SIEMENS

SIMATIC

IEC 62443-4-2 Conformity document for S7-1500 CPUs

Product Information

05/2025
A5E54384186-AA

Legal information

Warning notice system

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

⚠ DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E54384186-AA
Ⓟ 05/2025 Subject to change

Table of contents

Introduction 1

Content of this documentation

This product information describes conformity of the SIMATIC S7-1500 CPUs with the following standard:

- International standard IEC 62443 "Security for industrial automation and control systems", Part 4-2: "Technical security requirements for IACS components" (IEC 62443-4-2 | Version 1.0 | February 2019).

This document explains the result of certification. You will obtain additional information:

- The configurations necessary to meet the requirements of the standard.
- The special points considered during certification that can be included in a risk assessment.

Scope

This document is valid for the CPUs of the SIMATIC S7-1500, ET 200SP and ET 200pro product families in firmware version V3.1 or newer.

Table 1-1 List of CPUs as of firmware version V3.1

SIMATIC S7-1500 CPU	Article number
CPU 1510SP F-1 PN	6ES7510-1SK03-0AB0*
CPU 1510SP-1 PN	6ES7510-1DK03-0AB0*
CPU 1511-1 PN	6ES7511-1AL03-0AB0*
CPU 1511F-1 PN	6ES7511-1FL03-0AB0*
CPU 1511T-1 PN	6ES7511-1TL03-0AB0*
CPU 1511TF-1 PN	6ES7511-1UL03-0AB0*
CPU 1512SP F-1 PN	6ES7512-1SM03-0AB0*
CPU 1512SP-1 PN	6ES7512-1DM03-0AB0*
CPU 1513-1 PN	6ES7513-1AM03-0AB0*
CPU 1513F-1 PN	6ES7513-1FM03-0AB0*
CPU 1513pro F-2 PN	6ES7513-2GM03-0AB0*
CPU 1513pro-2 PN	6ES7513-2PM03-0AB0*
CPU 1513R-1 PN	6ES7513-1RM03-0AB0*
CPU 1514SP F-2 PN	6ES7514-2SN03-0AB0*
CPU 1514SP-2 PN	6ES7514-2DN03-0AB0*
CPU 1514SP T-2 PN	6ES7514-2VN03-0AB0*

* The CPUs as of this article number support "Secure Boot" and "Central user management" (for more information, see section "Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500").

SIMATIC S7-1500 CPU	Article number
CPU 1514SP TF-2 PN	6ES7514-2WN03-0AB0*
CPU 1515-2 PN	6ES7515-2AN03-0AB0*
CPU 1515F-2 PN	6ES7515-2FN03-0AB0*
CPU 1515R-2 PN	6ES7515-2RN03-0AB0*
CPU 1515T-2 PN	6ES7515-2TN03-0AB0*
CPU 1515TF-2 PN	6ES7515-2UN03-0AB0*
CPU 1516-3 PN/DP	6ES7516-3AP03-0AB0*
CPU 1516F-3 PN/DP	6ES7516-3FP03-0AB0*
CPU 1516pro F-2 PN	6ES7516-2GP03-0AB0*
CPU 1516pro-2 PN	6ES7516-2PP03-0AB0*
CPU 1516T-3 PN/DP	6ES7516-3TN00-0AB0
CPU 1516T-3 PN	6ES7516-3TP10-0AB0*
CPU 1516TF-3 PN/DP	6ES7516-3UN00-0AB0
CPU 1516TF-3 PN	6ES7516-3UP10-0AB0*
CPU 1517-3 PN/DP	6ES7517-3AP00-0AB0
CPU 1517-3 PN	6ES7517-3AQ10-0AB0*
CPU 1517F-3 PN/DP	6ES7517-3FP00-0AB0
CPU 1517F-3 PN	6ES7517-3FQ10-0AB0*
CPU 1517H-3 PN	6ES7517-3HP00-0AB0
CPU 1517H-4 PN	6ES7517-4HQ10-0AB0*
CPU 1517T-3 PN/DP	6ES7517-3TP00-0AB0
CPU 1517TF-3 PN/DP	6ES7517-3UP00-0AB0
CPU 1517T-3 PN	6ES7517-3TQ10-0AB0*
CPU 1517TF-3 PN	6ES7517-3UQ10-0AB0*
CPU 1518-3 PN	6ES7518-3AT10-0AB0*
CPU 1518F-3 PN	6ES7518-3FT10-0AB0*
CPU 1518T-3 PN	6ES7518-3TT10-0AB0*
CPU 1518TF-3 PN	6ES7518-3UT10-0AB0*
CPU 1518-4 PN/DP	6ES7518-4AP00-0AB0
CPU 1518-4 PN/DP MFP	6ES7518-4AX00-1AB0
CPU 1518-4 PN/DP MFP (incl. OPC UA RT license)	6ES7518-4AX00-1AC0
CPU 1518-4F PN/DP	6ES7518-4FP00-0AB0
CPU 1518F-4 PN/DP MFP	6ES7518-4FX00-1AB0
CPU 1518F-4 PN/DP MFP (incl. OPC UA RT license)	6ES7518-4FX00-1AC0
CPU 1518HF-4 PN	6ES7518-4JP00-0AB0

* The CPUs as of this article number support "Secure Boot" and "Central user management" (for more information, see section "Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500").

SIMATIC S7-1500 CPU	Article number
CPU 1518HF-4 PN	6ES7518-4JT10-0AB0*
CPU 1518T-4 PN/DP	6ES7518-4TP00-0AB0
CPU 1518TF-4 PN/DP	6ES7518-4UP00-0AB0

* The CPUs as of this article number support "Secure Boot" and "Central user management" (for more information, see section "Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500").

Table 1-2 List of SIPLUS CPUs as of firmware version V3.1

SIPLUS CPU	Article number
SIPLUS ET 200SP CPU 1510SPF-1PN	6AG1510-1SK03-2AB0*
SIPLUS ET 200SP CPU 1510SP-1PN	6AG1510-1DK03-2AB0*
SIPLUS ET 200SP CPU 1510SP-1PN	6AG1510-1DK03-7AB0*
SIPLUS ET 200SP CPU 1510SP-1PN RAIL	6AG2510-1DK03-1AB0*
SIPLUS ET 200SP CPU 1512SPF-1PN	6AG1512-1SM03-2AB0*
SIPLUS ET 200SP CPU 1512SPF-1PN	6AG1512-1SM03-7AB0*
SIPLUS ET 200SP CPU 1512SPF-1PN RAIL	6AG2512-1SM03-1AB0*
SIPLUS ET 200SP CPU 1512SPF-1PN RAIL	6AG2512-1SM03-4AB0*
SIPLUS ET 200SP CPU 1512SP-1 PN	6AG1512-1DM03-2AB0*
SIPLUS ET 200SP CPU 1512SP-1 PN	6AG1512-1DM03-7AB0*
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL	6AG2512-1DM03-1AB0*
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL	6AG2512-1DM03-4AB0*
SIPLUS ET 200SP CPU 1515SP PC2	6AG1677-2DB40-2AA0
SIPLUS ET 200SP CPU 1515SP PC2 FL RAIL	6AG2677-2SB43-2GB1*
SIPLUS ET 200SP CPU 1515SP PC2 RAIL	6AG2677-2DB40-2AA0
SIPLUS S7-1500 CPU 1511-1 PN	6AG1511-1AL03-2AB0*
SIPLUS S7-1500 CPU 1511-1 PN	6AG1511-1AL03-7AB0*
SIPLUS S7-1500 CPU 1511-1 PN RAIL	6AG2511-1AL03-1AB0*
SIPLUS S7-1500 CPU 1511F-1 PN	6AG1511-1FL03-2AB0*
SIPLUS S7-1500 CPU 1513-1 PN	6AG1513-1AM03-2AB0*
SIPLUS S7-1500 CPU 1513-1 PN	6AG1513-1AM03-7AB0*
SIPLUS S7-1500 CPU 1513F-1 PN	6AG1513-1FM03-2AB0*
SIPLUS S7-1500 CPU 1515F-2 PN	6AG1515-2FN03-2AB0*
SIPLUS S7-1500 CPU 1515F-2 PN RAIL	6AG2515-2FN03-4AB0*
SIPLUS S7-1500 CPU 1515R-2 PN RAIL	6AG2515-2RN03-4AB0*
SIPLUS S7-1500 CPU 1516-3 PN	6AG1516-3AP03-2AB0*
SIPLUS S7-1500 CPU 1516-3 PN	6AG1516-3AP03-7AB0*
SIPLUS S7-1500 CPU 1516-3 PN RAIL	6AG2516-3AP03-4AB0*
SIPLUS S7-1500 CPU 1516F-3 PN	6AG1516-3FP03-2AB0*
SIPLUS S7-1500 CPU 1516F-3 PN RAIL	6AG2516-3FP03-2AB0*

* The CPUs as of this article number support "Secure Boot" and "Central user management" (for more information, see section "Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500").

