancel the password prompt after the read access password prompt. You will then be prompted to enter the password for HMI access. The permission for HMI access is not sufficient for the online/offline comparison, however. For this you will need read access permissions.

Note

Configuring an access level is not a replacement for know-how protection.

It prevents improper modifications to the CPU by restricting download permissions. However, the blocks on the SIMATIC Memory Card are neither write-protected nor read-protected. Know-how protection should be used to safeguard the program code.

2.3 Block protection

Various block protection mechanisms are available in STEP 7 (TIA Portal) to protect the know-how in the blocks' programs from unauthorized persons.

2.3.1 Know-how protection

Know-how protection lets you guard blocks of type OB, FB, FC and global data blocks against unauthorized access by using a password.

Take the following features into account with know-how protection:

- You cannot manually protect instance data blocks; they are dependent on the know-how protection of the associated FB. This means that when you generate an instance data block for a know-how-protected FB, the instance data block likewise receives know-how protection. This happens regardless of whether you explicitly create the instance data block or whether it was generated by a block call.
- With global data blocks, you cannot edit the start values and comments, but this is possible with instance data blocks.
- ARRAY data blocks cannot be provided with know-how protection.
- Storage space requirements may be higher with know-how-protected blocks.
- During a comparison between the offline and online version of know-how-protected blocks, only the non-protected data are compared.
- Further access to the block is not possible without a password.
- When you add a know-how-protected block to a library, the resulting master copy also received know-how protection.

Restrictions

With a know-how-protected block, only the following data are readable without a password:

- Call parameters: Input, Output, InOut, Return, Static
- Block title
- Block comment
- Block properties
- Tags of global data blocks, minus information about the location of use

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

- Copying and deleting
- Calling in a program
- Offline/online comparison
- Downloading

Readme

References

You can find more information at the following link: \7\ in chapter 4.3, specifically regarding:

- Setting up know-how protection for blocks
- Opening blocks protected by know-how protection
- Removing know-how protection from blocks

2.3.2 Copy protection

Copy protection links a program or blocks with a specific SIMATIC Memory Card or CPU. By linking the serial number of a SIMATIC Memory Card or CPU, use of the program or block in question is only possible in connection with this specific SIMATIC Memory Card or CPU.

If a block with copy protection is downloaded to a device whose serial number does not match the defined serial number, the download process will be rejected. However, this does not mean that blocks without copy protection cannot be downloaded.

Copy protection is set up and the associated serial number is entered via the block properties.

Applications

- If the program is bound to the serial number of the CPU, use of TIA Portal to adjust the serial number is mandatory upon hardware replacement in the event of a fault.
- If the serial number is linked to the memory card, the hardware can be replaced and the memory card taken from the old CPU. Due to the fact that the program is stored on the memory card, it is still possible to ensure that the program only runs on one CPU.

Note

When setting up copy protection for a block, it is important that this block also receive block protection. Without know-how protection, anyone could reset the copy protection.

Copy protection must be set up prior to block protection. The copy protection settings are write-protected when the block has know-how protection.

There are two options for adding the serial number:

- Manual entry of serial number:
  The serial number must be known during the engineering phase.
- Automatic assignment during download:
  The serial number does not need to be known for engineering.
  During download to a new CPU, the password defined for copy protection is requested.

2.3.3 Write protection

Set up write protection for blocks of type OB, FB or FC to prevent inadvertent modifications.

Blocks with write protection can only be opened in read-only mode. However, you can still edit the block properties. There are no restrictions on diagnostics.

Note Note that write protection is not the same as know-how protection. When a block is write-protected, you cannot set up know-how protection on top of this. Remove the block's write protection if you want to give it know-how protection.

2.4 CPU integrity protection

Integrity refers to the protection of data against unauthorized modification or deletion.

In the context of CPU security, this entails the following:

- Protection of confidential CPU configuration data
- Protection of the CPU firmware signature

2.4.1 Protection of confidential PLC configuration data

Trouble-free functioning of certificate-based communication mechanisms for secure communication (see chapter 2.1) requires that the private keys employed by these certificates are protected as much as possible.

