SIEMENS

SIMATIC

SIMATIC Drive Controller

Product Information

Scope

Scope of validity of the product information

This product information supplements the documentation for the SIMATIC Drive Controller and takes precedence over our system manuals, function manuals and equipment manuals. The statements in this product information are valid for the following SIMATIC Drive Controllers:

SIMATIC Drive Controller	Article number
CPU 1504D TF	6ES7615-4DF10-0AB0
CPU 1507D TF	6ES7615-7DF10-0AB0

You might find an updated product information on the SIMATIC Drive Controller on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109772684)

The SIMATIC Drive Controller CPU has technology functions such as a modular S7-1500T CPU. You can find additional information on the technology functions in the Product Information for SIMATIC S7-1500 Motion Control on the Internet (https://support.industry.siemens.com/cs/de/en/view/109794046).

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 more information on protective industrial cybersecurity measures for implementation, please visit (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

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 customers' exposure to cyber threats.

To stay informed about product updates at all times, subscribe to the Siemens Industrial Cybersecurity RSS Feed under (https://new.siemens.com/global/en/products/services/cert.html).

Corrections to the SIMATIC Drive Controller System Manual, Edition 11/2023

Local user management

Loading to device

If you want to download changes to the user configuration in RUN mode, the hardware configuration in the CPU and in the STEP 7 project must be unchanged. Otherwise, a transition to STOP is required to download the user configuration together with the changed hardware configuration.

Save your STEP 7 project and then configure only the desired changes in the user configuration. Load your project into the CPU.

Changes to the access rights for the "Anonymous" user can only be loaded in STOP mode.

A fail-safe S7-1500 CPU may only load a user to whom the runtime right "Full access including fail-safe" is assigned. Otherwise, STEP 7 displays an error message when loading the configuration.

Explanations of the options for the user management download (Load preview):

- If you select the option "Keep online user management data", the local user management is not downloaded to the CPU.
- If you select the option "Download all user management data (reset to project)", all passwords changed online via WebAPI are deleted. After the download, the configured local user data is valid.
- If you select the option "Update user management data, but keep online passwords" and have not changed existing user names, the passwords changed online via WebAPI are retained. Only changes to function rights and/or roles take effect. Newly configured users are downloaded with their settings and deleted users are no longer available after the download to the CPU.
  If you have changed a user name in the project and assigned a password to this user in the project, this setting becomes valid after the download. The previously valid user name with the password changed online is deleted during the download.

Restrictions on continued use of the access levels

The🔒icon is incorrectly displayed in the web server when the access control is configured as follows:
You have not configured access control and the "Anonymous" user does not have full access rights (e.g. read-only access) to the CPU.

Corrections to the Communication Function Manual, Edition 11/2023

OPC UA - Global Discovery Push (GDS Push) function: Update problems for downloaded certificates

Under certain conditions, the CPU does not register a downloaded certificate (e.g. a new OPC UA server certificate, or an updated web server certificate). A certificate error may be signaled during a connection attempt in this case.

The update problem occurs only when the CPU still manages certificates that were provided during runtime (GDS Push) and when certificates are then transferred by loading the hardware configuration to the CPU. The certificates loaded via the hardware configuration are not registered by the CPU under these conditions.

Examples:

- You have initially enabled the GDS Push function and selected the option "... use certificates provided during runtime" for the certificate settings and loaded this configuration. The required server certificate as well as the trust lists/CRLs are provided exclusively via GDS Push methods in this case.
- You then change the hardware configuration by adding new certificates or changing existing certificates (e.g. web server certificates or certificates for secure PG/HMI communication). During loading, you have **not** deleted existing certificates provided during runtime so that you can use them later.
  Result: The newly loaded server certificates (e.g. web server certificates or certificates for secure PG/HMI communication) are not registered by the CPU.
- The problem also occurs when you have disabled the GDS Push function and selected the option "... use configured and downloaded certificates" for the certificate settings and loaded this configuration. During loading, you have **not** deleted existing certificates provided during runtime so that you can use them later.
  Result: The newly loaded OPC UA server certificate is not registered by the CPU.

Solution: When the CPU still has certificates that were provided during runtime and you want to transfer new/changed certificates by loading the hardware configuration to the CPU, proceed as outlined below:

- After loading the configuration, perform a "Memory reset" or restart the CPU (POWER OFF > POWER ON). After these measures, the CPU reorganizes the loaded configuration and uses the current certificates.

OPC UA server: Change in behavior when using multi-dimensional arrays in a UDT

From firmware version V2.9.4 onwards, S7-1500 CPUs code multi-dimensional arrays within structures according to OPC UA specification V1.04. CPUs with older firmware versions code the corresponding structures in another form. If you have used multi-dimensional arrays in structures for CPUs with older firmware versions and are upgrading to the latest firmware version, then you must modify your client programs accordingly.

Certificate checks when establishing encrypted connections (e.g. OPC UA)

An S7-1500 CPU as of firmware version V3.1 has an extended certificate check compared with predecessor versions.

Consequently, additional warnings/errors may appear in the diagnostics buffer (BadSecurityChecksFailed), which did not occur in predecessor versions. However, these messages do not prevent the connection from being established.

This refers to the following messages:

Error code (hexadecimal values)	Name of the error	Explanation
2852_0000	Key Usage Certificate Sign invalid for non CA	In a CA-derived certificate, the keyCertSign bit has been set in the KeyUsage field despite not being permitted.
2859_0000	Basic constraints not critical	The BasicContraints field of the CA of a certificate is not set as "critical", even though this should always be the case in CA certificates.
285C_0000	CA no Key Usage	The KeyUsage field of the CA of a certificate is not present, even though it should always be present in CA certificates.
2017_0000	CA-Signed Application Instance CA Certificate	In a CA-derived certificate, the CA bit has been set despite not being permitted.
2018_0000	Self-Signed Application Instance CA Certificate	In a self-signed certificate, the CA bit has been set despite not being permitted.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

SIMATIC Drive Controller
A5E48022408-AM, 02/2024