SIPLUS CPU	Article number
SIPLUS S7-1500 CPU 1516F-3 PN RAIL	6AG2516-3FP03-4AB0*
SIPLUS S7-1500 CPU 1517H-3 PN	6AG1517-3HP00-4AB0
SIPLUS S7-1500 CPU 1518-4 PN/DP	6AG1518-4AP00-4AB0
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	6AG1518-4AX00-4AB0
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	6AG1518-4AX00-4AC0
SIPLUS S7-1500 CPU 1518F-4 PN/DP	6AG1518-4FP00-4AB0
SIPLUS S7-1500 CPU 1518HF-4 PN	6AG1518-4JP00-4AB0

* The CPUs as of this article number support "Secure Boot" and "Central user management" (for more information, see section "Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500").

The document considers product characteristics and interfaces of the above-listed CPUs which contribute to compliance with the requirements of IEC 62443-4-2.

System properties that result in an overall protection concept through targeted networking and individual parameter assignment of the products do not fall within the scope of application. For the Declaration of Conformity of an entire industrial automation system according to Part 3-3 "System security requirements and security levels" of IEC 62443, all system-specific conditions and circumstances need to be taken into consideration.

Target group

This document is aimed primarily at individuals in the fields:

- System and device purchasing
- Project planning and implementation
- System integrators
- Network integrators

Objective

- The document acts as an orientation guide and supplements the product documentation.

- The document creates transparency with respect to product security functions to protect industrial automation systems in day-to-day operation from cyber threats in line with the requirements of IEC 62443. This includes an overview of the product features and interfaces that help to reduce threats to operation and thus support productivity and availability, even during security incidents.
- The transparency outlined above contributes to IEC 62443-compliant integration of products in an overall security concept with consideration of system-specific conditions.
- The transparency outlined above provides support with tenders or system designs with respect to compliance with IEC 62443 Part 4-2.

Notes on using the document

Following a risk-based approach, the IEC 62443 in multiple parts describes both a concept and technical requirements with which industrial automation systems can be protected from security threats. In addition to plant operators, service providers and system integrators, the standard is also aimed at product suppliers.

To enable service providers, operators and integrators to set up a secure automation system complying with Part 3-3, Part 4-2 is aimed at product manufacturers and describes the product characteristics of a component necessary for this purpose.

Because it is not necessary to meet all product safety requirements in order to achieve an IEC 62443-3-3-compliant system, it is particularly important to consider the intended use of the product and the corresponding usage environment. These definitions form the basis for further interpretation of which requirements a product needs to meet and how a product can be securely integrated in an overall system. These aspects are explained in general terms in the section Operational application environment and security assumptions (Page 14).

In addition to the technical product features, it is also essential that the development process defined according to IEC 62443-4-1 has been applied. You can find information on the requirements in the section IEC 62443-4-1 (Page 11).

Meeting of the product requirements from IEC 62443-4-2 is outlined in the section Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500 CPUs (Page 18). To simplify use of the information, the same structure and requirement IDs as in IEC 62443 are used.

Certification according to IEC 62443-4-1 and IEC 62443-4-2

The products of the SIMATIC S7-1500 CPU series (applies to firmware version V3.1 and later) are certified by:

- TÜV Süd

The certification process confirmed Maturity level 3 of the secure product development process.

The certificates can be downloaded:

- Certificate IEC 62443-4-1: (https://www.siemens.com/globalhttps://www.siemens.com/global/en/general/system-certificates/di-fa.html/en/general/system-certificates/di-pa.html)
- Certificate IEC 62443-4-2: (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity/certification-standards.html)

1.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry (https://www.siemens.com/cybersecurity-industry).

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 Cybersecurity RSS Feed under
https://new.siemens.com/cert (https://www.siemens.com/cert).

IEC 62443 standard 2

2.1 IEC 62443 for product manufacturer

2.1.1 IEC 62443-4-1

This part of the standard contains security-relevant requirements relating to the product development process. It covers requirements on topics including skills and knowledge, security of third-party components, process and quality assurance, secure architecture and secure design, troubleshooting and security updates, patches and change management. Secure implementation of the technical product capabilities is only possible when these requirements are met.

IEC 62443-4-1 describes the requirements on the manufacturer's development process, which are divided into eight so-called practices:

- Security management
- Specification of security requirements
- Secure by design
- Secure implementation
- Security verification and validation testing
- Management of security-related issues
- Security update management
- Security guidelines

In addition to these requirements, the standard defines four so-called "Maturity levels" which describe how strictly the requirements need to be observed during product development:

- Maturity level 1: Initial - Processes are unpredictable, poorly controlled and reactive
- Maturity level 2: Managed - Processes are characterized but reactively used
- Maturity level 3: Defined - Processes are characterized and proactively deployed
- Maturity level 4: Improved - Processes are measured, controlled and continuously improved

In the scope of certification according to IEC 62443-4-1, these maturity levels are checked and noted on the certificates.

2.1.2 IEC 62443-4-2

IEC 62443-4-2 defines security requirements for components used in Industrial Automation and Control Systems, IACS. These requirements are designated as Component Requirements, CR that are closely related to the System Requirements, SR defined in IEC 62443-3-3. Both CR and SR are technical requirements combined into seven Foundational Requirements, FR:

- Identification and authentication control (IAC): Identification and authentication of users and devices
- Use control (UC): Control of the usage of system resources
- System integrity (SI): Ensuring the integrity of the system
- Data confidentiality (DC): Protection of the confidentiality of data
- Restricted data flow (RDF): Limiting of the data flow within the system
- Timely response to events (TRE): Prompt response to security-relevant events
- Resource availability (RA): Ensuring the availability of system resources

Component Requirements (CR) can be supplemented by one or more Requirement Enhancements (RE) which demand further and stricter functions of a specific requirement.

Component Requirements (CR) and the associated Requirement Enhancements (RE) are each assigned to one of the four risk-based Security Levels (SL1 to SL4). The ability of a component to reach a specific Security Level is classified with this assignment.

To reach a specific Security Level for an entire IACS according to IEC 62443-3-3, it is possible to combine different components. The overall system thus reaches the desired Security Level, even if an individual component does not meet all Components Requirements (CR) and Requirement Enhancements (RE). To ensure that the required security functionality is present, the intended usage and the operational usage environment of the components must be checked.

2.1.3 What is a Security Level?

While IEC 62443 follows a risk-based approach, the defined Security Levels should provide an indication of the protection to be achieved. The standard defines four tiered Security Levels intended to offer protection again different capabilities, resources and efforts.

The Security Levels are defined in IEC 62443-3-3, Appendix A.3.2:

- Security Level 1: Protection against casual or coincidental violation
- Security Level 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation
- Security Level 3: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
- Security Level 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Security Level 0 is implicitly defined when there are no protection and security requirements.

Security Level 2 is the lowest level that offers protection from intentional misuse and is therefore considered the minimum requirement on a system.

For reasons of transparency and simplicity, no distinction is made in this document between the different types of Security Levels, nor is the fulfillment of the requirements combined into a general Security Level. Instead, the document provides information on the fulfillment of the individual requirement and its proper configuration.

Operational application environment and security assumptions 3

3.1 Application area

The SIMATIC S7-1500 automation system offers the required flexibility and performance for a wide range of controller applications in machine and plant engineering. The scalable configuration makes it possible to adapt the controller to the local conditions.

The CPUs are the heart of the automation system. You run the user program and network the SIMATIC S7-1500 with other automation components. The hardware is extremely compact and IP20- or IP65/67-certified.

The SIMATIC S7-1500 controller family consists of different variants that are all based on the same firmware:

- With respect to the functionality, **SIPLUS variants** are identical to the respective SIMATIC hardware variants and have robust designs to withstand harsher operating conditions.
- **ET 200SP and ET 200pro variants** allows intelligent preprocessing to relieve the higher-level controller in IP20 or IP65/67 environment.
- **Technology CPUs** offer more advanced Motion Control and technology functions and are used in particular for drive control.
- **Redundant and high availability CPUs** reduce the probability of production downtime by operating two systems in parallel.
- **Fail-safe CPUs** realize applications for safety engineering with the aim of protecting life and environment through safe shutdown.

Security of all CPU variants according to IEC 62443:

The CPUs contain preconfigured mechanisms for the protection of plants, networks and systems from unauthorized access. According to IEC 62443, the security mechanisms in the SIMATIC S7-1500 CPUs are continuously updated and improved.

Default security presettings according to the Security by Default concept for communication and user management increase network security.

The typical application area described serves merely as a guide to interpreting conformity with IEC 62443-4-2. The relevant product characteristics are described in the section Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500 CPUs (Page 18).

