Alarms & Events and Historical Data via OPC UA

SIMATIC NET OPC UA Server

https://support.industry.siemens.com/cs/ww/en/view/67295801

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

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

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Introduction

1.1 Overview

SIMATIC NET OPC server communication functions for OPC UA

OPC Server provides standardized access to the SIMATIC NET industrial communication networks.

SIMATIC NET OPC Server supports the interfacing of applications with any automation components networked over PROFIBUS or Industrial Ethernet. SIMATIC NET OPC Server offers the following communication functions for OPC UA:

- S7 communication
  - S7 OPC UA Server
  - S7OPT OPC UA Server
- Open communication services (SEND/RECEIVE)
  - SR OPC UA Server
- PROFIBUS DP
  - DP OPC UA Server

S7 communication services

The S7 communication of the SIMATIC NET OPC Server for OPC UA supports the following services, among others:

- OPC Alarms & Events
  Transfer of process alarms and events
- Historical data on OPC UA
  Reading of historical data from S7 tags stored in a database for up to 360 hours.

This application example shows how to use the above services.

The following components are used in this application example:

- SIMATIC NET OPC Server for OPC UA: S7OPT OPC UA Server
- OPC client: UA Expert
- S7-1500 CPUs

1.2 OPC Alarms & Events

OPC Alarms & Events is a specification for the transmission of process alarms and events. It is designed to be very flexible and can, therefore, be applied to a wide variety of event sources. The spectrum ranges from simple events to complex events and even events with an acknowledgement obligation.

The OPC specification defines the possible state transitions for conditional events in a state diagram.

The OPC Alarms & Events Servers have the following functions:

- Detection of events
- Determining the state of an event
- Acknowledging an event (acknowledgement)
- Monitoring the confirmation

New events can also be reported without confirmation.

The standardized OPC Alarms & Events interface allows to use these requirements.

1.2.1 Events

Events are special states in the process that must be reported to a receiver.

Event message

Event messages provide the parameters defined by the OPC specification and, if applicable, accompanying values defined by the manufacturer.

There are the following types of event messages:

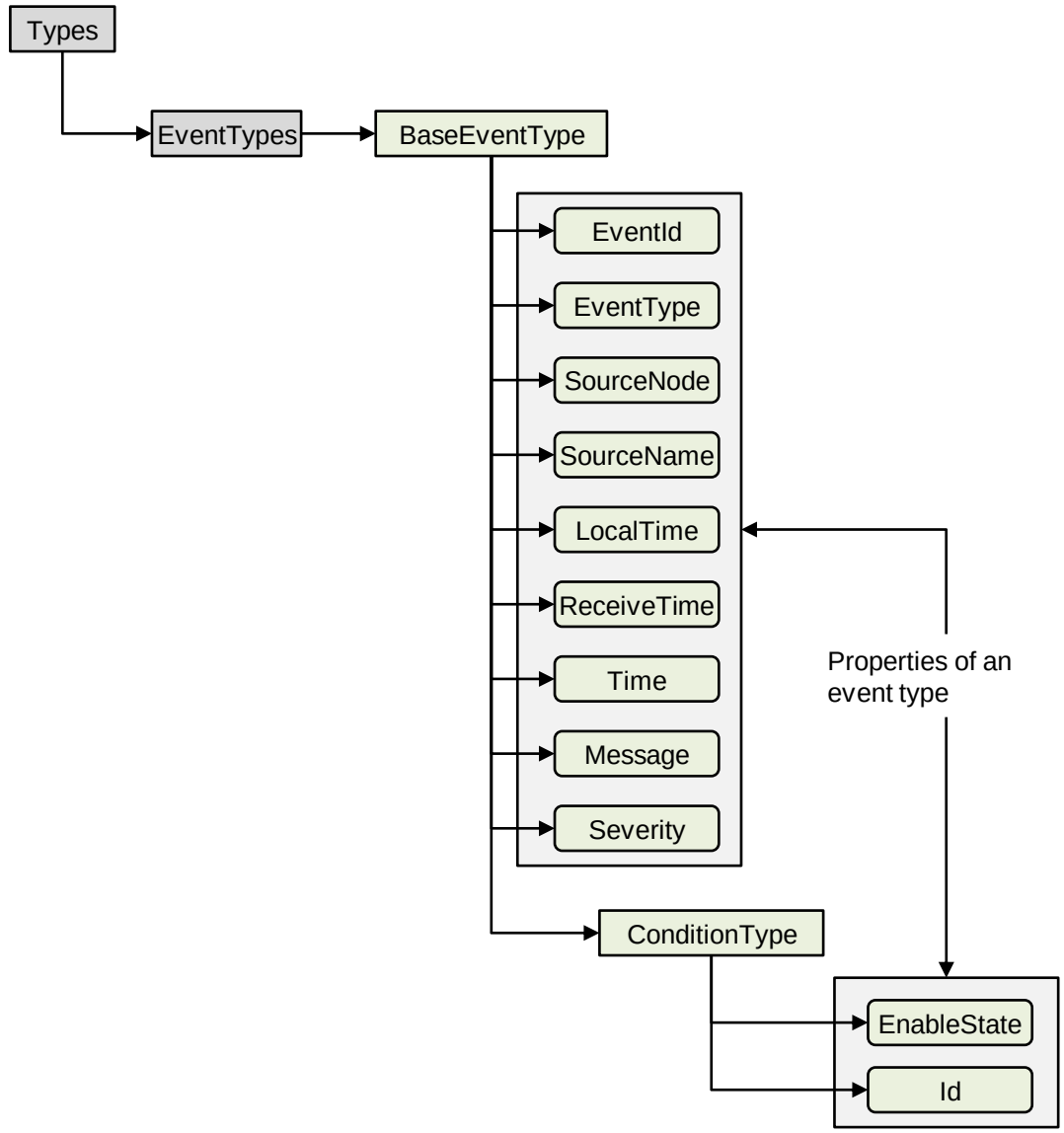
- simple event messages
- complex condition-based event messages with or without acknowledgement by the OPC Client

Properties of an event

All information of an event is stored in its properties. The properties of an event are defined by the event type.

- Each event type defines which properties it offers.
- Each event type has its own properties or inherited properties. This results in an extensive event type hierarchy.

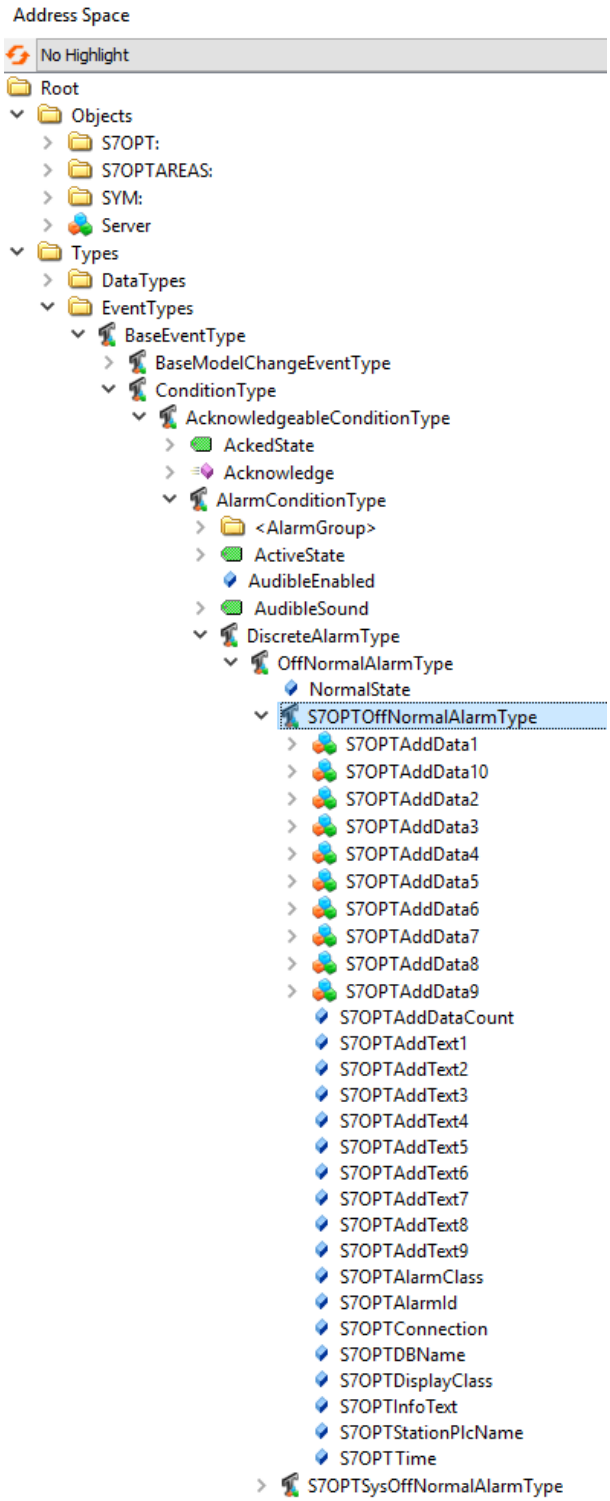
Figure 1-1



The event type hierarchy of the OPC Alarms & Events Server can be determined with an OPC client, e. g. UA Expert from Unified Automation.

The following figure shows an overview of the OPC UA event and alarm types of the SIMATIC NET S7OPT OPC UA Server in UA Expert.

Figure 1-2



1.2.2 Principle of operation

OPC Alarms & Events class model

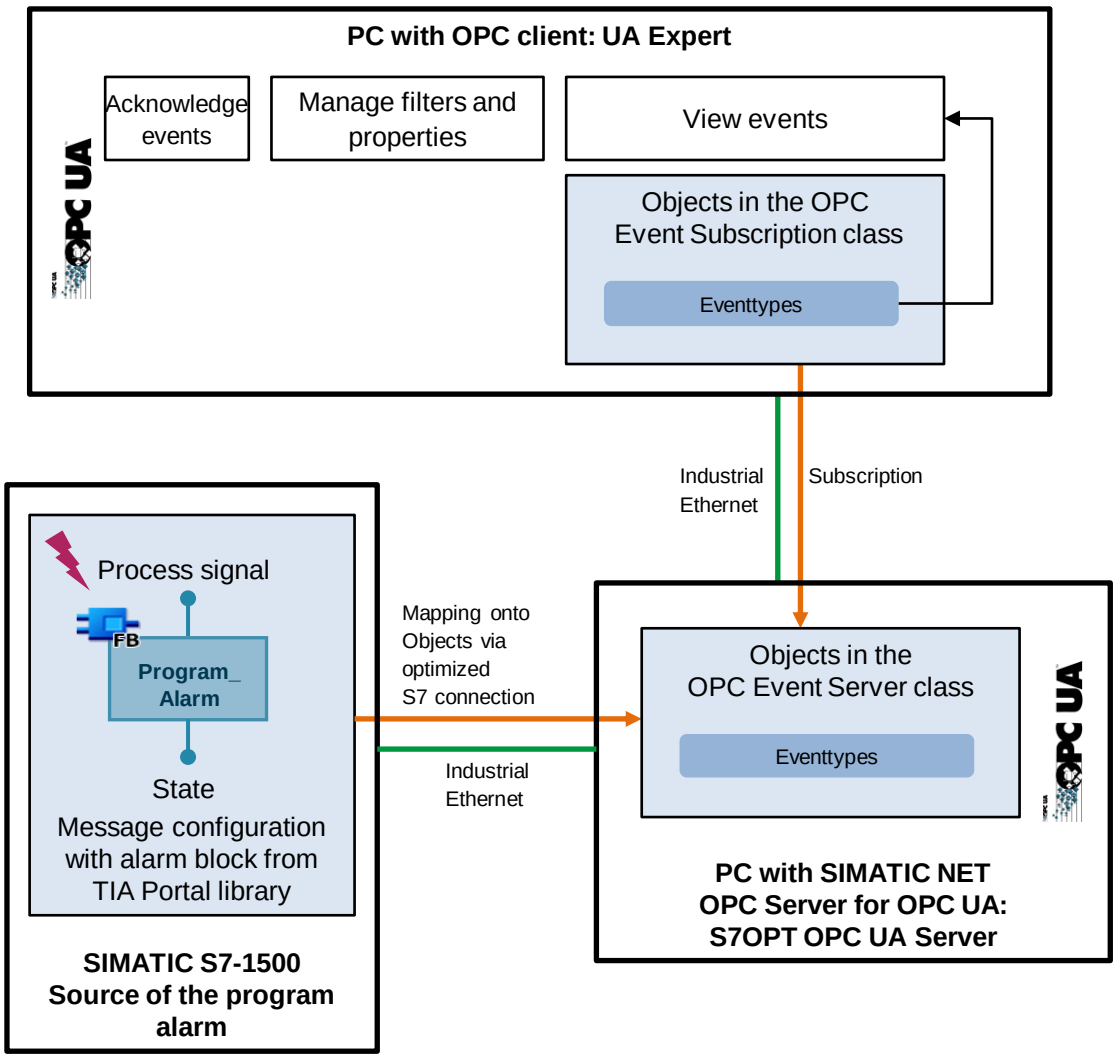
The class model of OPC Alarms & Events allows the adaptation of the OPC client to the requirements of an automation solution. OPC Alarms & Events distinguishes between three classes:

- OPC Event Server
- OPC Event Subscription
- OPC Event Area Browser

Note Objects in the OPC Event Area Browser class are optional and are not supported by the SIMATIC NET OPC Alarms & Events Server.