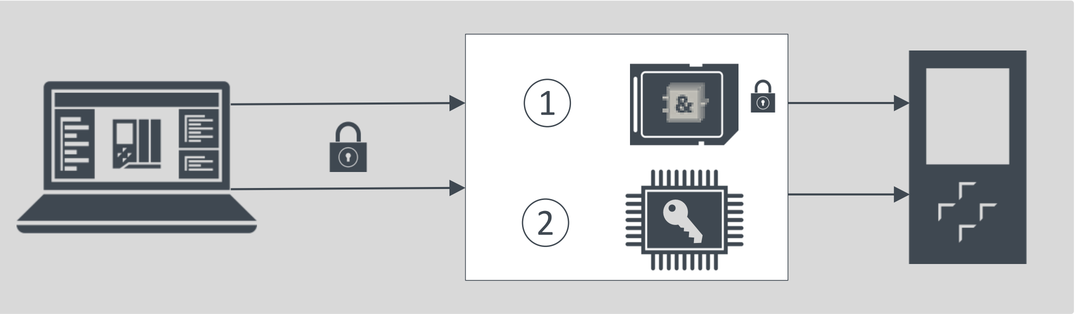
As of TIA Portal V17, you can set up a user defined password to protect these keys and other sensitive data.

Password for protecting confidential CPU configuration data

To protect the confidential configuration data of the CPU, for example certificates and private keys, enter the password in TIA Portal.

The following Figure is a simplified representation of how confidential CPU configuration data (for example a standard S7-1500 CPU) can be protected.

Figure 2-5 Secure memory concept



The project and key information is stored in different memory ranges during the initial download:

1. The project is stored in the load memory (SIMATIC Memory Card).
2. The key information is stored in a memory range in the CPU. This key is used to read the confidential configuration data on the SIMATIC Memory Card.

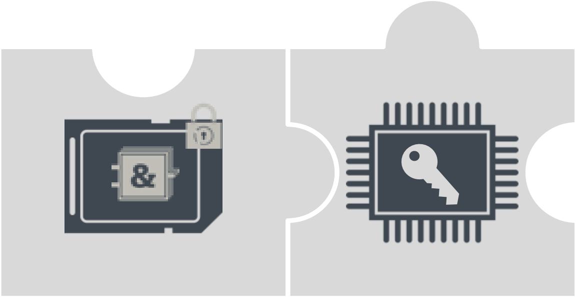
For target systems such as S7-1200 CPUs and software controllers with other storage concepts, the implementation is adapted to fit the relevant storage concept. The principle remains the same, however.

Two memory ranges for additional security

The project and the keys belong together like two interlocking puzzle pieces. The project is linked with the downloaded key information; the downloaded key information is in turn linked with the password that was assigned during configuration. The project and key information must match, otherwise the CPU will not start.

The principle of two separate memory ranges also applies for S7-1200 CPUs and S7-1500 CPU versions without a SIMATIC Memory Card, for example software controllers, PLCSIM or PLCSIM Advanced. In the versions without a SIMATIC Memory Card, two separate partitions are used so that the two information elements can be managed independently of one another.

Figure 2-6 Secure memory ranges



Readme

References

Further information on setting up protection of confidential PLC configuration data, as well as things to note when replacing the CPU, can be found at the following application example link:

https://support.industry.siemens.com/cs/ww/en/view/109798583

2.4.2 Firmware signature

Every CPU firmware is signed by Siemens. The CPU checks this signature at every firmware update. If the firmware signature verification fails, the firmware is not uploaded to the CPU. This ensures protection against manipulated firmware updates.

2.5 Additional CPU protection measures

The following measures additionally increase the protection against unauthorized access to functions and data on the S7 CPU, both externally as well as over the network:

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

Note These functions are disabled by default in the modules' default configurations.

Security functions for the web server

The web server allows you to remotely control and monitor the CPU via a company's internal intranet. This allows evaluation and diagnostics to be carried out remotely.