NOTE

You can find more detailed information on the product properties and possible uses of the SIMATIC S7-1500 automation system on the Internet (https://www.siemens.com/global/en/products/automation/systems/industrial/plc/simatic-s7-1500.html).

3.2 Comprehensive "defense in depth" security concept

The intended usage environment has a significant influence on the product features required by IEC 62443-4-2 and is essential for assessing conformity.
Generally, the SIMATIC S7-1500 should be operated in the context of a defense in depth security concept.

With defense in depth, Siemens provides a multi-layer security concept that offers industrial plants comprehensive and far-reaching protection in accordance with the recommendations of the IEC 62443 international standard.

Productivity and know-how are protected on 3 levels:

Plant security

Plant security uses various methods to safeguard critical components from physical access by people. This starts with classic building access and extends to securing sensitive areas using access control (for example, code card, iris scan, fingerprint or access code).

Network security

Automation networks must be protected against unauthorized access. This is achieved through security measures on the product, but also those in the product-related environment.

System integrity

Targeted measures must be taken to protect existing know-how or to prevent unauthorized access to automation processes. The measures protect against unauthorized configuration changes and highlight attempts at manipulation.

NOTE

You can find more information on the topics of defense in depth, plant security, network security, and system integrity on the SIEMENS Industrial cybersecurity (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html) Web page.

Also make use of the Download Center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) to obtain more information on industrial cybersecurity. The "Operational Guidelines (https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf)", for example, provide recommendations on basic security measures for secure machine and plant operation in an industrial environment.

3.3 Requirements for the operational application environment and security assumptions

Siemens recommends the following security measures:

- Threat and Risk Assessments (as part of security management)
- Network security concepts
  - Network segmentation
  - Asset and network management
  - Network protection
  - Remote access
- Plant security concepts
  - Physical protection
  - Physical corporate security
  - Physical production security

Threat and Risk Assessment

Risks are identified and evaluated by a combination of vulnarabilities, threats and impacts. On this basis, countermeasures are proposed to ensure the security of the system, networks, and data.

Network security concepts

You can find information on network security in the whitepaper "Industrial Network Security Architecture", available at the Download Center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) on the Industrial Cybersecurity (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html) website.

Plant security concepts

Physical protection

In addition to closing off and/or monitoring entire production facilities, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security

Physical corporate security can be ensured by the following measures:

- Closed off and monitored company premises
- Access control, locks/card readers, and/or security personnel
- Accompaniment of non-employees by company personnel
- Employees are trained on and embrace security processes within the company

Physical production security

Physical production security can be ensured by the following measures, among others:

- Separate access control for critical areas, such as production zones.
- Installation of critical components in lockable cabinets/control rooms with monitoring and alarm capabilities. The cabinets/control rooms must be secured with a cylinder lock. Do not use simple locks, such as universal, triangular/square, or double-bit locks.
- Radio field planning to limit WLAN coverage areas, preventing them from extending beyond defined zones (e.g. factory floor).
- Guidelines that prohibit the use of external data storage media (such as USB flash drives) and IT devices (such as laptops) classified as unsafe on systems.

Usage conditions of the CPUs in the context of IEC62443-4-2 certification

The following conditions of use are assumed for the assessment of conformity outlined in the section Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500 CPUs (Page 18):

Physical protection of the component in the usage environment

- Operation of the component in a controlled, monitored environment or in a closed area such as a control cabinet.
- Protection against unauthorized access by locking the front flap of the CPU with a seal or a lock.

Integrity protection

- The CPUs come with integrity protection functions as standard. These contribute to detecting manipulation of engineering data and encrypted firmware.

Network zones and interfaces

- Non-secure protocols are deactivated in the device configuration. Device access via secure protocol variants such as HTTPS.

Network infrastructure

- User authentication via local or central user management via a central server (UMC server).
- Password management and application of password policies is performed via central or local user management.
- Predefined events in a network device are collected as security events in the CPU (syslog client) and sent to a syslog server in the network for further processing.

Fulfillment of the functional scope of IEC 62443-4-2 by SIMATIC S7-1500 CPUs

4

4.1 Security Level (SL) according to IEC 62443-4-2 which can be achieved by SIMATIC S7-1500 CPUs - Overview

Achieved Security Level: Abbreviations

Table 4-1 Legend of labels in the following table

Number column	Meaning
CR	Component Requirement
EDR	Embedded Device Requirement
FR	Foundational Requirement
HDR	Host Device Requirement
NDR	Network Device Requirement
RE	Requirement Enhancement
SAR	Software Application Requirement
Integration column	
C	The requirement is met by the component itself.
S	The requirement can be met by integration in a system. A component can provide a technical feature or an interface for this purpose. Integration is described in the component's security guideline.
N	The requirement is not met.
N/A	The requirement does not apply to this component.
Security Level column	
✓	The requirement must be met for this Security Level.

HDR, NDR and SAR requirements

The HDR, NDR and SAR requirements are not explained further in the following sections because they are not relevant for the CPUs:

- Host Device Requirement (HDR) only applies to host systems (PCs)
- Network Device Requirement (NDR) only applies to network components
- Software Application Requirement (SAR) only applies to software applications

Achieved Security Level

Table 4-2 Overview: Achieved Security Level

Number	Description	Integration	Security Level			
			1	2	3	4
Identification and authentication control (IAC)						
CR 1.1 (Page 23)	Human user identification and authentication	C	✓	✓	✓	✓
CR 1.1 RE1 (Page 23)	Unique Identification and Authentication	N		✓	✓	✓
CR 1.1 RE2 (Page 23)	Multifactor Authentication for All Interfaces	N			✓	✓
CR 1.2 (Page 23)	Software process and device identification and authentication	C		✓	✓	✓
CR 1.2 RE1 (Page 23)	Unique Identification and Authentication	C			✓	✓
CR 1.3 (Page 24)	Account management	C	✓	✓	✓	✓
CR 1.4 (Page 25)	Identifier management	C	✓	✓	✓	✓
CR 1.5 (Page 25)	Authenticator management	C	✓	✓	✓	✓
CR 1.5 RE1 (Page 25)	Hardware Security for Authenticators	C			✓	✓
NDR 1.6	Wireless access management	N/A	✓	✓	✓	✓
NDR 1.6 RE1	Unique Identification and Authentication	N/A		✓	✓	✓
CR 1.7 (Page 25)	Strength of password-based authentication	C	✓	✓	✓	✓
CR 1.7 RE1 (Page 25)	Password Generation and Lifetime Restrictions for Human Users	N*			✓	✓
CR 1.7 RE2 (Page 25)	Password Lifetime Restrictions for All Users (Human, Software Process or Device)	C				✓
CR 1.8 (Page 26)	Public key infrastructure (PKI) certificates	C		✓	✓	✓
CR 1.9 (Page 26)	Strength of public key authentication	C		✓	✓	✓
CR 1.9 RE1 (Page 26)	Hardware Security for Public Key-Based Authentication	C			✓	✓
CR1.10 (Page 27)	Authenticator feedback	C	✓	✓	✓	✓
CR 1.11 (Page 27)	Unsuccessful login attempts	C	✓	✓	✓	✓
CR 1.12 (Page 27)	System use notification	C	✓	✓	✓	✓
NDR 1.13	Access via untrusted networks	N/A	✓	✓	✓	✓
NDR 1.13 RE1	Explicit Access Request Approval	N/A			✓	✓
CR 1.14 (Page 28)	Strength of Symmetric Key-Based Authentication	N/A		✓	✓	✓
CR 1.14 RE1 (Page 28)	Hardware Security for Symmetric Key-Based Authentication	N/A			✓	✓
Use Control (UC)						
CR 2.1 (Page 28)	Authorization Enforcement	C	✓	✓	✓	✓
CR 2.1 RE1 (Page 28)	Authorization Enforcement for All Users (Humans, Software Processes and Devices)	C		✓	✓	✓
CR 2.1RE2 (Page 28)	Permission Mapping to Roles	C		✓	✓	✓
CR 2.1 RE3 (Page 28)	Supervisor Override	N/A			✓	✓
CR 2.1 RE4 (Page 28)	Dual Approval	N/A				✓