The following figure shows what the classes of OPC Alarms & Events do in order to report program alarms of an S7-1500 CPU to the S7OPT OPC UA server and display them in the OPC client.

Figure 1-3



In this example, the alarm block "Program_Alarm" is called in the user program of the S7-1500 CPU in order to trigger the following program alarms:

- Program alarm with required acknowledgement and 2 associated values
- Program alarm for information purposes only

The program alarms are transferred to the S7OPT OPC UA Server via an optimized S7 connection. In the S7OPT OPC UA server, the program alarms are mapped to objects of the OPC Event Server class and displayed in the OPC client.

The OPC client registers with the S7OPT OPC UA server for receipt of messages and creates one or more objects of the OPC Event Subscription class. An object of the OPC Event Subscription class is a subscription to several events.

Objects of the OPC Event Subscription classes manage the necessary filters and properties on a client-specific basis. Thanks to filtering, the OPC client can define which events are received.

Event messages requiring acknowledgement can be acknowledged in the OPC client.

Filtering

The OPC client can filter for events with certain properties and for the values of those properties.

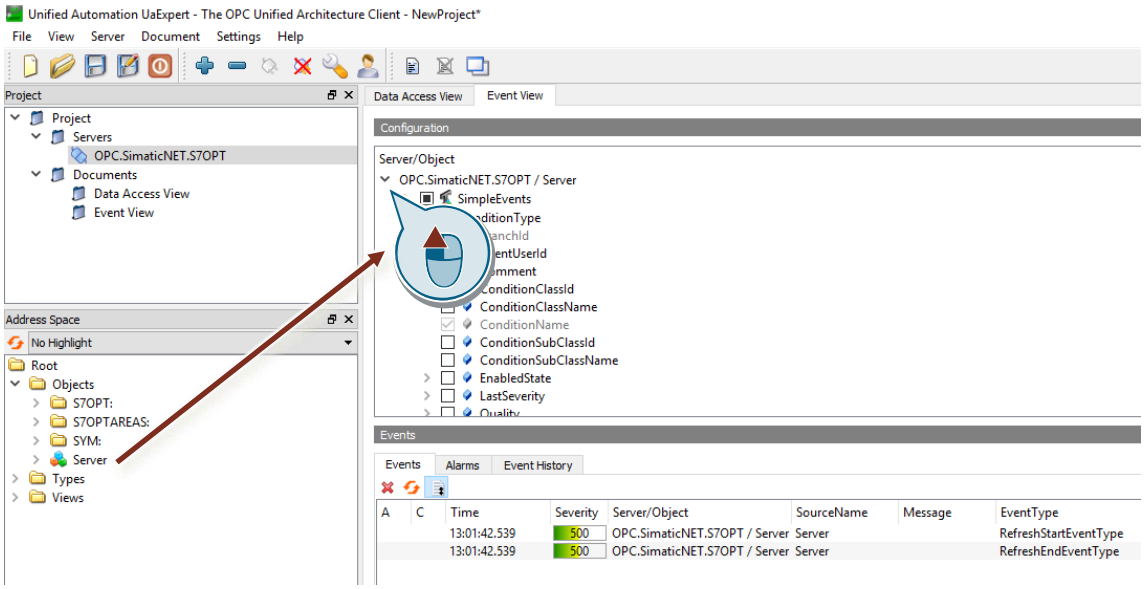
The OPC client can define which events it wants to receive by using the following filter criteria:

- Event type
- Category
- Priority
- Event source

An event is only forwarded to the OPC client if it matches the filter values in all filter criteria.

Display events in UA Expert

Figure 1-4



In this example, UA Expert is used as the OPC Client.

In UA Expert, the events reported by the S7OPT OPC UA server appear in the "Event View". In the "Event View" it is possible to acknowledge event messages requiring acknowledgement.

The "Event View" consists of 3 sections:

1. Configuration
   To display events, drag & drop the object, e. g. server object, whose EventNotifier attribute is set to "SubscribeToEvents", into the Configuration section.
   When you expand the server object tree, you can define the properties of the event messages to be displayed in the "Details" section, such as associated values and additional informational texts.
2. Events
   The Events section has 3 tabs:
   - Events
     When an event message is triggered, the event is displayed in the "Events" tab. Select the event to display more properties of the event in the Details section.
   - Alarms
     In the "Alarms" tab, you have the option of acknowledging event messages.
   - Event History
     The event history is displayed in the "Event History" tab.
   -
3. Details
   The "Details" section displays the properties of the event messages, such as associated values and additional informational texts.

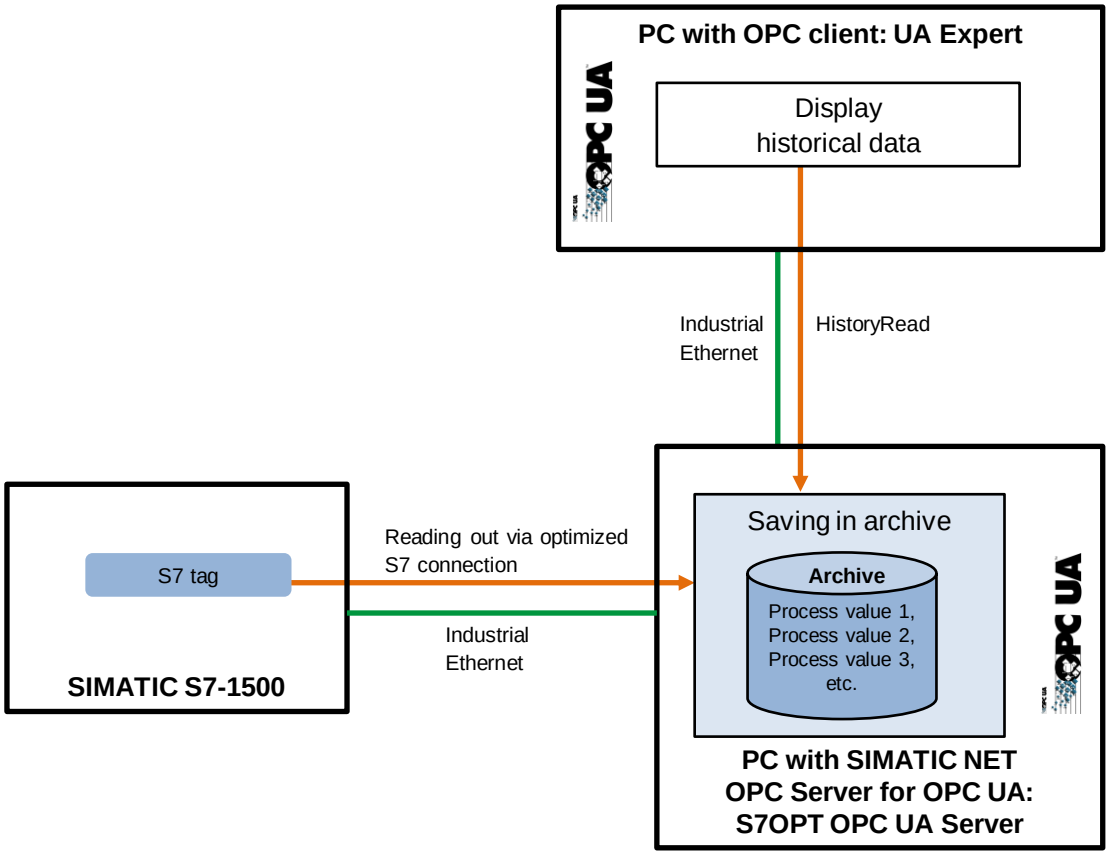
1.3 Historical data on OPC UA

OPC UA HA (Historical Data Access) enables access to historical data from S7 tags archived in a database for up to 360 hours.

Principle of operation

The following figure shows how to use the S7OPT OPC UA Server to get historical data for one or more objects in the OPC client.

Figure 1-5

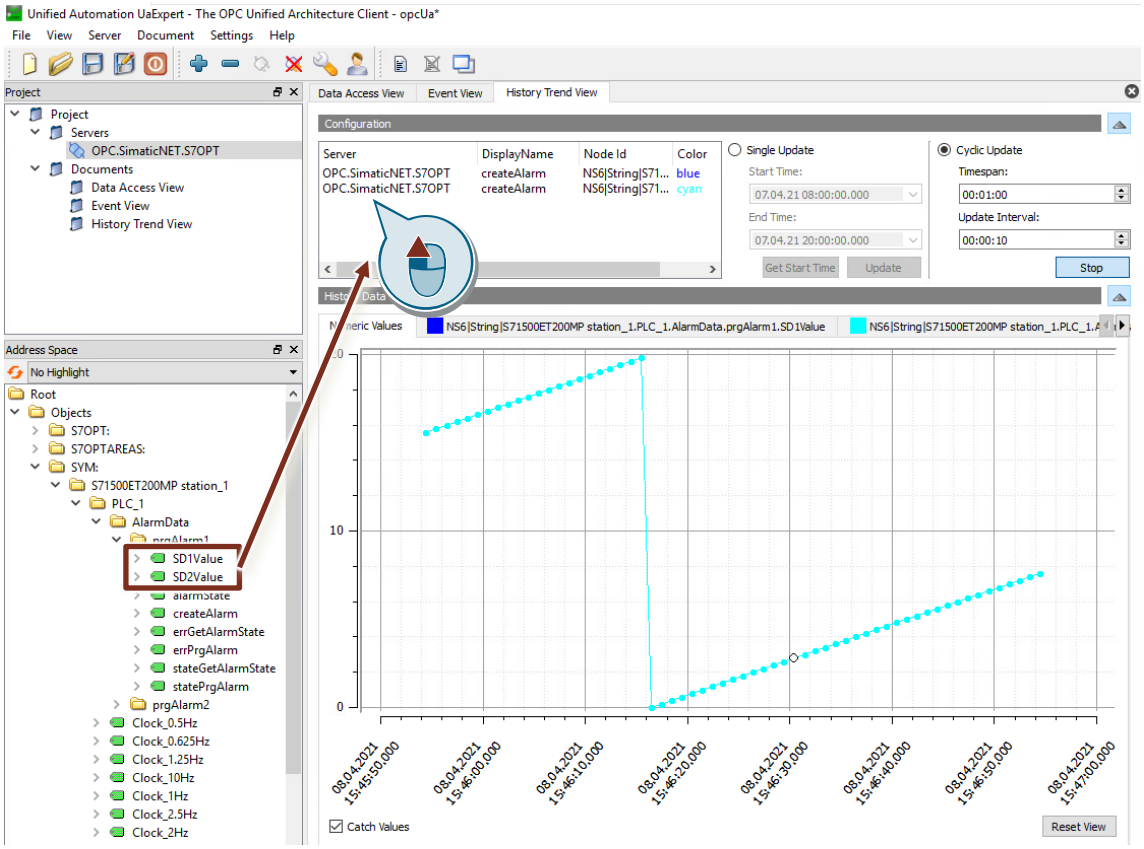


The S7OPT OPC UA server reads S7 tags from an S7-1500 CPU via an optimized S7 connection. The S7 tags are saved in the archive by the S7OPT OPC UA server. The timestamp and the quality characteristic of the S7 tags are stored together with the process value.

OPC clients, such as UA Expert from Unified Automation, use the "HistoryRead" function to access the process values of the archived S7 tags.

Display historical data in UA Expert

Figure 1-6



In this example, UA Expert is used as the OPC Client.

UA Expert has the "History Trend View" for getting historical data on one or more S7 tags.

Drag & drop one or more S7 tags containing historical data from the "Address Space" window into the "Configuration" section of the "History Trend View".

UA Expert has read access to the S7 tags stored in the archive of the S7OPT OPC UA server to graphically display the process values in the "History Trend View".