However, enabling the web server can increase the risk of unauthorized access to the CPU.

If you wish to enable the web server, the following measures are recommended for protecting the CPU:

- Access via the secure transmission "https" transmission protocol
- Configurable user and function privileges via user list
  - Create users
  - Define execution rights
  - Assign passwords

  User management grants users exclusively the options that are assigned to execution rights. If a user is configured, the user's password grants access to the web pages in accordance with the user's access rights.
  A user with the name "Jeder" [German: *Everyone*] has been preconfigured. This user has minimal access permissions (write-protected access to Intro and Start page). The "Jeder" user has been set without a password and cannot be modified.

Disable PUT/GET communication (S7-1200(V4)/S7-1500)

The CPU can act as a server for a number of communication services. Other communication participants can access CPU data even if you do not configure or program any CPU connections. This renders the local CPU, in its role as a server, incapable of controlling communication with the clients.

You can use the "Connection mechanisms" parameter in the "Protection" area of the CPU parameters to set whether this type of communication is permissible for the local CPU while in operation.

By default, the option "Allow access via PUT/GET communication from remote partners" is disabled. Read and write access to CPU data is only possible with communication connections that require configuration/programming not only for the local CPU but also for the communication partner. Access operations, such as those via BSEND/BRCV instructions, are possible.

Connections for which the local CPU is only a server (i.e. for the local CPU, no configuration/programming has been carried out for the communication to the communication partner) are this not possible when the CPU is in operation. Examples of such connections include:

- PUT/GET, FETCH/WRITE or FTP access operations via communication modules.
- PUT/GET access from other S7 CPUs
- HMI access operations implemented via PUT/GET communication

If you wish to allow client-side access to CPU data, i.e. if you do not wish to restrict the CPU's communication services, then enable the option "Allow access via PUT/GET communication from remote partners".

3 Security mechanisms on the S7 CPs

The chapters below show which security mechanisms are offered by the SIMATIC S7 CPs (CP x43-1 Advanced V3 and CP 1x43-1).

Note

> The functions in the CP 1543-1 are configurable as of STEP 7 Professional V12 incl. Update 1.
> The CP 1243-1 requires at least STEP 7 Professional V13 Update 3.

Figure 3-1 Types of CPs

3.1 Stateful inspection firewall

Description

The filtering performance of a packet filter can be greatly improved by checking the IP packets in their respective context. For example, it is desirable to let in a UDP packet inbound from an external computer only if another UDP packet was recently sent out to the same computer (e.g. in the event of a DNS query sent from a client in the internal network to an external DNS server). To enable this feature, the packet filter on all current connections must be able to manage a status. Packet filters with this capability are thus referred to as "stateful".

Properties

Stateful inspection firewalls have the following properties:

- With TCP connections: Emulation of status inspection of a full TCP/IP protocol stack.
- With UDP connections: Simulation of virtual connections.
- Generation and deletion of dynamic filter rules.

3.2 Data encryption via VPN

Description

A VPN (virtual private network) refers to a private network that uses a public network (e.g. the internet) as a transit network to transmit private data to a private destination network. The networks do not need to be compatible with one another for this.

While VPNs use the addressing mechanisms of the transit network to work, they use their own network packets to separate the transport of private data packets from the others. This fact allows the private networks to appear as a contiguous logical (virtual) network.

IPSec

An important aspect of data communication across network boundaries is IPSec (IP security). It is a standardized protocol suite that allows for vendor-agnostic, secure and protected data exchange over IP networks. The essential aim of IPSec is to secure and safeguard data during transmission into an unsecure network. All known vulnerabilities, such as eavesdropping and modification of data packets, can be prevented using this security standard. This is made possible through encrypted data packets and authentication of participants.

3.3 NAT/NAPT (address translation)

Description

Network Address Translation (NAT) and Network Address Port Translation (NAPT) are protocols for translating private IP addresses into public IP addresses.

Address translation with NAT

NAT is a protocol for translating between two address spaces. Its primary function is to translate public addresses, that is, IP addresses used and routed in the public internet, into private IP addresses and vice versa.