* As of firmware version V4.0, met by CPU or integration

Number	Description	Integration	Security Level			
			1	2	3	4
CR 2.2 (Page 29)	Wireless Use Control	N/A	✓	✓	✓	✓
SAR 2.4	Mobile code	N/A	✓	✓	✓	✓
SAR 2.4 RE1	Mobile Code Authenticity Check	N/A		✓	✓	✓
EDR 2.4 (Page 29)	Mobile Code	C	✓	✓	✓	✓
EDR 2.4 RE1 (Page 29)	Mobile Code Authenticity Check	C		✓	✓	✓
HDR2.4	Mobile Code	N/A	✓	✓	✓	✓
HDR 2.4 RE1	Mobile Code Authenticity Check	N/A		✓	✓	✓
NDR 2.4	Mobile Code	N/A	✓	✓	✓	✓
NDR 2.4 RE1	Mobile Code Authenticity Check	N/A		✓	✓	✓
CR 2.5 (Page 30)	Session Lock	C	✓	✓	✓	✓
CR 2.6 (Page 30)	Remote Session Termination	C		✓	✓	✓
CR 2.7 (Page 31)	Concurrent Session Control	C			✓	✓
CR 2.8 (Page 31)	Auditable Events	C	✓	✓	✓	✓
CR 2.9 (Page 32)	Audit Storage Capacity	S	✓	✓	✓	✓
CR 2.9 RE1 (Page 32)	Warn when Audit Record Storage Capacity Threshold Reached	N/A			✓	✓
CR 2.10 (Page 32)	Response to Audit Processing Failures	C	✓	✓	✓	✓
CR 2.11 (Page 33)	Time stamps	C	✓	✓	✓	✓
CR 2.11 RE1 (Page 33)	Time Synchronization	C		✓	✓	✓
CR 2.11 RE2 (Page 33)	Protection of Time Source Integrity	C				✓
CR 2.12 (Page 34)	Non-Repudiation	C	✓	✓	✓	✓
CR 2.12 RE1 (Page 34)	Non-Repudiation for All Users	C				✓
EDR 2.13 (Page 34)	Use of Physical Diagnostic and Test Interfaces	C		✓	✓	✓
EDR 2.13 RE1 (Page 34)	Active Monitoring	N/A			✓	✓
HDR 2.13	Use of Physical Diagnostic and Test Interfaces	N/A		✓	✓	✓
HDR 2.13 RE1	Active Monitoring	N/A			✓	✓
NDR 2.13	Use of Physical Diagnostic and Test Interfaces	N/A		✓	✓	✓
NDR 2.13 RE1	Active Monitoring	N/A			✓	✓
System Integrity (SI)						
CR 3.1 (Page 35)	Communication Integrity	C	✓	✓	✓	✓
CR 3.1 RE1 (Page 35)	Communication Authentication	C		✓	✓	✓
SAR 3.2	Protection from Malicious Code	N/A	✓	✓	✓	✓
EDR 3.2 (Page 36)	Protection from Malicious Code	C	✓	✓	✓	✓
HDR 3.2	Protection from Malicious Code	N/A	✓	✓	✓	✓
HDR 3.2 RE1	Protection from Malicious Code	N/A		✓	✓	✓
NDR 3.2	Protection from Malicious Code	N/A	✓	✓	✓	✓
CR 3.3 (Page 37)	Security Functionality Verification	C	✓	✓	✓	✓

* As of firmware version V4.0, met by CPU or integration

Number	**Description**	**Integration**	**Security Level**			
			1	**2**	**3**	**4**
CR 3.3 RE1 (Page 37)	Security Functionality Verification During Normal Operation	C				✓
CR 3.4 (Page 37)	Software and Information Integrity	C	✓	✓	✓	✓
CR 3.4 RE1 (Page 37)	Authenticity of Software and Information	C		✓	✓	✓
CR 3.4 RE2 (Page 37)	Automated Notification of Integrity Violations	S			✓	✓
CR 3.5 (Page 38)	Input Validation	C	✓	✓	✓	✓
CR 3.6 (Page 38)	Deterministic Output	C	✓	✓	✓	✓
CR 3.7 (Page 38)	Error Handling	C	✓	✓	✓	✓
CR 3.8 (Page 39)	Session Integrity	C		✓	✓	✓
CR 3.9 (Page 40)	Protection of Audit Information	C		✓	✓	✓
CR 3.9 RE1 (Page 40)	Audit Records on Write-Once Media	N				-✓
EDR 3.10 (Page 41)	Support for Updates	C	✓	✓	✓	✓
EDR 3.10 RE1 (Page 41)	Update Authenticity and Integrity	C		✓	✓	✓
HDR 3.10	Support for Updates	N/A	✓	✓	✓	✓
HDR 3.10 RE1	Update Authenticity and Integrity	N/A		✓	✓	✓
NDR 3.10	Support for Updates	N/A	✓	✓	✓	✓
NDR 3.10 RE1	Update Authenticity and Integrity	N/A		✓	✓	✓
EDR 3.11 (Page 41)	Physical Temper Resistance and Detection	N		✓	✓	✓
EDR 3.11 RE1 (Page 41)	Notification of a Tampering Attempt	N			✓	✓
HDR 3.11	Physical Temper Resistance and Detection	N/A		✓	✓	✓
HDR 3.11 RE1	Notification of a Tampering Attempt	N/A			✓	✓
NDR 3.11	Physical Temper Resistance and Detection	N/A		✓	✓	✓
NDR 3.11 RE1	Notification of a Tampering Attempt	N/A			✓	✓
EDR 3.12 (Page 41)	Provisioning Product Supplier Roots of Trust	C		✓	✓	✓
HDR 3.12	Provisioning Product Supplier Roots of Trust	N/A		✓	✓	✓
NDR 3.12	Provisioning Product Supplier Roots of Trust	N/A		✓	✓	✓
EDR 3.13 (Page 42)	Provisioning Asset Owner Roots of Trust	C		✓	✓	✓
HDR 3.13	Provisioning Asset Owner Roots of Trust	N/A		✓	✓	✓
NDR 3.13	Provisioning Asset Owner Roots of Trust	N/A		✓	✓	✓
EDR 3.14 (Page 42)	Integrity of the Boot Process	N*	✓	✓	✓	✓
EDR 3.14 RE1 (Page 42)	Authenticity of the Boot Process	N*		✓	✓	✓
HDR 3.14	Integrity of the Boot Process	N/A	✓	✓	✓	✓
HDR 3.14 RE1	Authenticity of the Boot Process	N/A		✓	✓	✓
NDR 3.14	Integrity of the Boot Process	N/A	✓	✓	✓	✓
NDR 3.14 RE1	Authenticity of the Boot Process	N/A		✓	✓	✓
Data Confidentiality (DC)						
CR 4.1 (Page 43)	Information Confidentiality	C	✓	✓	✓	✓

* As of firmware version V4.0, met by CPU or integration

Number	Description	Integration	Security Level			
			1	2	3	4
CR 4.2 (Page 43)	Information Persistence	C		✓	✓	✓
CR 4.2 RE1 (Page 43)	Erase of Shared Memory Resources	C			✓	✓
CR 4.2 RE2 (Page 43)	Erase Verification	C			✓	✓
CR 4.3 (Page 43)	Use of Cryptography	C	✓	✓	✓	✓
Restricted Data Flow (RDF)						
CR 5.1 (Page 44)	Network Segmentation	C	✓	✓	✓	✓
NDR 5.2	Zone Boundary Protection	N/A	✓	✓	✓	✓
NDR 5.2 RE1	Deny All, Permit by Exception	N/A		✓	✓	✓
NDR 5.2 RE2	Deny All, Permit by Exception	N/A			✓	✓
NDR 5.2 RE3	Fail Close	N/A			✓	✓
NDR 5.3	General Purpose Person-To-Person Communication Restrictions	N/A	✓	✓	✓	✓
Timely Response to Events (TRF)						
CR 6.1 (Page 44)	Audit Log Accessibility	C	✓	✓	✓	✓
CR 6.1 RE1 (Page 44)	Programmatic Access to Audit Logs	C			✓	✓
CR 6.2 (Page 45)	Continuous Monitoring	S		✓	✓	✓
Resource Availability (RA)						
CR 7.1 (Page 45)	Denial of Service Protection	C	✓	✓	✓	✓
CR 7.1 RE1 (Page 45)	Manage Communication Load from Component	C		✓	✓	✓
CR 7.2 (Page 46)	Resource Management	C	✓	✓	✓	✓
CR 7.3 (Page 46)	Control System Backup	C	✓	✓	✓	✓
CR 7.3 RE1 (Page 46)	Backup Integrity Verification			✓	✓	✓
CR 7.4 (Page 47)	Control System Recovery and Reconstitution	C	✓	✓	✓	✓
CR 7.6 (Page 47)	Network and Security Configuration Settings	C	✓	✓	✓	✓
CR 7.6 RE1 (Page 47)	Machine-Readable Reporting of Current Security Settings	C			✓	✓
CR 7.7 (Page 48)	Least Functionality	C	✓	✓	✓	✓
CR 7.8 (Page 48)	Control System Component Inventory	C		✓	✓	✓

* As of firmware version V4.0, met by CPU or integration

4.2 FR 1 – Identification and Authentication Control (IAC)

4.2.1 CR 1.1 – Human User Identification and Authentication

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.1	User identification and authentication takes place via UMAC, which contains local user management that is used by the various interfaces to the CPU (PG/HMI communication, web server, OPC UA) for all authentication and authorization purposes. All CPUs as of firmware version V4.0 support central user management via a remote UMC server.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management" and section "Central user management" List of CPUs with article numbers; see section "Introduction (Page 5)"
		Access to the CPU display can be protected with a password. The password is defined in the CPU properties in STEP 7.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "CPU display"
Achievement of SL 2 – 4	CR 1.1 RE1	The CPU display is an exception. Because the password for the display does not allow unique identification of the access, corresponding measures need to be taken to regulate physical access to the CPU, e.g. through installation in a lockable control cabinet.	See CR 1.1 S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Requirements for the operational application environment and security assumptions"
Achievement of SL 3 – 4	CR 1.1 RE2	No functions that contribute to achieving the defined Security Level are implemented in the product.	