1.4 Components used

This application example was created with the following hardware and software components:

Table 1-1

Component	Quantity	Item number	Note
CPU 1513-1 PN	1	6ES7513-1AL01-0AB0	Alternatively, you may use any S7-1500 CPU and ET 200 CPU (ET 200SP and ET 200pro).
SIMATIC NET DVD V16	1	6GK1704-1LW16-0AA0	In the Sales and Delivery Release you will find the item numbers for the SIMATIC NET products (see article 109775589).
TIA Portal V16	1	Package: 6ES7822-1AA06-0YA5 Download: 6ES7822-1AE06-0YA5	–
UA Expert	1	–	OPC Client from Unified Automation https://www.unified-automation.com/products/development-tools/uaexpert.html

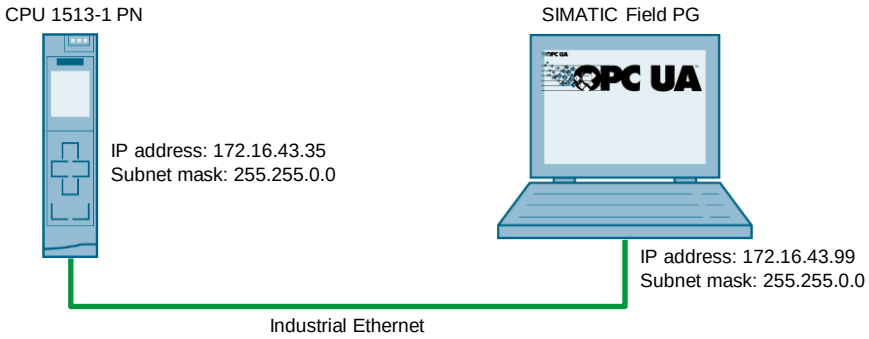
You can obtain the listed components from the Siemens Industry Mall.

2 Engineering

2.1 Hardware setup

The following figure shows the structure of the application example.

Figure 2-1



The SIMATIC NET OPC server for OPC UA and the OPC client are installed on the SIMATIC field PG that will be used as a PC station.

- SIMATIC NET OPC server for OPC UA: S7 OPT OPC UA Server
- OPC client: UA Expert

Note You will need an OPC client that supports OPC Alarms & Events and historical data about OPC UA.

Note

With this application you get a ready configured TIA Portal project.

The project is protected. The login is:

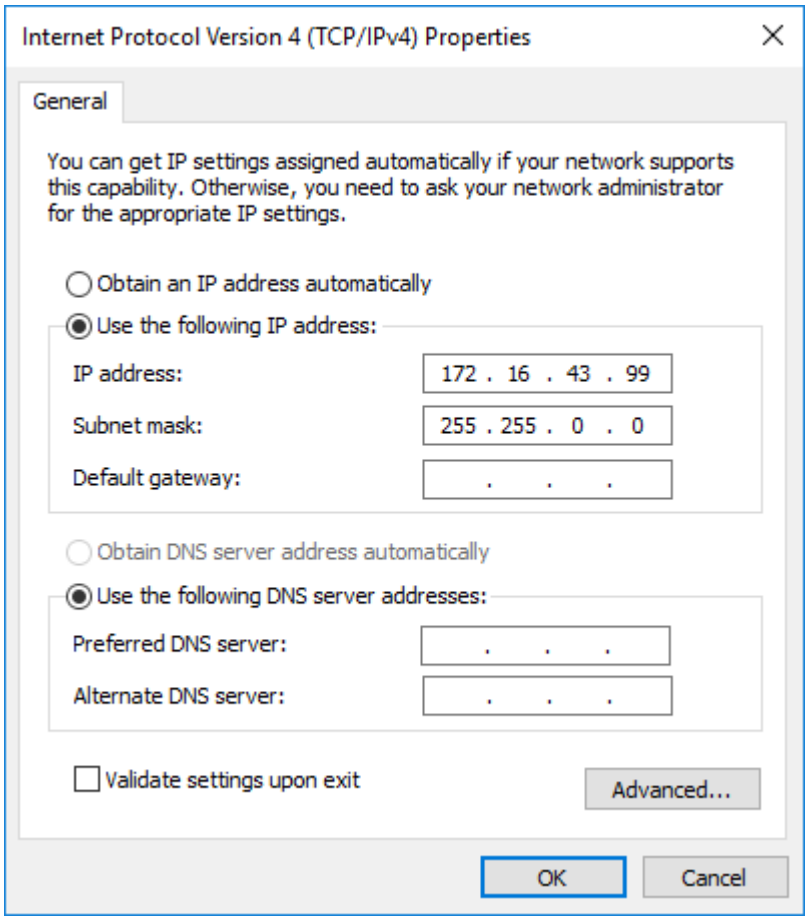
- User: admin
- Password: Siemens.1

2.2 Setting IP addresses and subnet mask

2.2.1 Setting IP address and subnet mask for the PC station

In Windows, go to the Properties for the network adapter via which the PC station is connected to the S7 CPU, then set the IP address and subnet mask for the PC station.

Figure 2-2



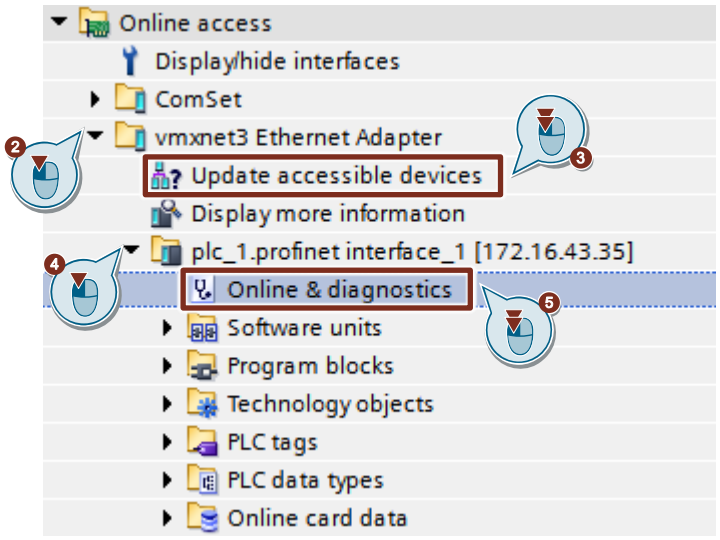
1. In the "Control Panel", open the "Network and Sharing Center" under "Network and Internet".
2. Select the function "Change adapter settings".
3. Right-click on the corresponding network adapter and select the "Properties" context menu. The Properties dialog for network adapter opens.
4. Select the "Internet Protocol Version 4 (TCP/IPv4)" element and click the "Properties" button.
   The Properties dialog box for the "Internet Protocol Version 4 (TCP/IPv4)" element will open.
5. Set the IP address and subnet mask of the PC station and apply the settings with "OK", e. g.:
   - IP address: 172.16.43.99
   - Subnet mask: 255.255.0.0

Note You will configure the fixed IP address and subnet mask later during hardware configuration for TIA Portal.

2.2.2 Setting the IP Address of the S7 CPU

Open the "Online & diagnostics" dialog

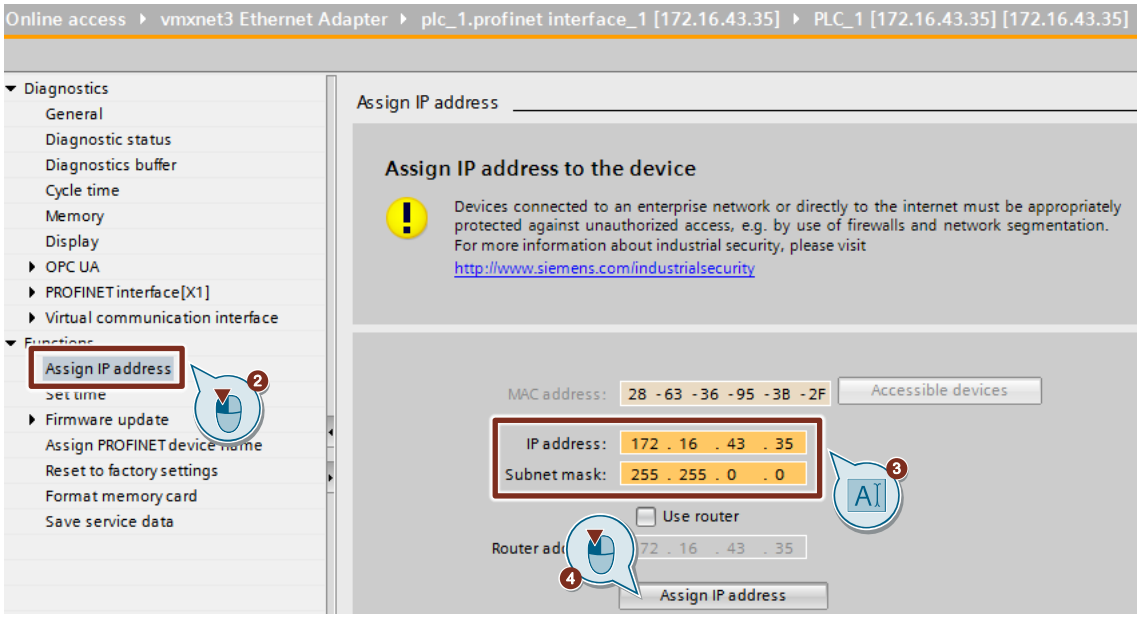
Figure 2-3



1. Open TIA Portal.
2. In the project tree under "Online access", click the arrow to the left of the network adapter that is connected to your S7 CPU.
3. Double-click the "Update accessible devices" command.
   All devices available to the network adapter will be shown.
4. Click the arrow to the left of the S7 CPU to which you wish to assign the IP address and subnet mask.
5. Double-click the command "Online & diagnostics".
   The "Online & diagnostics" dialog will open.

Assign IP address and subnet mask

Figure 2-4



1. Switch the S7 CPU to "STOP" mode.
2. Under "Functions", click "Assign IP address".
3. Set the IP address and subnet mask of the S7 CPU, e. g.:
   - IP address: 172.16.43.35
   - Subnet mask: 255.255.0.0
4. Click "Assign IP address" to set the parameters.

Note

You will enter the IP address and subnet mask later during configuration.

If you have an S7-1500 CPU, you can also set the IP address and subnet mask on the display.

2.3 "Communication settings"

Open the program "Communication Settings" via the Windows Start Menu "Siemens Automation > Communication Settings".

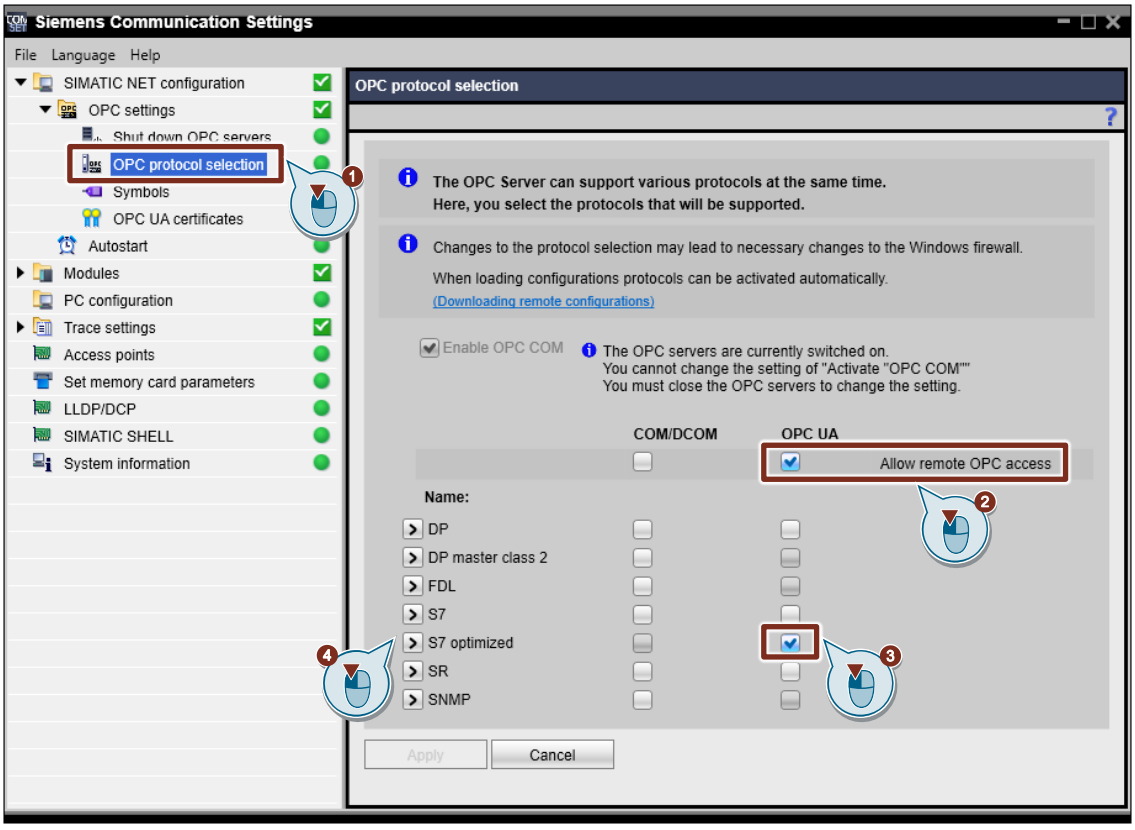
The "Communication Settings" program provides a number of ways to configure and diagnose PC hardware components, PC user programs and the SIMATIC NET OPC server.