This technique allows for addresses in the internal network to be hidden from the outside in the external network. The internal nodes are only visible in the external network via the external IP addresses defined in the address translation list (NAT table).

Traditional NAT is a 1:1 translation, i.e. one private IP address is translated to one public one.

The address by which an internal node is reached is thus an external IP address.

The NAT table contains a mapping between private and public IP addresses, and is configured and managed in a gateway or router.

Address translation with NAPT

NAPT is a variant of NAT and the two are often equated with one another. The difference to NAT is that with this protocol, ports can also be translated.

There is no longer a 1:1 translation of IP addresses. Rather, there is only one public IP address which is translated into a series of private IP addresses through the addition of port numbers.

The address by which an internal node is reached is an external IP address with a port number.

The NAPT table contains a mapping from external ports to the private IP addresses, including port number; it is configured and managed in a gateway or router.

3.4 Secure IT functions

3.4.1 File Transfer Protocol (FTP)

Description

The File Transfer Protocol is a specific network protocol used for data transmission between an FTP server and FTP client or, when client-driven, between two FTP servers.

FTP allows data to be exchanged and folders created, renamed or deleted. Communication between an FTP client and FTP server takes place in the form of an exchange of text-based commands. Each command sent by the FTP client induces a response from the FTP server in the form of a status code and a message in cleartext.

FTP creates two logical connections for this purpose: one control channel via port 21 for transmitting FTP commands (and the responses thereto), and one data channel via port 20 for transmitting data.

With passive FTP, both channels are initiated by the FTP client, while with active FTP one of the channels is initiated by the FTP server.

Solution for secure FTP

To protect data during transmission, FTP also has the capability of data encryption and authentication.

The simplest method of implementing a secure FTP connection is Transport Layer Security, or TLS (formerly Secure Sockets Layer, or SSL). TLS is located on the Presentation Layer of the OSI layer model. Here, the data stream is encrypted with a key at the lowest bit level at the start of a connection.

The TLS handshake protocol is used for identification and authentication of the participants. Negotiation of an encryption key takes place through the public key method. To this end, the FTP server sends the FTP client a certificate with its public key. The public key to the certificate must be certified before the fact by a certificate authority and provided with a digital signature.

FTPS

The explicit FTP for secure data transmission is a combination of FTP and the TLS protocols. It uses the same ports as in normal FTP mode (port 20/21).

The key for TLS is a certificate that is generated and shipped with the configuration of the security CPs.

Secure FTP data transfer with the CP x43-1 Advanced V3 and CP 1x43-1 is only possible with security function enabled, and is explicitly required in the CP configuration.

3.4.2 Network Time Protocol (NTP)

Description

The Network Time Protocol (NTP) is a standardized protocol for time synchronization on multiple computers/modules via the network. Its accuracy is in the millisecond range.

The clock time is provided to NTP clients by an NTP server.

NTP (secure)

Secure NTP allows for secure and authenticated time synchronization utilizing authentication methods and a shared encryption code. The NTP server and the NTP clients must support this function.

Secure time synchronization is supported by the CP x43-1 Advanced V3 and CP 1x43-1 as long as the security function and the advanced NTP configuration are explicitly enabled in the CP's configuration in STEP 7.

3.4.3 Hypertext Transfer Protocol (HTTP)

Description

The Hypertext Transfer Protocol (HTTP) belongs to the family of internet protocols and is a standardized method of transmitting data on a network. HTTP is preferred for loading web pages from a web server on a web browser.

HTTPS

Data transmitted over HTTP are readable as cleartext and can be eavesdropped by third parties.

Today more than ever – in the age of online banking, online shopping and social networks – it is important that confidential and private data be transmitted safely and away from the eyes of unauthorized parties.

The easiest method of tap-proof transmission is Hypertext Transfer Protocol Secure (HTTPS). HTTPS is structured like HTTP, but it always uses the TLS protocol for encryption.