4.2.2 CR 1.2 – Software Process and Devices Identification and Authentication

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 1.2	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 1.2	The CPU can be supplied with certificates using the certificate manager in the TIA Portal. Examples of CPU-unique certificates: • Device certificate of the manufacturer • Certificates imported by the user • PG/HMI communication via TLS certificate • Web server certificate • OPC UA certificate • Secure OUC certificate • Transfer the syslog messages to a syslog server (via TLS certificate)	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Managing certificates" Application example "Using Certificates with TIA Portal" (https://support.industry.siemens.com/cs/ww/de/view/109769068/en)

Achievement of SL 2 – 4	CR 1.2	Protocols and functions that support identification/authentication are: • PG/HMI communication • Web server • OPC UA • Secure Open User Communication (OUC) • Syslog messages	
		Note: Network authentication according to IEE 802.1X via EAP can be performed by using a CP 1543-1.	CP 1543-1 operating instructions (https://support.industry.siemens.com/cs/ww/en/view/109973328) Section "Network authentication"
Achievement of SL 3 – 4	CR 1.2 RE1	See CR1.2 Authentication of the CPU via certificates on other devices/systems (e.g. other CPUs) is possible: • For Secure OUC • For OPC UA • For syslog messages • Central user management (as of CPU FW 4.0)	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Secure OUC between two S7-1500 CPUs" Section "Security at OPC UA" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Transfer the syslog messages to a syslog server"

4.2.3 CR 1.3 – Account Management

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.3	User management is implemented locally on the CPU. The user configures the user accounts using the TIA Portal. The accounts are then synchronized with the local data memory of the CPU. All CPUs as of firmware version V4.0 support central user management via a remote UMC server.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management", section "Central user management" STEP 7 online help List of CPUs with article numbers; see section "Introduction (Page 5)"

4.2.4 CR 1.4 – Identifier Management

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.4	The user names from the user management are used for the CPUs for identification.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management", section "Central user management"

4.2.5 CR 1.5 – Authenticator Management

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.5	The user passwords are managed via the TIA Portal and synchronized with the component. a) The initial passwords are defined using the TIA Portal. b) There are no default user names and passwords c) Passwords and other authentication procedures can be changed at any time. d) Passwords are saved in encrypted form. Confidential configuration data in a TIA project can be protected against unauthorized access with a password.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Protection of confidential configuration data" Section "Local user management", section "Central user management" STEP 7 online help
Achievement of SL 3 – 4	CR 1.5 RE1	Through the protection of confidential PLC configuration data, sensitive data such as passwords and private keys can be encrypted using a password. The password for confidential configuration data is saved in a Secure Element on the CPU.	See CR 1.5

4.2.6 CR 1.7 – Strength of Password-Based-Authentication

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.7	The CPU offers the possibility to configure password policies relating to complexity and validity: • Minimum length • Minimum number of digits • Minimum number of special characters • Maximum validity in days • Time frame before invalidity when warnings are shown to users • Last password not accepted when changing the password	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "User management", section "Api.Login", section "Api.GetPasswordPolicy", section "Api.ChangePassword" STEP 7 online help

Achievement of SL 3 – 4	CR 1.7 RE1	All CPUs as of firmware version V4.0 support central user management via a remote UMC server. The CPU provides extended password policy options as of V4.0.	List of CPUs with article numbers; see section "Introduction (Page 5)" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Central user management"
Achievement of SL 4	CR 1.7 RE2	See CR 1.7 RE1	See CR 1.7

4.2.7 CR 1.8 – Public Key Infrastructure (PKI) Certificates

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 1.8	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 1.8	The CPU can be supplied with certificates using the certificate manager in the TIA Portal by either generating or importing these certificates.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Managing certificates" Application example "Using Certificates with TIA Portal" (https://support.industry.siemens.com/cs/ww/de/view/109769068/en)

4.2.8 CR 1.9 – Strength of Public Key-Based Authentication

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 1.9	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 1.9	Certificate-based authentication is supported with OPC UA and OUC.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Managing certificates" Application example "Using Certificates with TIA Portal" (https://support.industry.siemens.com/cs/ww/de/view/109769068/en)

Achievement of SL 2 – 4	CR 1.9	Certificate Revocation Lists can be configured via OPC UA.	Application example Dynamic certificate management with SIMATIC S7-1500: OPC UA GDS Push (https://support.industry.siemens.com/cs/ww/en/view/109799888)
Achievement of SL 3 – 4	CR 1.9 RE1	The material of the private key is encrypted in a hierarchical setup where the secret key derived from the password is saved at the top level in a Secure Element in the CPU (see also "Authenticator management" section (Page 25)).	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Confidentiality through encryption"

4.2.9 CR 1.10 – Authenticator Feedback

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.10	All password fields are hidden/masked in the respective dialogs. The Web API defines the error codes and messages for logins. The web pages use the same information and cannot provide additional details on why login failed.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "Api.Login"

4.2.10 CR 1.11 – Unsuccessful Login Attempts

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.11	After multiple failed authentication attempts, the CPU automatically blocks further attempts for several seconds.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "Api.Login"

4.2.11 CR 1.12 – System Use Notification

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 1.12	In the case of authentication via engineering or the web server, the configured device name is shown. This should already indicate the intended use of the CPU. In addition, user-defined web pages can be implemented by authorized personnel to display additional information.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "API (Application Programming Interface)"

4.2.12 CR 1.14 – Strength of Symmetric Key-Based Authentication

Configuration of the products to meet the functional scope of IEC 62443-4-2		
Achievement of SL 1	CR 1.14	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.
Achievement of SL 2 – 4	CR 1.14	No functions that contribute to achieving the defined Security Level are implemented in the product.
Achievement of SL 3 – 4	CR 1.14 RE1	No functions that contribute to achieving the defined Security Level are implemented in the product.

4.3 FR 2 – Use Control

4.3.1 CR 2.1 – Authorization Enforcement

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 2.1	The CPU implements predefined roles and associated user rights and authorizations that can be assigned to users. Local user management: All project users along with their roles and rights (for example, function rights) for all CPUs are managed in the project in the TIA Portal. Central user management: The central user management allows system-wide, central management of users outside TIA Portal. The users and user groups can work in all projects in which they are activated and for the appropriate rights have been assigned to them. All CPUs as of firmware version V4.0 support central user management via a remote UMC server.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management" and section "Central user management" You can find information on function rights and roles and their assignment in the TIA Portal in the STEP 7 online help under "Managing users and roles". List of CPUs with article numbers; see section "Introduction (Page 5)"
Achievement of SL 2 – 4	CR 2.1 RE1	See CR 2.1	See CR 2.1
Achievement of SL 2 – 4	CR 2.1 RE2	Local or central user management enables user-defined creation of roles based on specific functional requirements. In contrast to the previous assignment of protection levels for the CPU, local/central user management is not tied to nested authorization hierarchies.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management", section "Central user management"
Achievement of SL 3 – 4	CR 2.1 RE3	No functions that contribute to achieving the defined Security Level are implemented in the product.	
Achievement of SL 4	CR 2.1 RE4	No functions that contribute to achieving the defined Security Level are implemented in the product.	

4.3.2 CR 2.2 – Wireless Use Control

Configuration of the products to meet the functional scope of IEC 62443-4-2		
Achievement of SL 1 – 4	CR 2.2	Not relevant because the CPU does not have wireless interfaces.