Enable protocols for the OPC server

The SIMATIC NET OPC server supports various protocols for the controller level. All protocols are activated in the initial configuration.

You can disable protocols that you don't want to use.

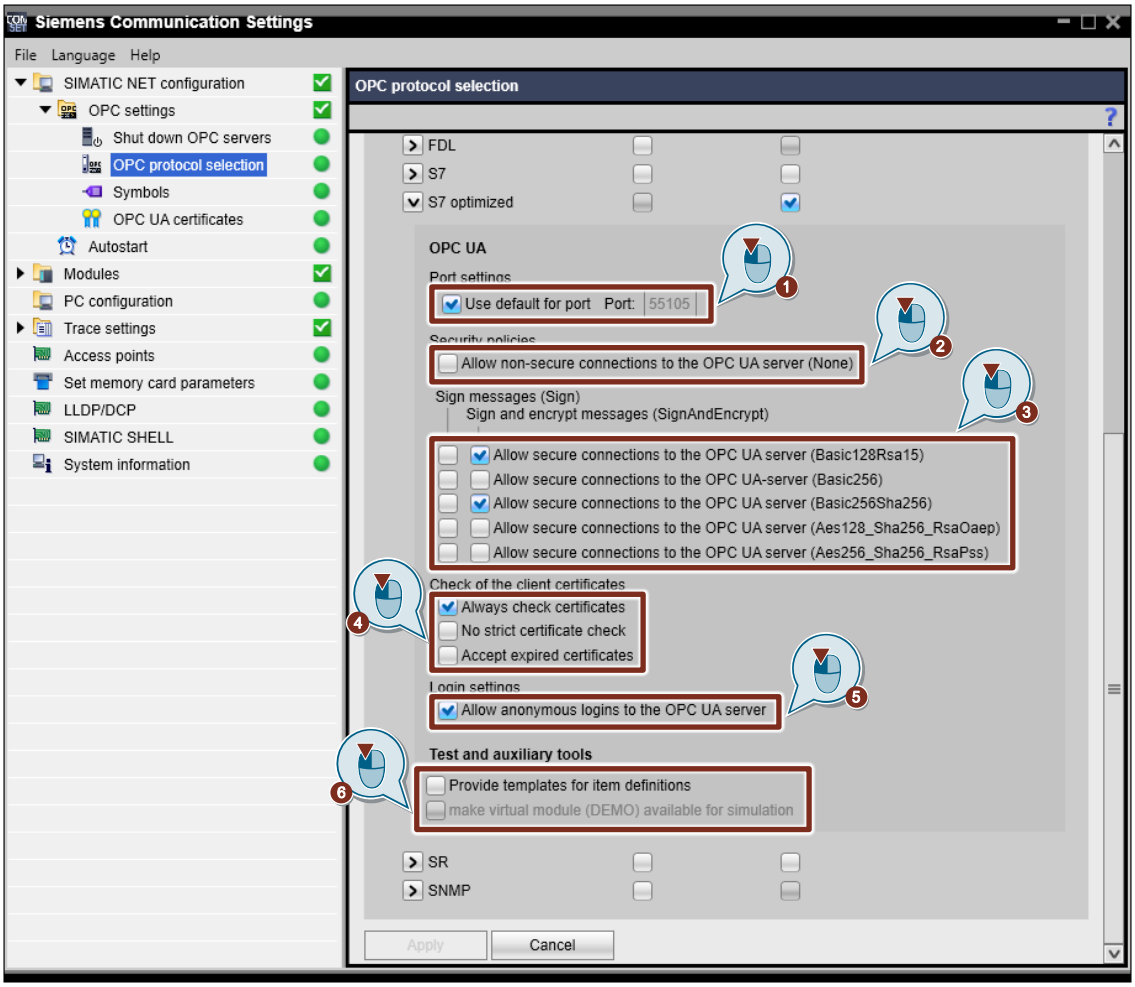
Figure 2-5



1. In the navigation area, navigate to "SIMATIC NET configuration > OPC Settings > OPC protocol selection".
2. Enable the function "Allow remote OPC access" for OPC UA.
3. Enable the following protocol for OPC UA:
   - "S7 optimized": SIMATIC S7 communication with S7-1200 (V4 onward) and S7-1500 via Industrial Ethernet (access to optimized data blocks)
4. Click on the arrow symbol next to the protocol "S7 optimized" to access the extended parameter list for the protocol.

Set parameters for the protocols

Figure 2-6



1. Port settings:
   - If the checkbox is selected, the default setting is used for the specified port.
   - If the checkbox is not selected, you can edit the input field for the port.
2. Security policies:
   - If the checkbox is selected, unsecured connections (none) to the OPC server are allowed.
   - If the checkbox is not selected, no unsecured connections (none) to the OPC server will be allowed.
3. Define which connections to the OPC server will be allowed and determine whether the messages will be signed (Sign) or signed and encrypted (SignAndEncrypted):
   - Secured connections based on the security policy "Basic128Rsa15"
   - Secured connections based on the security policy "Basic256"
   - Secured connections based on the security policy "Basic256Sha256"
   - Secured connections based on the security policy "Aes128_Sha256_RsaOaep"
   - Secured connections based on the security policy "Aes256_Sha256_RsaPss"

4. Check of the client certificates
   - Always check certificates
     Enabled: The certificates will always be checked.
     Disabled: The certificates will not be checked.
   - No strict certificate verification
     Enabled: Certain certificate checks will be ignored, e. g. CertificateRevocationUnknown, CertificateIssuerRevocationUnknown, NonceLengthCheck, TokenPolicyIdCheck.
     Disabled: The certificates will be fully checked.
   - Accept expired certificates
     Enabled: The certificates will be accepted even if the time stamp of the certificate is invalid, i. e. the certificates are not yet valid or have already expired.
     Disabled: The certificates are only accepted if the timestamp is valid.
5. Login settings
   - If the checkbox is selected, the SIMATIC NET OPC server allows anonymous login of OPC UA clients.
   - If the checkbox is not selected, anonymous logins are not allowed. User authentication with Windows login and password is then required.

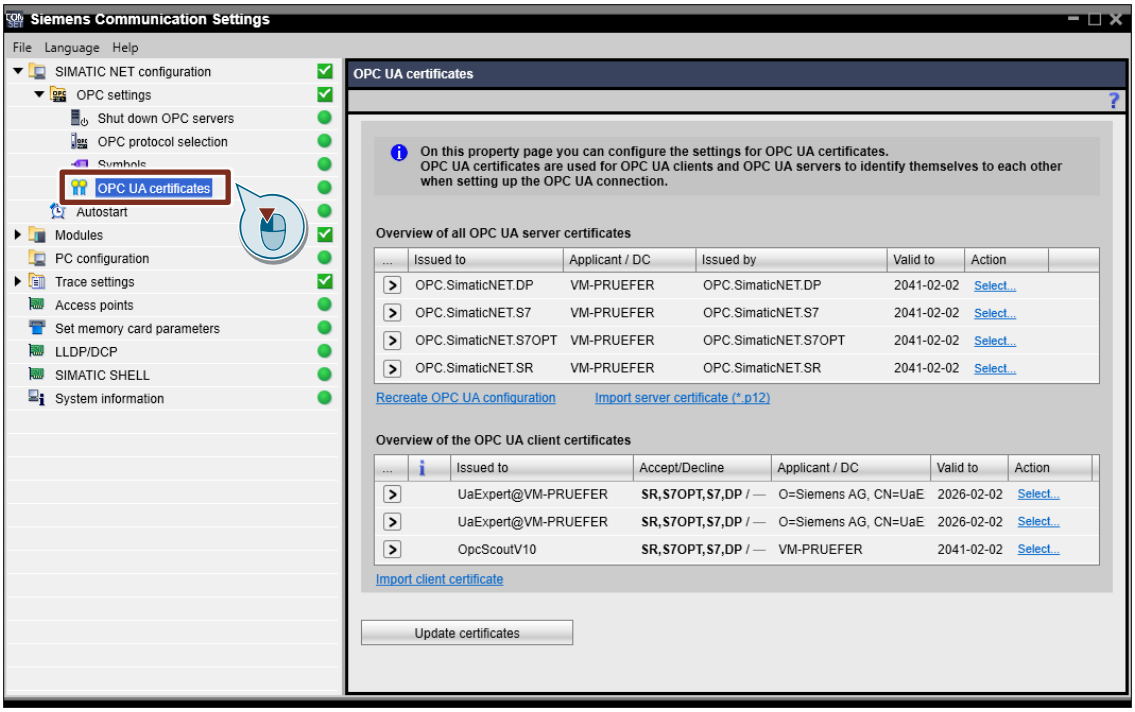
Note

The SIMATIC NET OPC server uses the Windows user management for user authentication. In the OPC client, log in to the SIMATIC NET OPC server with your Windows username and password.

6. Test and auxiliary tools
   - Provide templates for item definitions:
     If the checkbox is selected, the OPC server creates Templates for item definitions in its namespace, which can be used to easily define a new Item.
   - make virtual module (Demo) available for simulation:
     The SIMATIC NET OPC server gives you the ability to use the OPC interface for tests, presentations, and development work without a communication module. For this purpose, the OPC server provides a virtual module or "DEMO" connection, depending on the protocol (CP simulation). This option enables activation of the simulation function depending on the protocol.
7. Click "Apply" to enable the settings you have made.

"OPC UA certificates"

Figure 2-7



1. In the navigation area, navigate to "SIMATIC NET configuration > OPC settings > OPC UA certificates".
   The certificates of the local OPC UA server and the certificates the OPC clients used to identify themselves to the server are displayed and managed here.
2. You can import other OPC client certificates, such as the certificate for the OPC client "UA Expert".
3. Accept the imported OPC client certificates.

2.4 Overview of the engineering steps

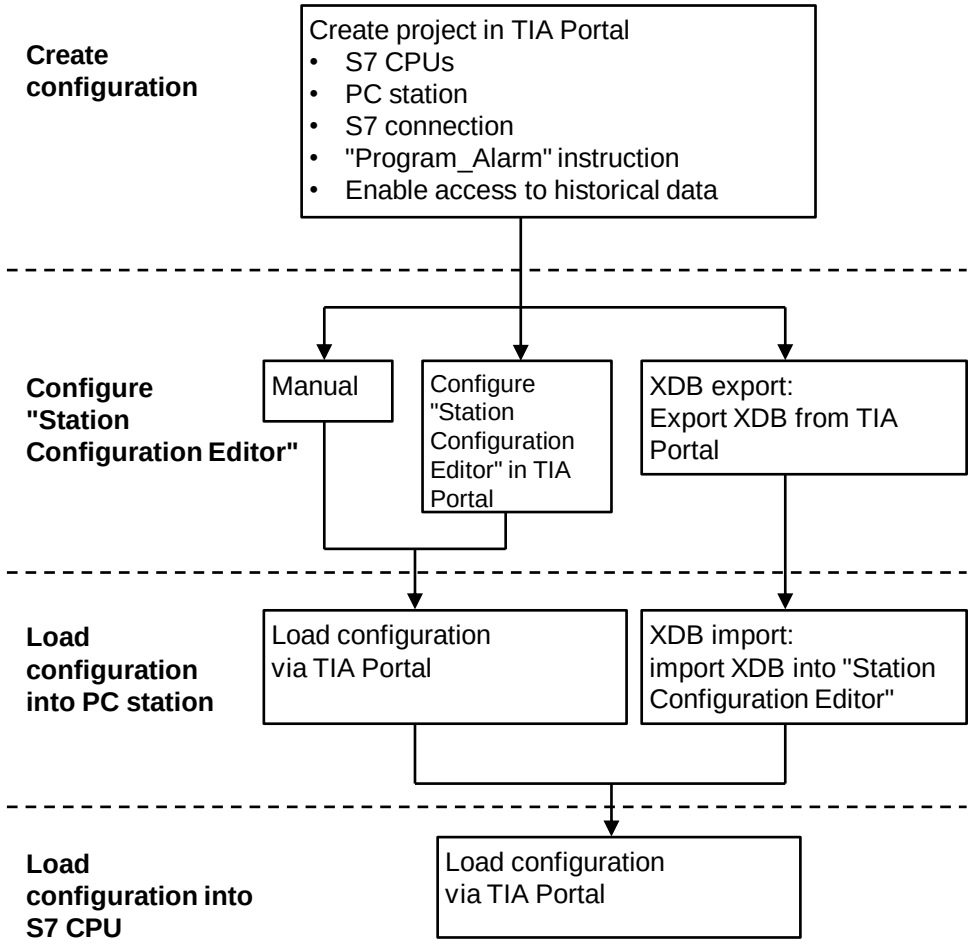
The following figure shows an overview of the steps performed during the engineering stage.