3.4.4 Simple Network Management Protocol (SNMP)

Description

SNMP (Simple Network Management Protocol) is a UDP-based protocol that was defined specifically for the administration of data network. It has become established as the de facto standard in TCP/IP devices. The individual nodes in the network (network components or end devices) are equipped with a so-called SNMP agent that provides information in structured form. This structure is called MIB, or Management Information Base. The agent in the network node is typically implemented as a firmware functionality.

Management Information Base – MIB

An MIB (Management Information Base) is a standardized data structure made up of different SNMP variables and written in a language that is independent of the target system. Thanks to the cross-vendor standardization of MIBs and the access mechanisms, even a heterogeneous network with components from different manufacturers can be monitored and controlled. If component-specific data and non-standardized data are needed for the network monitoring, these can be described by manufacturers in so-called "Private MIBs".

Secure SNMP (SNMPv3)

SNMP is available in different versions: SNMPv1, SNMPv2 and SNMPv3. SNMPv1 are SNMPv2 still in use to some extent. However, SNMPv1 and SNMPv2 should not be used because these versions implement limited or no security mechanisms unless other security mechanisms have been implemented (e.g. the cell security concept). From version 3 onward, SNMP additionally offers user management with authentication as well as optional encryption of data packets. This aspect greatly increased the security of SNMP. Secure SNMP is supported by the CP x43-1 Advanced V3 and CP 1x43-1 if the security function and SNMPv3 have been explicitly enabled in the configuration of the CP in STEP 7.

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers
– ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:

siemens.com/SupportRequest

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

4.3 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the manual https://support.industry.siemens.com/cs/de/en/view/90885010
\3\	Using Certificates with TIA Portal https://support.industry.siemens.com/cs/ww/en/view/109769068
\4\	Secure OUC between two S7-1500 CPUs https://support.industry.siemens.com/cs/de/en/view/109798671/143787499659
\5\	Secure transfer of messages (OPC UA) https://support.industry.siemens.com/cs/de/en/view/109798671/143868596107
\6\	Automated certificate management with GDS https://support.industry.siemens.com/cs/de/en/view/109798671/143868648715
\7\	Protecting user-defined functions https://support.industry.siemens.com/cs/de/en/view/109798671/94283635595
\8\	Questions and answers about the new security features in TIA Portal V17 https://support.industry.siemens.com/cs/ww/en/view/109799540
\9\	Central User Management with "User Management Component (UMC)" https://support.industry.siemens.com/cs/at/en/view/109780337
\10\	SIMATIC S7-1500, ET 200MP Automation system https://support.industry.siemens.com/cs/ww/en/view/59191792
\11\	SIMATIC S7 S7-1200 Programmable controller https://support.industry.siemens.com/cs/ww/en/view/109759862
\12\	SIMATIC S7-1200 Update to the S7-1200 System Manual, edition 11/2019 https://support.industry.siemens.com/cs/ww/en/view/109780810
\13\	Device manual for CP 343-1 Advanced - Part B http://support.automation.siemens.com/WW/view/en/62046619
\14\	Device manual for Industrial Ethernet CP 443-1 Advanced http://support.automation.siemens.com/WW/view/en/59187252
\15\	SIMATIC NET: S7-1500 - Industrial Ethernet CP 1543-1 https://support.industry.siemens.com/cs/ww/en/view/67700710

\16\	All-round protection with Industrial Security – Plant Security https://support.industry.siemens.com/cs/ww/en/view/50203404
\17\	All-round protection with Industrial Security – Network Security https://support.industry.siemens.com/cs/ww/en/view/92651441
\18\	All-round protection with Industrial Security – System Integrity https://support.industry.siemens.com/cs/ww/en/view/92605897
\19\	Overview document: Secure remote access with VPN https://support.industry.siemens.com/cs/de/en/view/26662448
\20\	Getting Started with Industrial Remote Communication https://support.industry.siemens.com/cs/de/en/view/64721753

4.4 Change documentation

Table 4-2

Version	Date	Change
V1.0	09/2013	First version
V2.0	03/2016	Added CP 1243-1, inserted additional links
V3.0	11/2022	Added new security functions from TIA V17