4.3.3 EDR 2.4 – Mobile code

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	EDR 2.4	Mobile code as defined in IEC62443 is executable program code that can be run on a third system without being explicitly installed. The CPU itself does not run any mobile code. However, such mobile code is used within the CPU on the web server, e.g. in the form of JavaScript. The "System web pages" and "Previous web pages" provided by the system are integrity-protected as part of the firmware.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246)
		The installation or modification of user pages requires configuration access to the CPU and can or must be protected accordingly. "User-defined web pages" (HTML) can communicate with the CPU using a limited number of user program commands in order to exchange data between the CPU and the HTML pages via tags. User-defined web pages can contain JavaScript code that is only run in a web browser and not on the CPU itself. User pages can be protected using two runtime rights "open_user_pages" and "manage_user_pages".	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59193560), section "User pages", section "Api.Login"
		User-defined web applications can also be used. The so-called "Web applications that can be loaded by the user" do not interact with the CPU, but are provided only as static content. This can also be JavaScript code which is not run on the CPU.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "Web applications that can be loaded by the user"
		The contents of the SIMATIC Memory Card are integrity-protected and therefore cannot be modified by unauthorized persons.	Structure and use of the CPU memory (https://support.industry.siemens.com/cs/ww/en/view/59193101) Function Manual, section "SIMATIC Memory Card - Overview"
Achievement of SL 2 – 4	EDR 2.4 RE1	See EDR 2.4	See EDR 2.4

4.3.4 CR 2.5 – Session Lock

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 2.5	The CPU web server supports both explicit logout from the session by the user and automatic termination of the session after 30 minutes of inactivity. Users can only access pages to which they have access rights.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "User management"
		The CPU display supports both explicit and automatic removal of access-protected write access after a definable period of time.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "CPU display"
		PG/HMI communication and OPC UA connections are not "Human User Interfaces" that are connected directly to the CPU and should be addressed by operating system mechanisms (e.g. Windows Session Lock). For communication via the TIA Portal, an automatic project lock can be enabled in the settings.	STEP 7 online help, "Overview of user management settings"

4.3.5 CR 2.6 – Remote Session Termination

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 2.6	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 2.6	The various forms of remote communication to the CPU can be terminated as follows: • TIA Portal/HMI (PG/HMI communication): The session can be terminated by the connected communication partner.	
		• Web server: The logged-in session is terminated by explicit logout on the web page. A fixed session timeout of 120 seconds is preset for the Web API. A Runtime timeout can be configured in the TIA Portal user management and used in user-defined web applications.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "Web API sessions", section "User management"

Achievement of SL 2 – 4	CR 2.6	- The OPC UA session can be ended by connected users/applications.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "OPC UA communication"
		If a new configuration is downloaded to the CPU, changed function rights are immediately applied to all existing sessions in the various services (e.g. web server, OPC UA).	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management", section "Central user management"

4.3.6 CR 2.7 – Concurrent Session Control

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 2	CR 2.7	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 3 – 4	CR 2.7	The connection resources for the various communications services are limited by default. The exact limits depend on the CPU type.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "Connection resources"

4.3.7 CR 2.8 – Auditable Events

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 2.8	Various security-relevant events are logged in the diagnostic buffer of the CPU. These include, for example, successful/failed login attempts, password changes, replacement of the SIMATIC Memory Card or copy protection errors.	Diagnostics Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192926) Section "CPU diagnostics buffer"
		In addition, the CPU collects security events as syslog messages in its local cache. Advantages of syslog messages as compared to diagnostic buffer messages: • The CPU records more syslog messages than the diagnostic buffer • Name/IP address of the component that sent the syslog message is visible In addition, the security events can be forwarded to a registered HMI system and saved in an alarm log or forwarded to an external system via CPU program and syslog protocol, for example.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Recording Security events" Full list of security events as syslog messages: "Syslog Messages" product information (https://support.industry.siemens.com/cs/ww/en/view/109823696)

4.3.8 CR 2.9 – Audit Storage Capacity

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 2.9	The diagnostic buffer is a ring buffer. The maximum number of entries depends on the CPU type. If the storage capacity requirements for events exceed the memory capacity of the diagnostic buffer, the oldest entries are overwritten. In addition, the CPU collects security events as syslog messages in its local cache. If the storage capacity requirements for syslog messages exceed the memory capacity of the retentivity medium (cache), the oldest entries are overwritten. For CPUs as of FW version V4.0, the local cache is located in the retentive memory area. As a result, syslog messages are retained after a POWER OFF/POWER ON transition or when the CPU is switched off. This means that events that require one or more CPU restarts, such as restoring the CPU configuration, are also retained in the syslog storage.	Diagnostics Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192926) Section "CPU diagnostics buffer" Maximum number of entries: CPU manuals (https://support.industry.siemens.com/cs/de/de/view/109742691/en) Section "Technical specifications" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Syslog messages"
Achievement of SL 3 – 4	CR 2.9 RE1	The requirement is not met. The requirement can only be met if the syslog messages are forwarded to an external syslog server that supports a configurable memory consumption threshold. Overwriting syslog messages that have not yet been transferred to a syslog server is reported as security event (overflow event) in the syslog storage. If a syslog server is configured in the CPU properties, the CPU also records overwriting of non-transmitted syslog messages in the diagnostic buffer.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Transfer the syslog messages to a syslog server"

4.3.9 CR 2.10 - Response to Audit Processing Failures

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 2.10	a) The CPU saves the security events in a ring buffer for system and diagnostic events in the cache of the CPU. Saving is independent of the main services and functions of the CPU. b) If the storage capacity requirements for syslog messages exceed the memory capacity of the retentivity medium (cache), the oldest entries are overwritten.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Syslog messages"

4.3.10 CR 2.11 – Time stamps

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 2.11	The CPU uses the time stamp format from the syslog protocol (derived from RFC3339). Time stamps are always Universal Time Coordinated (UTC) and specify when the event occurred in the CPU.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Time synchronization"
Achievement of SL 2 – 4	CR 2.11 RE1	The CPU supports NTP via Industrial Ethernet interfaces and DP time synchronization via PROFIBUS. In addition, time synchronization via the central backplane bus in connection with inserted communications processors (e.g. CP1543-1) are supported.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Time synchronization" Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Industrial Ethernet Security with CP 1543-1"
Achievement of SL 4	CR 2.11 RE2	All changes to the time system are logged as critical operations.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Recording Security events"

4.3.11 CR 2.12 – Non-Repudiation

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 2.12	The CPU contains user information in a structured data lock (SD) in each syslog frame that is logged. The user information can contain either a user name or a session ID. If the "anonymous" user performs an action, some of the user information in a log entry can either be empty or contain, for example, "Anonymous" or "not applicable", depending on the security event.	"Syslog Messages" product information (https://support.industry.siemens.com/cs/ww/en/view/109823696) Section "SE_SYSTEMTIME_CHANGED"
		By default, the anonymous user is not enabled.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "From the access level to the function right of users"
Achievement of SL 4	CR 2.12 RE1	See CR 2.12 The session information in the SD block contains fields such as "protocolType", "userName" and "src" to determine which person, which software process or which device performed a specific action.	"Syslog Messages" product information (https://support.industry.siemens.com/cs/ww/en/view/109823696) Section "SE_SYSTEMTIME_CHANGED", Section "Parameter Details"

4.3.12 EDR 2.13 – Use of physical diagnostic and test interfaces

Configuration of the products to meet the functional scope of IEC 62443-4-2		
Achievement of SL 1	EDR 2.13	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.
Achievement of SL 2 – 4	EDR 2.13	Not relevant because there are no external diagnostics and test interfaces.
Achievement of SL 3 – 4	EDR 2.13 RE1	Not relevant because there are no external diagnostics and test interfaces.

4.4 FR 3 – System Integrity

4.4.1 CR 3.1 – Communication Integrity

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 3.1	The following communications services/protocols have mechanisms for checking the integrity of the received communication data: • PG/HMI access via the TLS-based S7 protocol after establishment of an authenticated connection. • Syslog messages to a syslog server (authentication on client and server side configurable) • As of FW version V4.0: Central user management via UMC server (authentication of the UMC server)	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Configuring access protection for the CPU" Section "Syslog messages" Section "Central user management"
		• Web server via HTTPS after successful user authentication.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "How communication with certificates works: HTTP over TLS"
		• OPC UA with corresponding security concept (additional user authentication with user name/password configurable) • Authentication on client side with OPC UA certificate	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Security at OPC UA"
		• Open User Communication incl. TLS layer and authentication on client side via Secure OUC certificate	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Secure Communication", "Open User Communication"
		For PROFINET communication, additional measures should be implemented to secure this communication. The same applies to protocols without native security such as Modbus/TCP. In addition, other security measures should also be used, e.g. Security CPs or SCALANCE S.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Industrial Ethernet Security with CP 1543-1" SCALANCE S documentation (https://sieportal.siemens.com/su/bljyJ)

Achievement of SL 1 – 4	CR 3.1	The functions OPC UA, web server and Open User Communication are disabled by default and need to be enabled in STEP 7 if needed.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Communications protocols and port numbers used for Ethernet communication"
Achievement of SL 2 – 4	CR 3.1 RE1	See CR 3.1	See CR 3.1