- Create configuration (see chapter 2.5)
- Configure the "Station Configuration Editor" (see chapter 2.6)
- Load the configuration into the PC station (see chapter 2.7.1)
- Load the configuration into the S7 CPU (see chapter 2.7.1)

When configuring the "Station Configuration Editor" and when loading the configuration into the PC station, there are multiple ways of performing the engineering step. Performing either one of the options for the engineering step is sufficient.

This application example describes all possibilities for the engineering steps.

Figure 2-8



2.5 Creating the configuration

2.5.1 Create S7 CPU in TIA Portal

Note

With this application you get a ready configured TIA Portal project.

The project is protected. The login is:

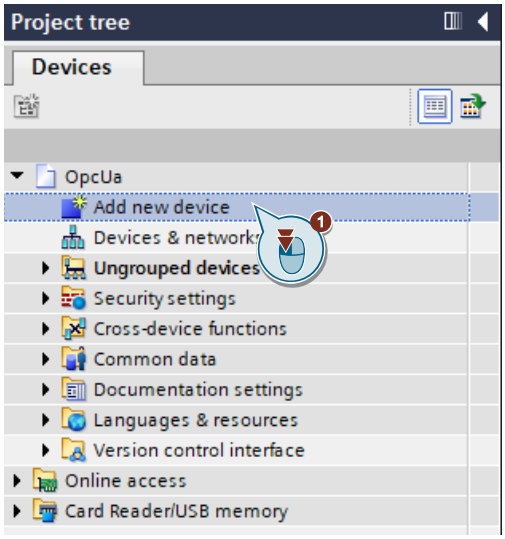
- User: admin
- Password: Siemens.1

Requirements

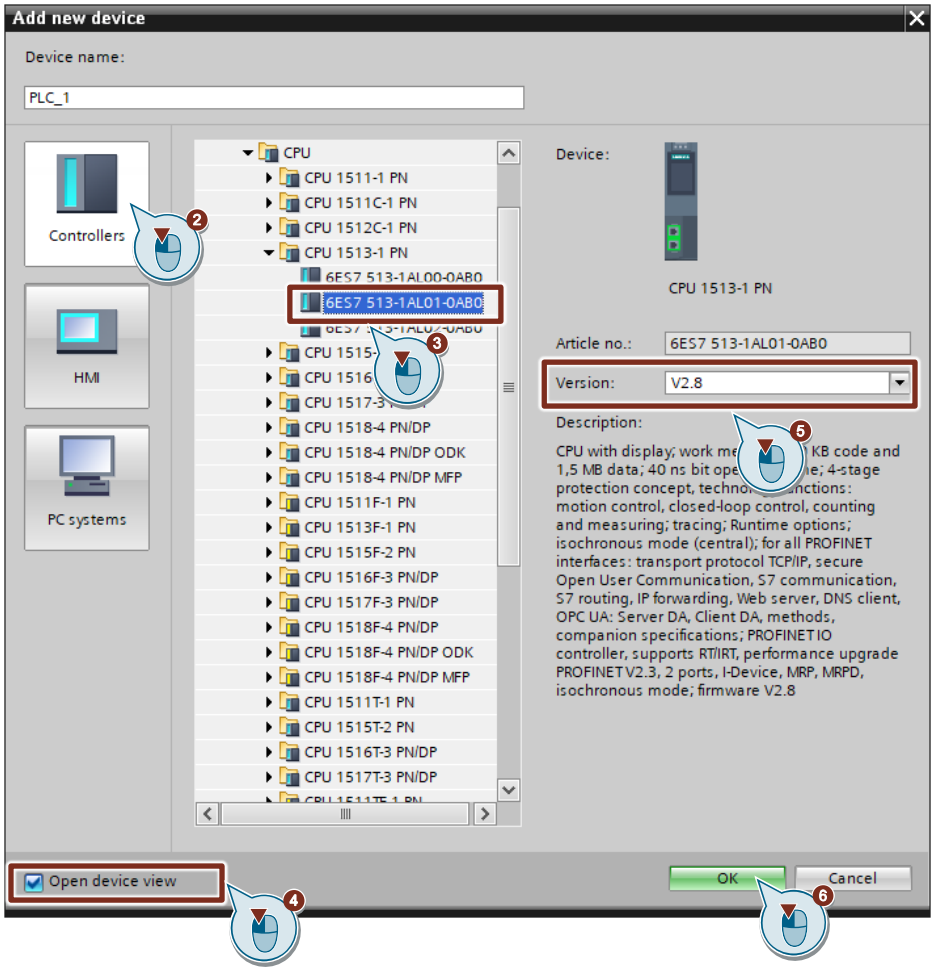
- TIA Portal is open.
- A new project is created, or an existing project is opened.

Insert device

1. Double-click the command "Add new device" in the project tree.



The dialog box "Add new device" opens.



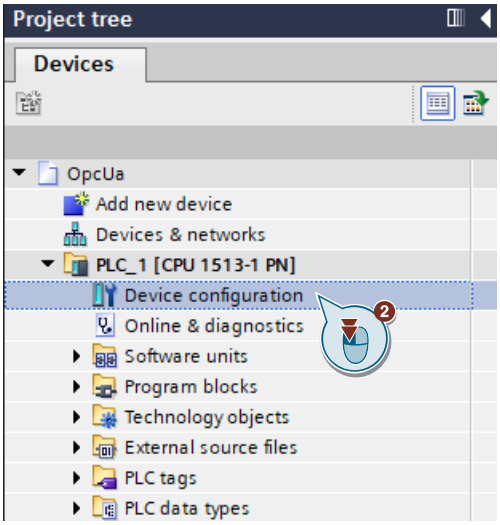
2. Click the "Controllers" button.
3. Select the S7 CPU according to your hardware setup, e. g. CPU 1513-1 PN.
4. Enable the option "Open device view".
5. Under "Version", select the firmware version of the S7 CPU.
6. Click the "OK" button.

The selected S7 CPU will be added.

Note If you enabled the option "Open device view", the "Device view" for the S7 CPU will open automatically in the hardware and network editor.

Open the device view

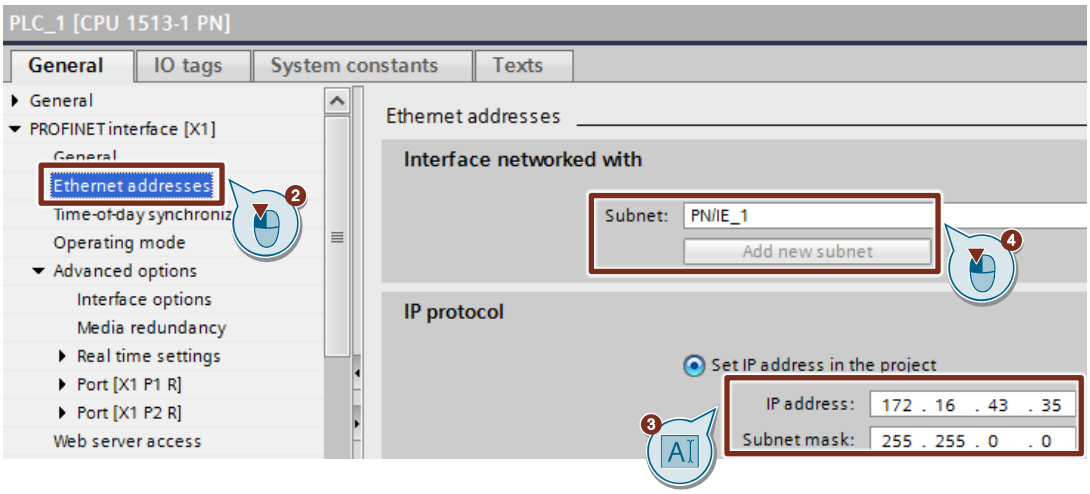
1. In the project tree, open the device folder of the S7 CPU.
2. Double-click the "Device configuration" command.



The "Device view" of the S7 CPU opens in the hardware and network editor.

Set address parameters

1. Select the S7 CPU in the device view.
   The properties of the S7 CPU are displayed in the Inspector window.

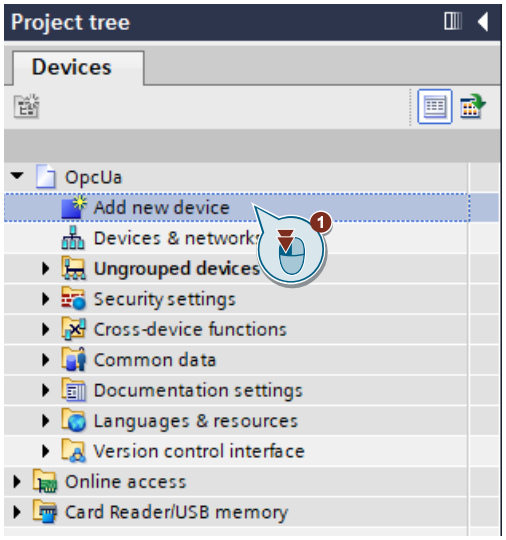


2. In the "General" tab, navigate to "PROFINET interface [X1] > Ethernet addresses".
3. Enter the following address parameters:
   - IP address: 172.16.43.35
   - Subnet mask: 255.255.0.0
4. Click on the "Add new subnet" button to create a new subnet or select an existing subnet.

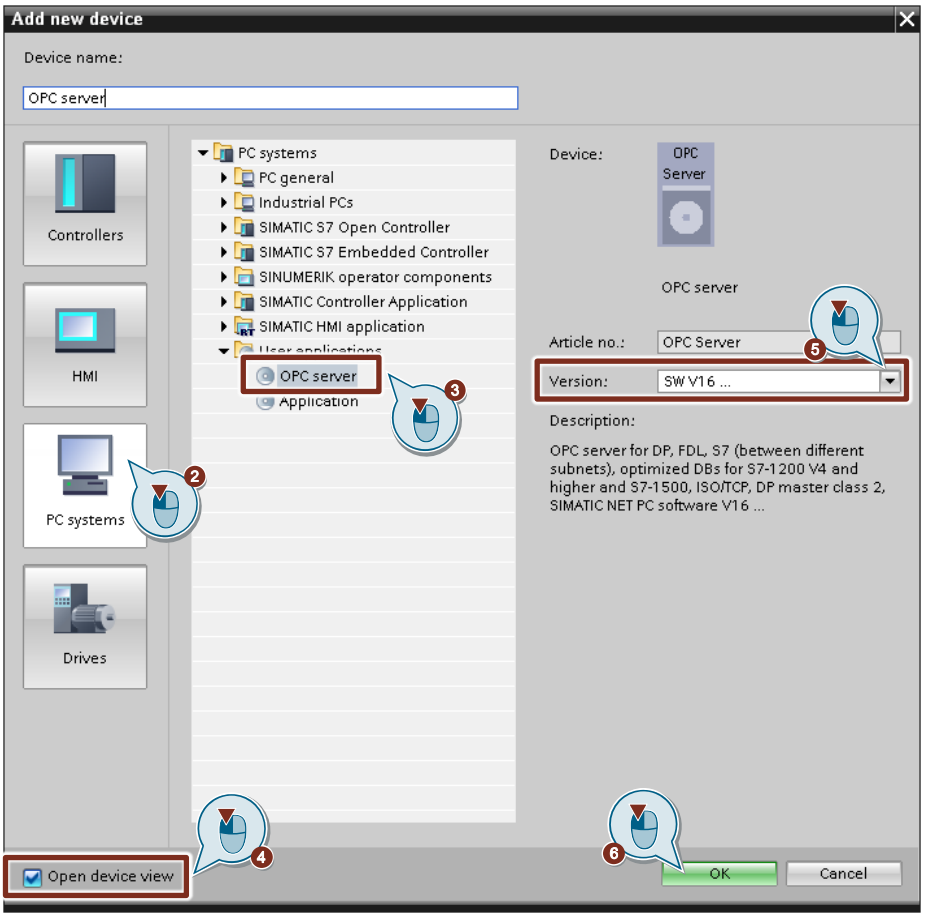
2.5.2 Create PC station in TIA Portal

Adding a PC station

1. Double-click the command "Add new device" in the project tree.



The dialog box "Add new device" opens.



2. Click the "PC systems" button.
3. Select the user application "OPC server".
4. Enable the option "Open device view".
5. Set the version of the "OPC server" user application, e. g. "SWV16...".
6. Click the "OK" button.