4.4.2 EDR 3.2 – Protection from malicious code

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	EDR 3.2	The CPUs offer access protection for engineering based on passwords in user management. In addition, the firmware is protected against unauthorized manipulated by digital signatures. The CPU checks these signatures during firmware updates. Additional detection/notification can be achieved by monitoring the configuration changes (security event).	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management", section "Central user management" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Signed firmware update for CPUs" You can find more information on the integrity check of CPU programs based on checksums in the STEP 7 online help, "Comparison of PLC programs based on checksums"

4.4.3 CR 3.3 – Security Functionality Verification

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 3.3	The security functions can be checked by regularly testing the security measures used, including an evaluation of the corresponding response (e.g. no access, triggering of a security event). Security events are created when security mechanisms respond during the test (e.g. incorrect login, installation of a manipulated firmware file, replacement of the SIMATIC Memory Card).	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) "Industrial cybersecurity" section List of security events and the associated trigger conditions: "Syslog Messages" product information (https://support.industry.siemens.com/cs/ww/en/view/109823696)
Achievement of SL 4	CR 3.3 RE1	See CR 3.3	See CR 3.3

4.4.4 CR 3.4 – Software and Information Integrity

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 3.4	The component performs an integrity check of the firmware (verification of the digital signature during the firmware update). In addition, the CPU offers an integrity check for configuration data during download and CPU start: • Integrity check of the user program configuration • Integrity check of the hardware configuration If an integrity protection error is detected, a message is shown in the diagnostic buffer (security event).	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Signed firmware update for CPUs" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Overview of the protection functions", "Integrity protection" You can find more information on the integrity check of CPU programs based on checksums in the STEP 7 online help, "Comparison of PLC programs based on checksums"
Achievement of SL 2 – 4	CR 3.4 RE1	See CR 3.4 The component firmware is encrypted and signed by a trusted instance (Siemens Trust Center). The firmware is only loaded during the boot procedure if the signature has been verified successfully.	See CR 3.4 S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Signed firmware update for CPUs", section "Secure Boot for CPUs"

Achievement of SL 3 – 4	CR 3.4 RE2	If integrity protection violations are detected, security events that can be evaluated or archived by external systems are generated automatically.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Recording Security events"

4.4.5 CR 3.5 – Input Validation

Configuration of the products to meet the functional scope of IEC 62443-4-2		
Achievement of SL 1 – 4	CR 3.5	The CPU checks the syntax and content of the input data received via the network.

4.4.6 CR 3.6 – Deterministic Output

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 3.6	The CPU provides the possibility of placing outputs into a predefined state (switched off or configured) in the event of an unusual situation, e.g. network overload.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "STOP mode"

4.4.7 CR 3.7 – Error Handling

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 3.7	The error messages in the diagnostic buffer are designed in such a way that no critical information can be read out unauthorized.	
		Web server: The Web API is based on JSON-RPC V2.0. All error codes and descriptions for the API end points are documented in the Web server Function Manual in the sections on the API methods.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "API (Application Programming Interface)"
		If a user does not have the authorization to open a specific web page, the user is forwarded to a login page. If an action fails, corresponding information is displayed.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "System web pages", section "Api.Login", section "Api.GetPermissions"

4.4.8 CR 3.8 – Session Integrity

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 3.8	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 3.8	The following communications services/protocols of the CPU can use TLS (Transport Layer Security) for secure data transfer: • PG/HMI communication • Web server • OPC UA • Secure OUC • Syslog • Communication with UMC server (as of CPU FW version V4.0) The following communications services/protocols of the CPU have mechanisms for checking the integrity of the received communication data:	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Confidentiality through encryption" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Syslog messages" Section "Central user management"
		• It is ensured within the CPU that PG/HMI communication uses unique, non-reusable sessions.	
		• Web server via HTTPS after successful user authentication. A client contains either an authentication token for the JSON-RPC Web API or a session cookie for web page access.	Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109977246) Section "Web API sessions", section "Interaction between web applications"
		• OPC UA provides its own session management.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Security at OPC UA"
		• Secure OUC offers programmable TLS communication. Session negotiation must be implemented via a user program depending on the desired communication method.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Secure Communication" Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Open User Communication"

Achievement of SL 2 – 4	CR 3.8	For PROFINET communication, additional measures should be implemented to secure this communication. The same applies to protocols without native security such as Modbus/TCP. In addition, other security measures should also be used, e.g. Security CPs or SCALANCE S.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Industrial Ethernet Security with CP 1543-1" SCALANCE S documentation (https://sieportal.siemens.com/su/bljyJ)
		If a new configuration is loaded to the CPU, changed function rights are immediately applied to all existing sessions in the various services.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Local user management", Section "Central user management"

4.4.9 CR 3.9 – Protection of Audit Information

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 3.9	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 3.9	Access to the diagnostic buffer and the syslog messages in the CPU is only possible with the relevant access rights: • From the TIA Portal via TLS (only to the diagnostic buffer) • Via the CPU web server With the required access rights, syslog messages may be deleted because decommissioning of the CPU is a valid use case. Writing to the diagnostic buffer and the syslog messages of the CPU is only possible from the firmware. If the CPU is connected to an external syslog server as syslog client, the connection can be secured via TLS.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Recording security events", section "Syslog messages"
Achievement of SL 4	CR 3.9 RE1	No functions that contribute to achieving the defined Security Level are implemented in the product. Syslog messages can be sent to external systems (SIEM systems) that may support this requirement.	See CR 3.9

4.4.10 EDR 3.10 – Support for Updates

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	EDR 3.10	CPUs can be updated by the firmware updates made available by the manufacturer (in STOP mode of the CPU). It is currently only possible to perform a firmware update of S7-1500R/H-CPUs when the R/H system is in STOP mode.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Firmware update"
Achievement of SL 2 – 4	EDR 3.10 RE1	The firmware images have mechanisms to protect the integrity and authenticity and are automatically checked by the CPU during the firmware update with the "Secure Boot" function before the actual installation.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Secure Boot for CPUs"

4.4.11 EDR 3.11 – Physical Tamper Resistance and Detection

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	EDR 3.11	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	EDR 3.11	No functions that contribute to achieving the defined Security Level are implemented in the product. The front flap of the CPU can be secured with a lock or seal to detect unauthorized access to the SIMATIC Memory Card, for example. Additional physical protection is not integrated, but can be implemented by external measures such as a locked control cabinet, etc.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Protection by locking the CPU/interface module"
Achievement of SL 3 – 4	EDR 3.11 RE1	No functions that contribute to achieving the defined Security Level are implemented in the product. When the SIMATIC Memory Card is replaced, a corresponding security event is created in the diagnostic buffer. External measures are required for further protection.	STEP 7 online help, "What you should know about group alarms for security events (S7-1500)".

4.4.12 EDR 3.12 – Provisioning Product Supplier Roots of Trust

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	EDR 3.12	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	EDR 3.12	The CPU supports Product Supplier Roots of Trust in order to check, for example, the authenticity of the firmware images during the boot and update process ("Secure Boot" function).	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Secure Boot for CPUs"

4.4.13 EDR 3.13 – Provisioning Asset Owner Roots of Trust

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	EDR 3.13	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	EDR 3.13	Trusted certificates can be installed via the certificate management in the TIA Portal and transferred to the CPU. This function can be used for various communications services.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Managing certificates" Application example "Using Certificates with TIA Portal" (https://support.industry.siemens.com/cs/ww/de/view/109769068/en)
		The contents of the SIMATIC Memory Card, especially the certificates contained, cannot be changed by unauthorized persons because the integrity check of the configuration data will fail and the CPU will not accept the SIMATIC Memory Card.	Structure and use of the CPU memory (https://support.industry.siemens.com/cs/ww/en/view/59193101) Function Manual Section "SIMATIC Memory Card - Overview"

4.4.14 EDR 3.14 – Integrity of the Boot Process

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1-4	EDR 3.14	All CPUs as of firmware version V4.0 guarantee a boot process protected by a hardware mechanism. On startup, the firmware and configuration data is checked by the CPU with "Secure Boot".	List of CPUs with article numbers; see section "Introduction (Page 5)" CPU manuals (https://support.industry.siemens.com/cs/de/de/view/109742691/en) Section "Technical specifications", "Secure Boot" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Secure Boot for CPUs"
Achievement of SL 2 – 4	EDR 3.14 RE1	See EDR 3.14	See EDR 3.14

4.5 FR 4 – Data Confidentiality

4.5.1 CR 4.1 – Information Confidentiality

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 4.1	Confidential data such as cryptographic keys for the CPU are saved encrypted in the project and transferred encrypted to the CPU. The loaded components are related to each other like two matching puzzle pieces: • The project is bound to the loaded key information. • The loaded key information is bound to the password that was assigned during configuration. Project and key information must match; otherwise, the CPU will not start. In a replacement part scenario, the password and thus the key information must be transferred to the new (replacement) CPU in addition to the configuration; otherwise, the project cannot be decrypted.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Protection of confidential configuration data", section "Useful information for the protection of confidential PLC configuration data"

4.5.2 CR 4.2 – Information Persistence

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 4.2	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 4.2	This requirement can be met by removing the SIMATIC Memory Card and resetting the CPU to factory settings.	S7-1500/ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Secure decommissioning" Section "Resetting the CPU to factory settings"
Achievement of SL 3 – 4	CR 4.2 RE1	The internal architecture of the CPU ensures that firmware components can only access memory assigned to them. In addition, sensitive data such as keys is deleted securely after use.	
Achievement of SL 3 – 4	CR 4.2 RE2	Relevant data is saved on the SIMATIC Memory Card and can be physically removed by removing the card. The data can be deleted via the PC. Successful removal of retentive data in the CPU can be checked through later online access to the CPU.	