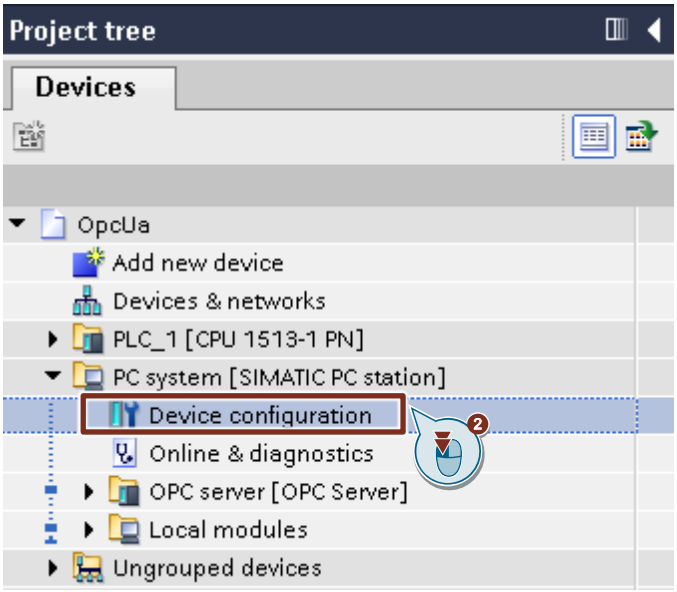
A PC station with the user application "OPC server" will be added.

Note If you enabled the option "Open device view", the "Device view" for the PC station will open automatically in the hardware and network editor.

Open the device view

1. In the project tree, open the device folder of the PC station.
2. Double-click the "Device configuration" command.

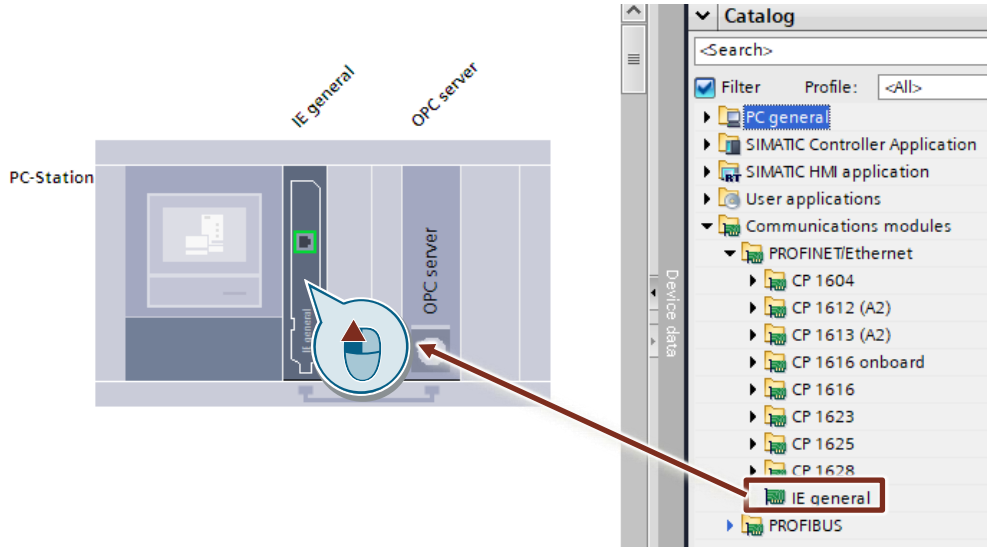
The "Device view" of the PC station opens in the hardware and network editor.



Configure PC station in the "Device view"

The "OPC server" user application has been automatically added to the slot.

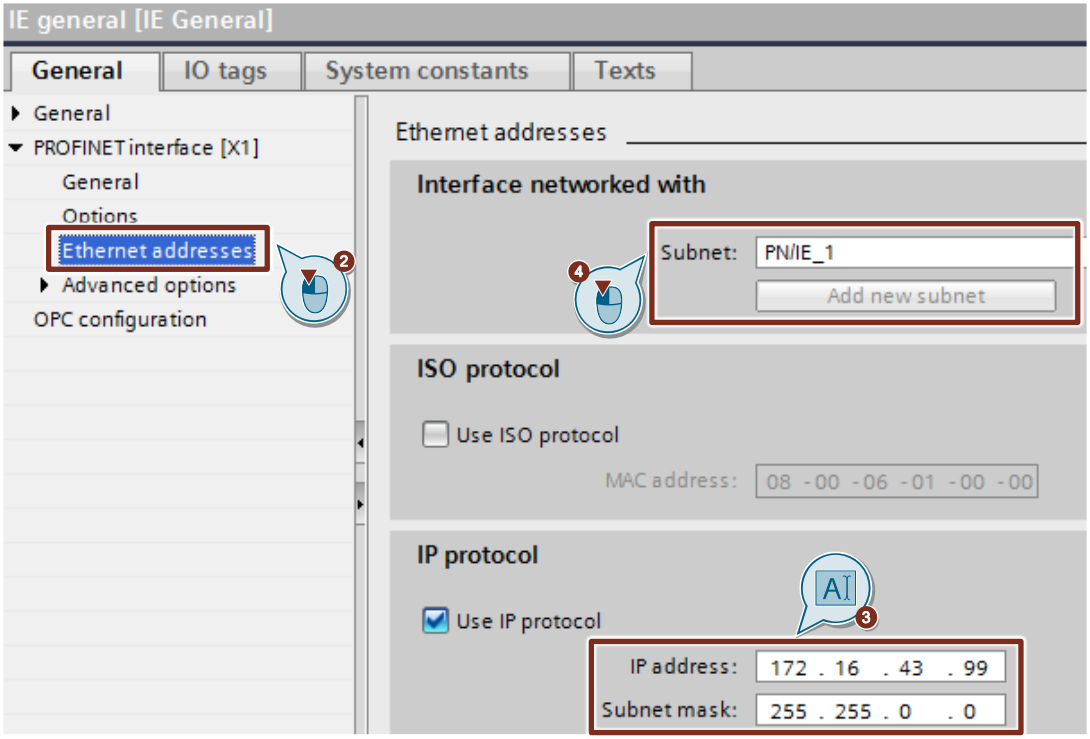
Figure 2-9



1. Insert a communications module, e. g. "IE general", into slot 2 of the PC station by dragging and dropping.

Set address parameters

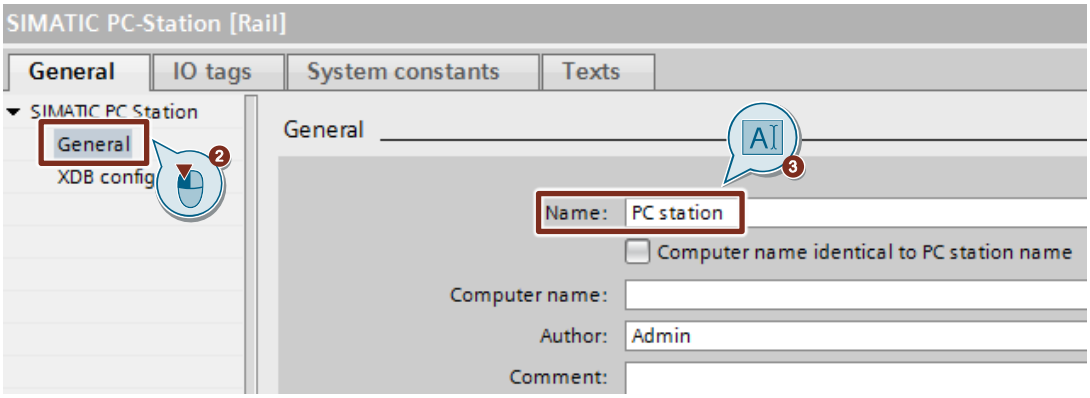
1. In the device view, select the communications module "IE general".
   The properties of the communications module are displayed in the Inspector window.



2. In the "General" tab, navigate to "PROFINET interface [X1] > Ethernet addresses".
3. Enter the following address parameters:
   - IP address: 172.16.99
   - Subnet mask: 255.255.0.0
4. Click on the "Add new subnet" button to create a new subnet or select an existing subnet.

Set the name of the PC station

1. Select the PC station in the device view.
   The properties of the PC Station are displayed in the Inspector window.



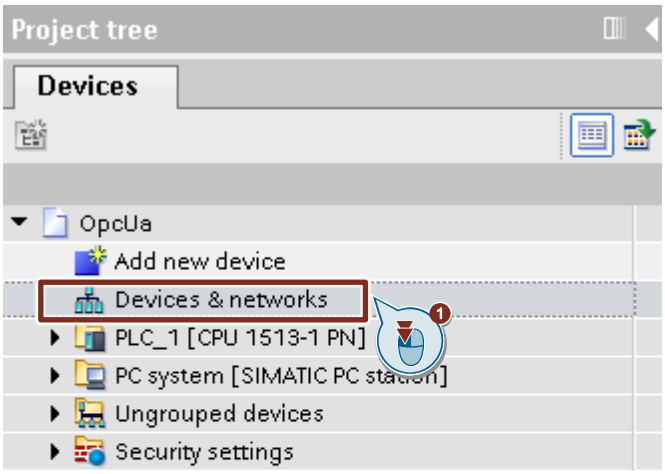
2. In the "General" tab, navigate to "General".
3. Enter the name of the PC station, e. g. "PC station".

2.5.3 Configuring a connection

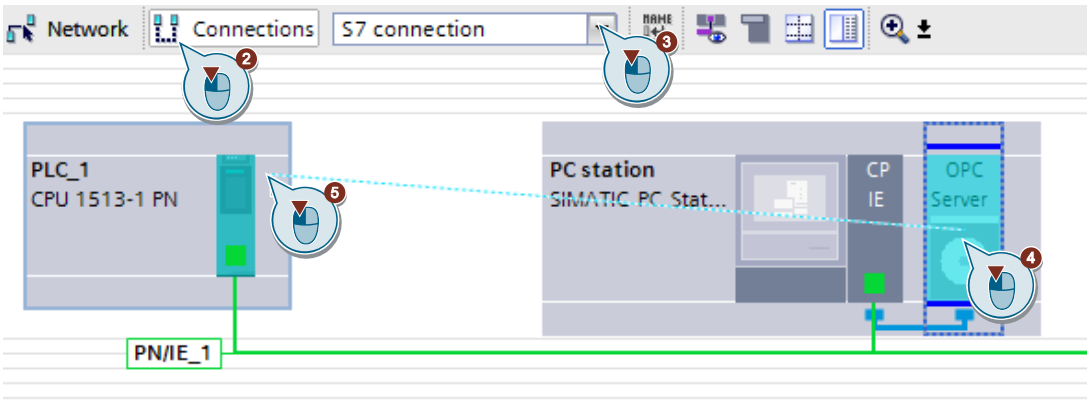
S7 CPU and PC station are created in the same project

Add S7 connection

1. Double-click "Devices & networks" in the project tree.



The graphical area of the "Network view" opens in the hardware and network editor.

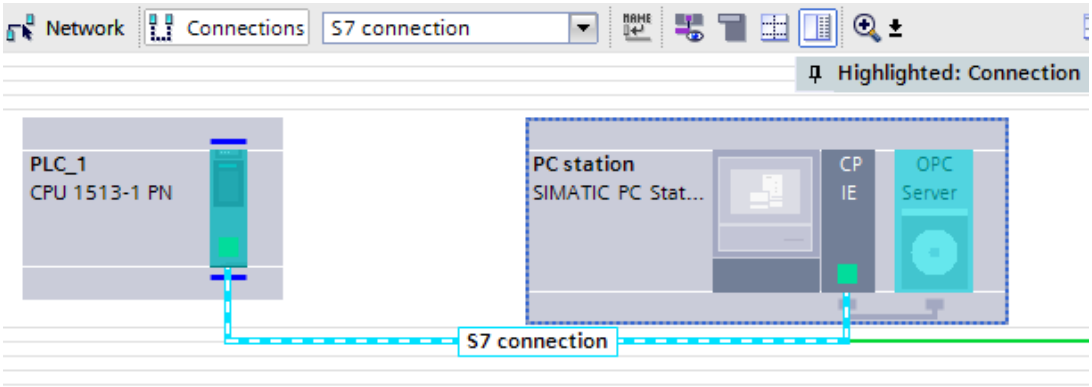


2. In the function bar, click "Connections" to enable the connection mode.
3. Select the connection type "S7 connection" in the nearby dropdown menu.
   All devices that are relevant to an S7 connection are highlighted in color in the "Network view".
4. Click and drag the mouse from the OPC server to the S7 CPU.
5. Release the mouse button on the target device to create the S7 connection between the OPC server and the S7 CPU.

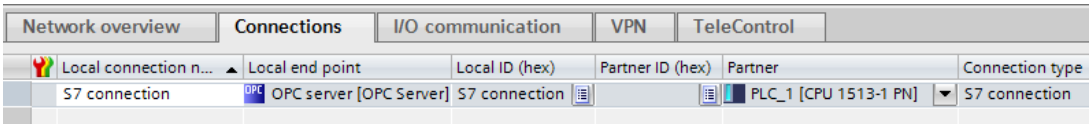
Result:

A specified S7 connection is created and is configured on both sides.

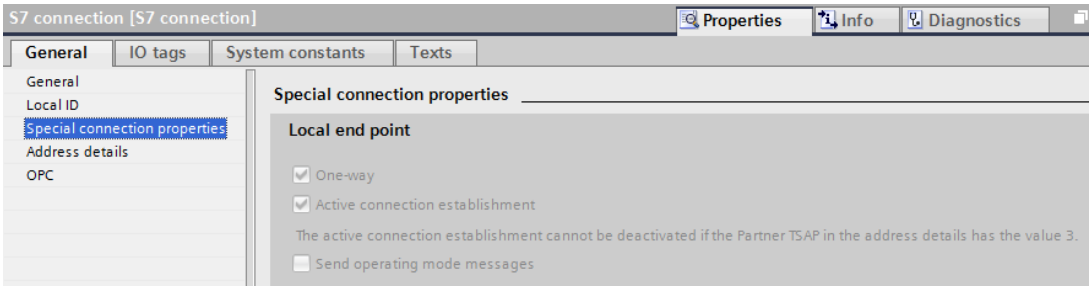
- The connection path is highlighted.



- The S7 connection is entered in the connection table.

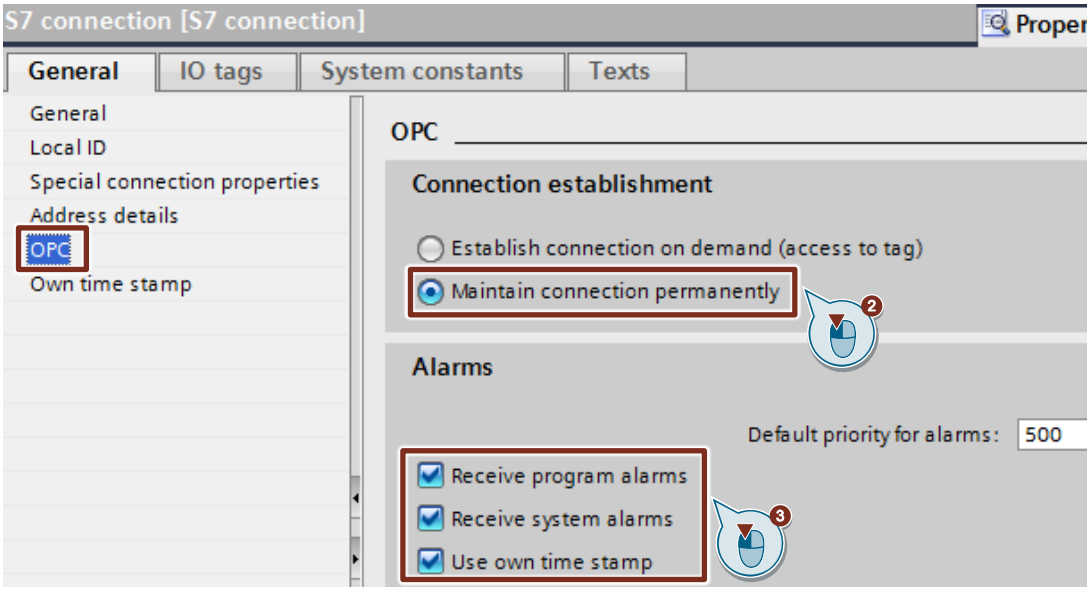


- The OPC server actively establishes the S7 connection. The S7 CPU is a passive participant as the connection is established.



Set connection parameters

1. Select the S7 connection in the connection table.
   The properties of the S7 connection are displayed in the Inspector window.

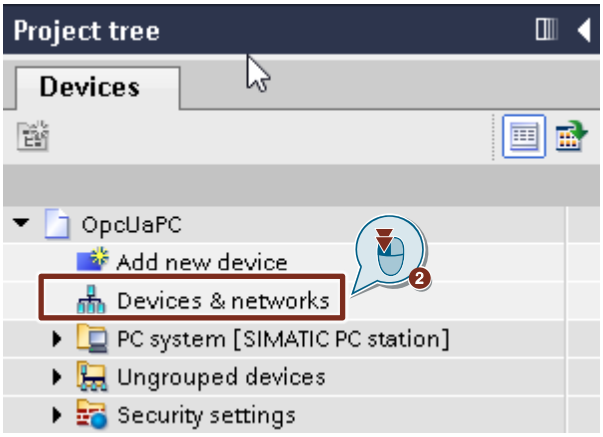


2. In the "General" tab under "OPC", enable the function "Maintain connection permanently".
3. Enable the following functions for alarms:
   - "Receive program alarms"
   - "Receive system alarms"
   - "Use own time stamp"

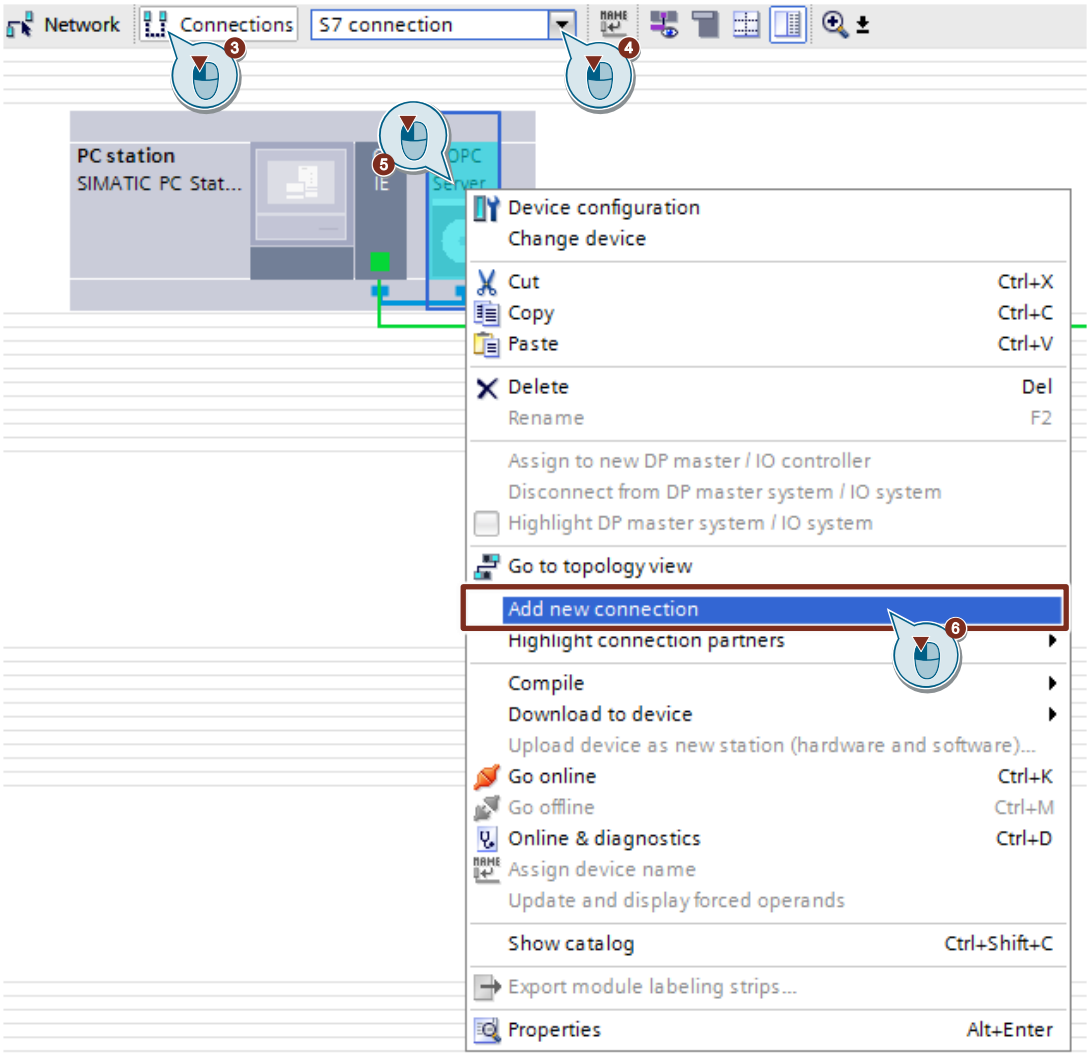
S7 CPU and PC station are created in different projects

Add an unspecified S7 connection

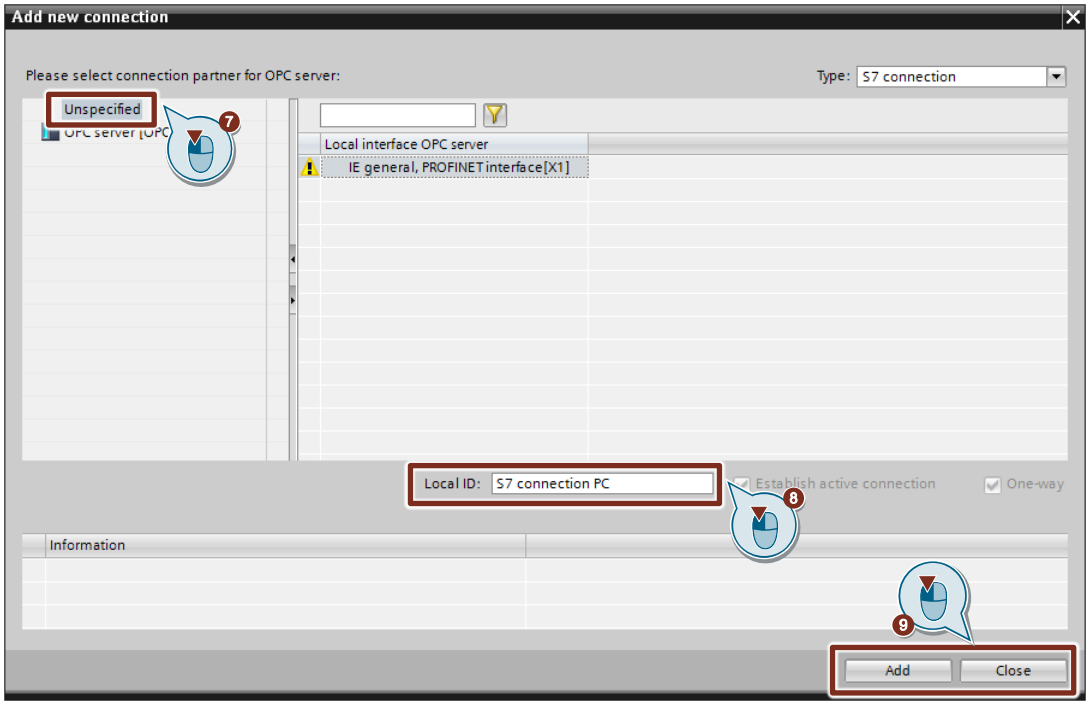
1. Open the project tree in the PC station's project.
2. Double-click "Devices & networks".



The graphical area of the "Network view" opens in the hardware and network editor.



3. In the function bar, click "Connections" to enable the connection mode.
4. Select the connection type "S7 connection" in the nearby dropdown menu.
   The OPC server that is relevant for an S7 connection will be highlighted in color in the "Network view".
5. Right click on the OPC server.
   The context menu opens.
6. Select "Add new connection".
   The "Add new connection" dialog will open.

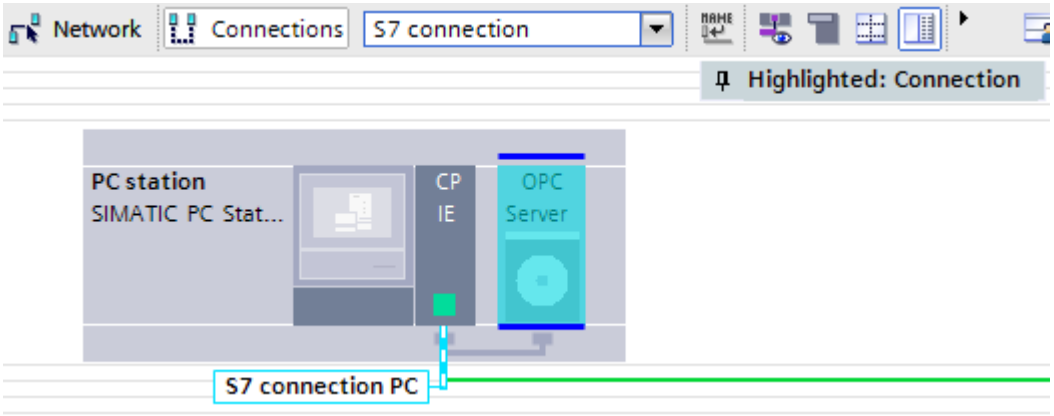


7. Specify the following connection parameters: "Unspecified".
8. Enter the local ID, e. g. "S7 connection PC".
   The local ID is visible in the OPC client if the OPC client has established the connection to the SIMATIC NET S7OPT OPC UA server.
9. Click "Add" to add the unspecified S7 connection; click the "Close" button to close the dialog.