4.5.3 CR 4.3 – Use of Cryptography

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 4.3	The CPUs use state-of-the-art cryptographic algorithms and individual requirements within different use cases: • Protection of authorizations in the CPU configuration • Protection of confidential PLC configuration data • Firmware integrity and authenticity • Web server (HTTPS) • Transfer the syslog messages to a syslog server (via TLS certificate) • Communication with a UMC server (as of CPU FW version V4.0)	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Protection", Section "Signed firmware update for CPUs", Section "Syslog messages"

		- PG/HMI communication (integrity of the TLS-based S7 protocol) - Secure Open User Communication (TLS) - OPC UA	Section "Central user management" Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Secure PG/HMI communication", section "Secure Communication"

4.6 FR 5 – Restricted Data Flow

4.6.1 CR 5.1 – Network Segmentation

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 5.1	The CPU offers support for segmented networks through IP-based communication and multiple network interfaces across network boundaries. Some protocols (e.g. PROFINET) are only designed for one local area network, in principle. However, PROFINET can be used in connection with VLANs. In this case, Ethernet frames are specifically tagged to support real-time communication.	PROFINET with STEP 7 Function Manual (https://support.industry.siemens.com/cs/ww/en/view/49948856) Section "Network components and software" SCALANCE X documentation (https://sieportal.siemens.com/su/blisn)
		In addition, through the availability of multiple interfaces, some CPUs offer further support for network segmentation because PROFINET/PROFIBUS segments can be separated by the CPU.	Detailed information on the individual CPU types and their interfaces can be found in the manuals for the CPUs (https://support.industry.siemens.com/cs/de/de/view/109742691/en)

4.7 FR 6 – Timely Response to Events

4.7.1 CR 6.1 – Audit Log Accessibility

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 6.1	The CPU provides a diagnostic buffer containing system and diagnostics information. Read access to the diagnostic buffer is possible via the: - TIA Portal - CPU web server - CPU display - HMI connection (diagnostics viewer or HMI alarm log)	Diagnostics Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192926) Section "CPU diagnostics buffer" STEP 7 online help, "Reading out the diagnostics buffer of a CPU" Web server Function Manual (https://support.industry.siemens.

			com/cs/ww/en/view/109977246) Section "API (Application Programming Interface)"
Achievement of SL 3 – 4	CR 6.1 RE1	The security events can be read out from the diagnostic buffer via the user program. They can also be forwarded to an external SIEM system by means of syslog messages.	STEP 7 online help, "GET_DIAG: Read diagnostic information" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Syslog messages"

4.7.2 CR 6.2 – Continuous Monitoring

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 6.2	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 6.2	In the case of security-relevant events such as login, configuration changes or violation of integrity protection, security events are created in the CPU's cache. They can be monitored by external systems (e.g. SIEM system via syslog messages).	STEP 7 online help, "What you should know about group alarms for security events (S7-1500)" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Syslog messages"

4.8 FR 7 – Resource Availability

4.8.1 CR 7.1 – Denial of Service Protection

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 7.1	The CPU works with specific and limited communication resources. In the case of high communication load or a denial of service (DoS) attack, this can affect the overall communication performance. However, the core functions of the CPU are unaffected.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Connection resources"
Achievement of SL 2 – 4	CR 7.1 RE1	The CPU has a defined set of resources for the communication functionality which can be configured within certain limits. If these resources are used up by denial of service events, this affects the CPU communication, but not the execution of the user program.	See CR 7.1 You can find more information on connection resources and connection diagnostics in the STEP 7 online help.

4.8.2 CR 7.2 – Resource Management

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 7.2	The CPU has a various real-time priority levels. User programs can define priority levels within a specific range.	Cycle and response times Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59193558) Section "Program execution" S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Events and OBs" Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Connection resources"
		System components run on specified priority levels which can extend from non-real-time to real-time depending on the runtime requirements.	PROFINET with STEP 7 Function Manual (https://support.industry.siemens.com/cs/ww/en/view/49948856) Section "Real-time communication"

4.8.3 CR 7.3 – Control System Backup

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 7.3	A backup of all data (except diagnostic buffer), such as: • Configuration data (fail-safe with an F-CPU) • Data for backup and restore • Dynamic configurations is possible via: • TIA Portal • SIMATIC Automation Tool • CPU web server • CPU display In addition, the following methods are supported: • Backup from online device • Upload from device (software) • Upload device as new station (hardware and software) Depending on the backup method used, it may be necessary to switch the CPU to STOP mode. The integrity of this data is always verified by the CPU.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Backups and data backups" Section "Backing up and restoring the CPU configuration" Section "SIMATIC Automation Tool"

Achievement of SL 2 – 4	CR 7.3 RE1	The backup files created by a CPU contain integrity protection that is used for verification on later restore to a CPU. In addition, the CPU configuration data forms part of a TIA Portal project and is therefore subject to the same integrity protection mechanisms.	You can find information on integrity protection in the S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Overview of the protection functions"

4.8.4 CR 7.4 – Control System Recovery and Reconstitution

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 7.4	All previously backed-up, such as: • Configuration data • Data for backup and restore • Dynamic configurations can be restored using the TIA Portal or the SIMATIC Memory Card.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Backing up and restoring the CPU configuration" Structure and use of the CPU memory (https://support.industry.siemens.com/cs/ww/en/view/59193101) Function Manual Section "SIMATIC Memory Card"

4.8.5 CR 7.6 – Network and Security Configuration Settings

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 7.6	The security function is implemented in CPUs and must be used in accordance with the general security policies.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Industrial cybersecurity" Specific information on configuring the CPU for secure operation: S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Secure operation of the system" Section "Protection" Device-specific properties: CPU manuals (https://support.industry.siemens.com/cs/de/de/view/109742691/en)

			Section "Cybersecurity-related information"
Achievement of SL 3 – 4	CR 7.6 RE1	The TIA Portal provides an Openness interface that enables machine-readable access to certain CPU-configured configuration data. The user can perform the following actions with TIA Portal Openness: • Create project data • Change projects and project data • Delete project data • Read in project data • Make projects and project data available to other applications There is no predefined report of the security settings, but one can be created based on the data from TIA Portal Openness.	System Manual SIMATIC Openness: Automating creation of projects (https://support.industry.siemens.com/cs/ww/en/view/109477163)

4.8.6 CR 7.7 – Least Functionality

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1 – 4	CR 7.7	Only essential functions and services are enabled in the CPU as standard. Additional functions can be enabled if required. Physical network ports can also be disabled if required.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Communications protocols and port numbers used for Ethernet communication"

4.8.7 CR 7.8 – Control System Component Inventory

Configuration of the products to meet the functional scope of IEC 62443-4-2			More information
Achievement of SL 1	CR 7.8	Not applicable. In 62443-4-2, no requirement to achieve the Security Level is defined.	
Achievement of SL 2 – 4	CR 7.8	Information on the device type, serial number etc. is available in the form of I&M data from the CPU.	S7-1500, ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792) Section "Identification and maintenance data"
		DCP is a protocol for automatic detection and basic configuration of PROFINET devices. For PROFINET networks, the DCP protocol can be used to detect and request information from a CPU.	PROFINET with STEP 7 Function Manual (https://support.industry.siemens.com/cs/ww/en/view/49948856) Section "Configuring DCP"

Achievement of SL 2 – 4	CR 7.8	To protect the components from malicious or inadvertent write access, DCP is enabled by default in a write protection mode.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Communications protocols and port numbers used for Ethernet communication"
		The network management protocol SNMP (Simple Network Management Protocol) is used for performing monitoring and diagnostics of the network topology. SNMP is also used in a PROFINET IO system for managing the network infrastructure and the IO controller/IO devices. The CPU supports SNMP to make information available for inventory purposes through network requests.	PROFINET with STEP 7 Function Manual (https://support.industry.siemens.com/cs/ww/en/view/49948856) Section "Configuring SNMP"
		SNMP is disabled in the CPU by default and must be explicitly enabled.	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) Section "Communications protocols and port numbers used for Ethernet communication", section "SNMP"