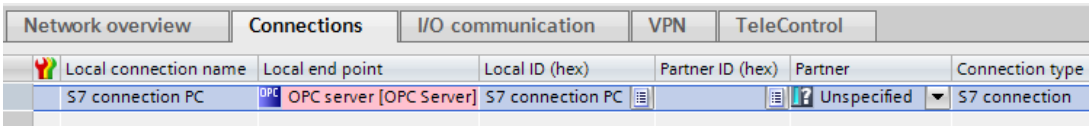
Result:

An unspecified S7 connection is created.

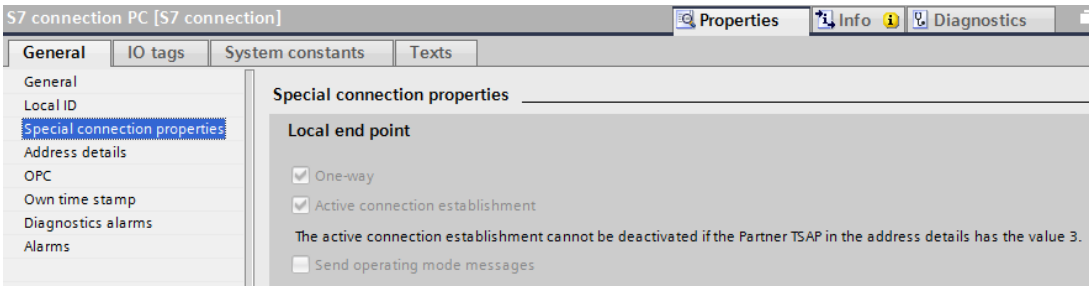
- The connection path is highlighted.



- The S7 connection is entered in the connection table.



- The OPC server actively establishes the S7 connection.

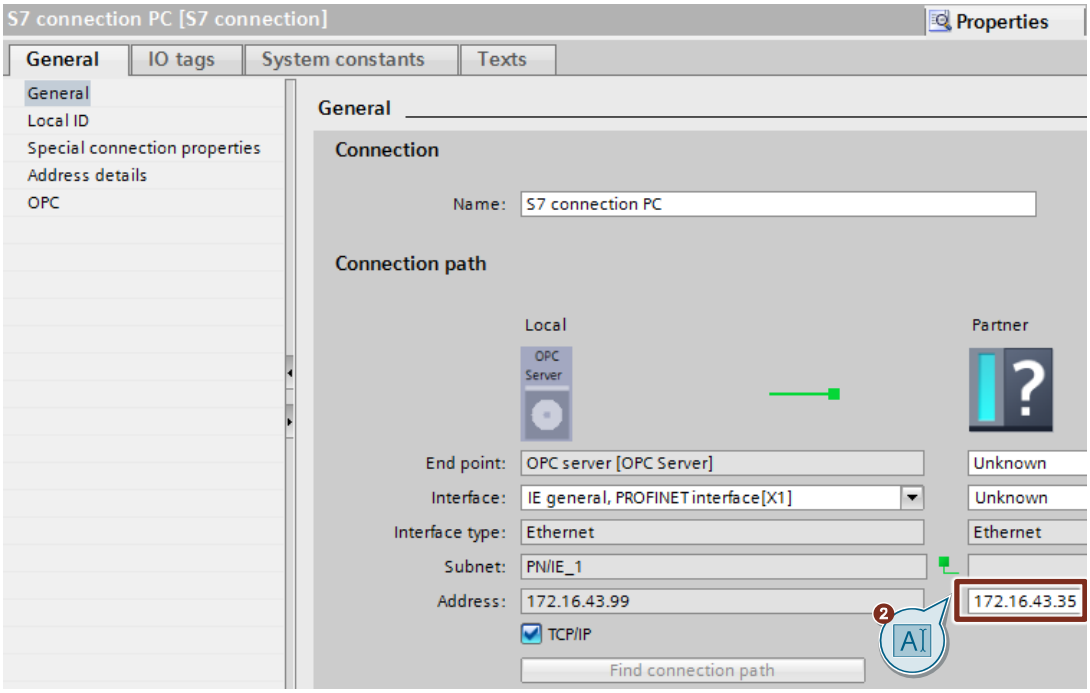


Note

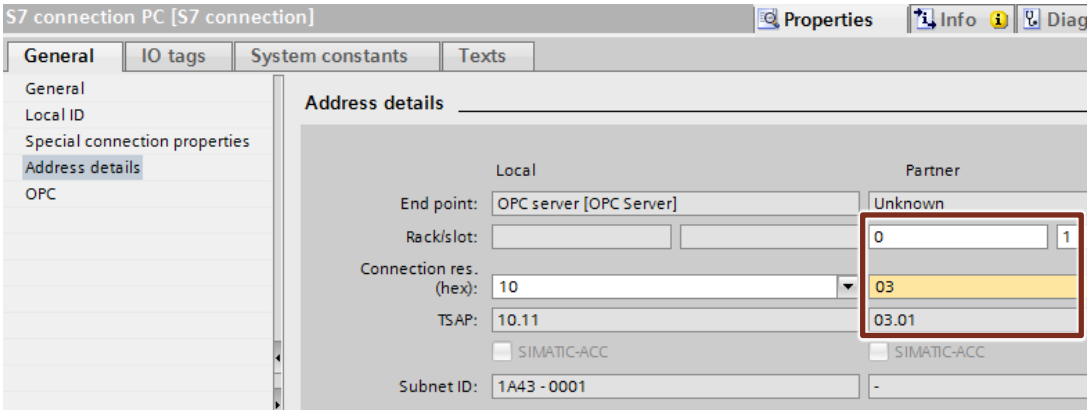
If the connection parameters are not yet fully set up, the S7 connection will be shown with errors in the connection table.

Set connection parameters

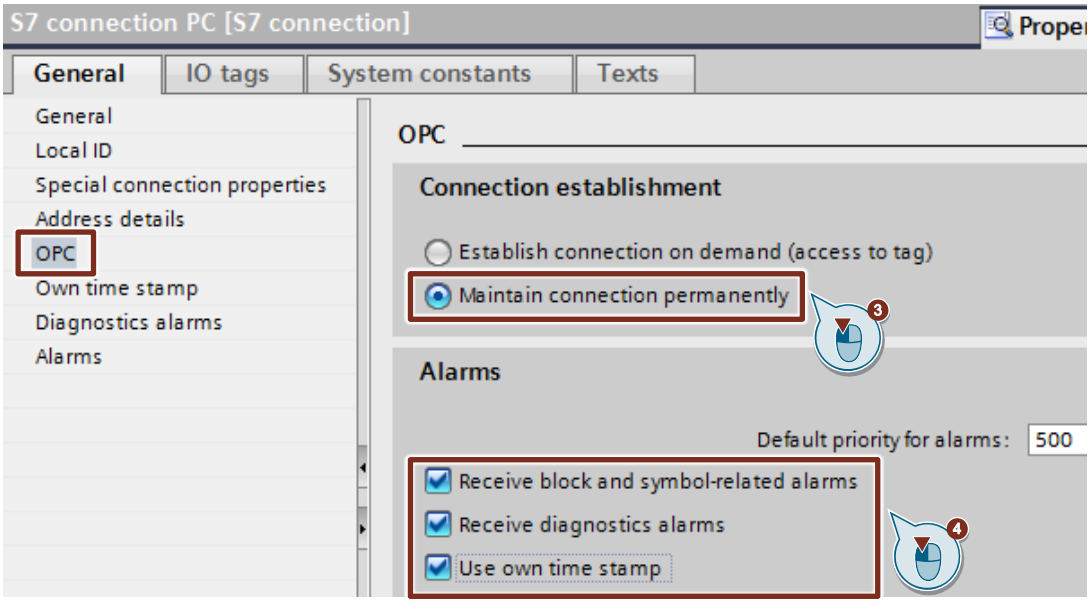
1. Select the S7 connection in the connection table.
   The properties of the S7 connection are displayed in the Inspector window.
2. Enter the IP address of the communication partner in the "General" tab under "General", e. g. 172.16.43.35 (IP address of the S7-1500 CPU).



3. In the "General" tab under "Address details", enter the partner TSAP. The partner TSAP is composed as follows: 03. <slot of the CPU>, e. g. S7-1500 at port 1: 03.01



4. In the "General" tab under "OPC", enable the function "Maintain connection permanently".
5. Enable the following functions for alarms:
   - "Receive block and symbol-related alarms"
   - "Receive diagnostics alarms"
   - "Use own time stamp"



2.5.4 User program of the S7-1500 CPU

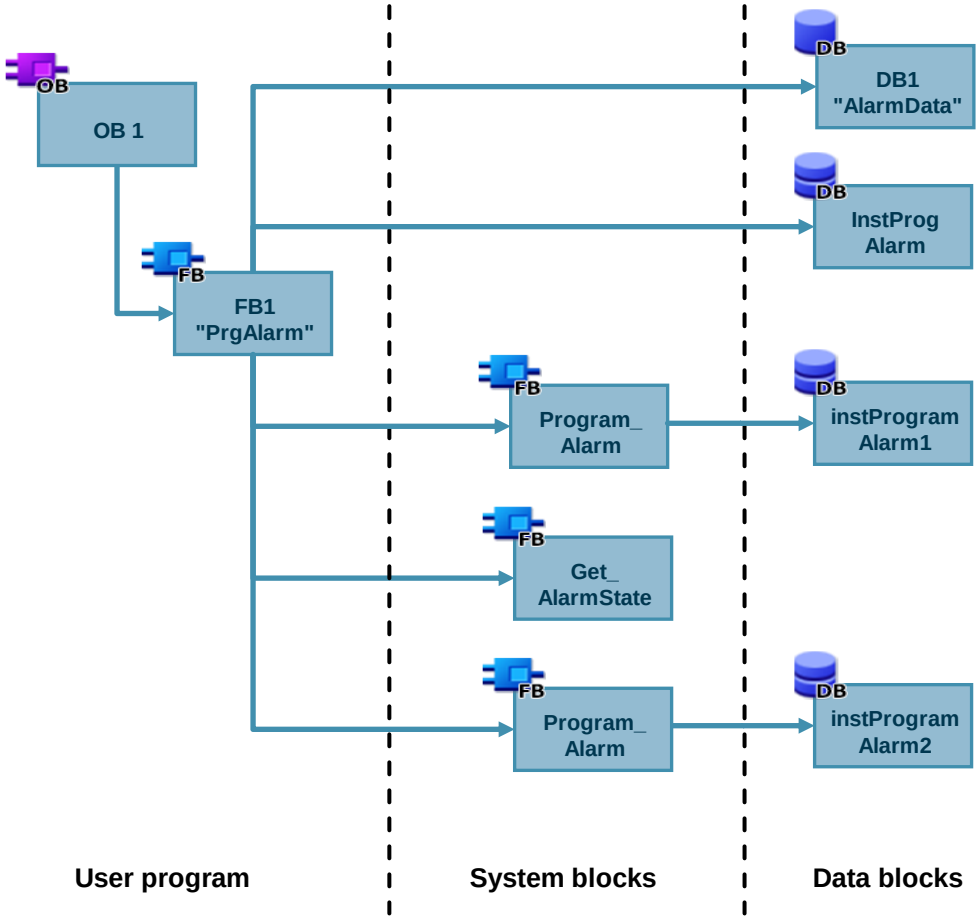
To generate a program alarm, it is necessary to call the "Program_Alarm" instruction in the user program of the S7-1500 CPU. The "Get_AlarmState" instruction is used to output the alarm state of a program alarm. There are 3 options:

- Incoming
- Outgoing
- Acknowledged

The following figure shows an overview of the user program in the S7-1500 CPU that is required to generate 2 program alarms:

- Program alarm with required acknowledgement and 2 associated values
- Program alarm for information purposes only

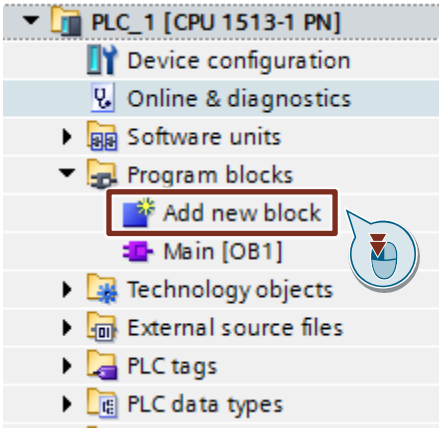
Figure 2-10



FB "PrgAlarm" for calling the alarm blocks

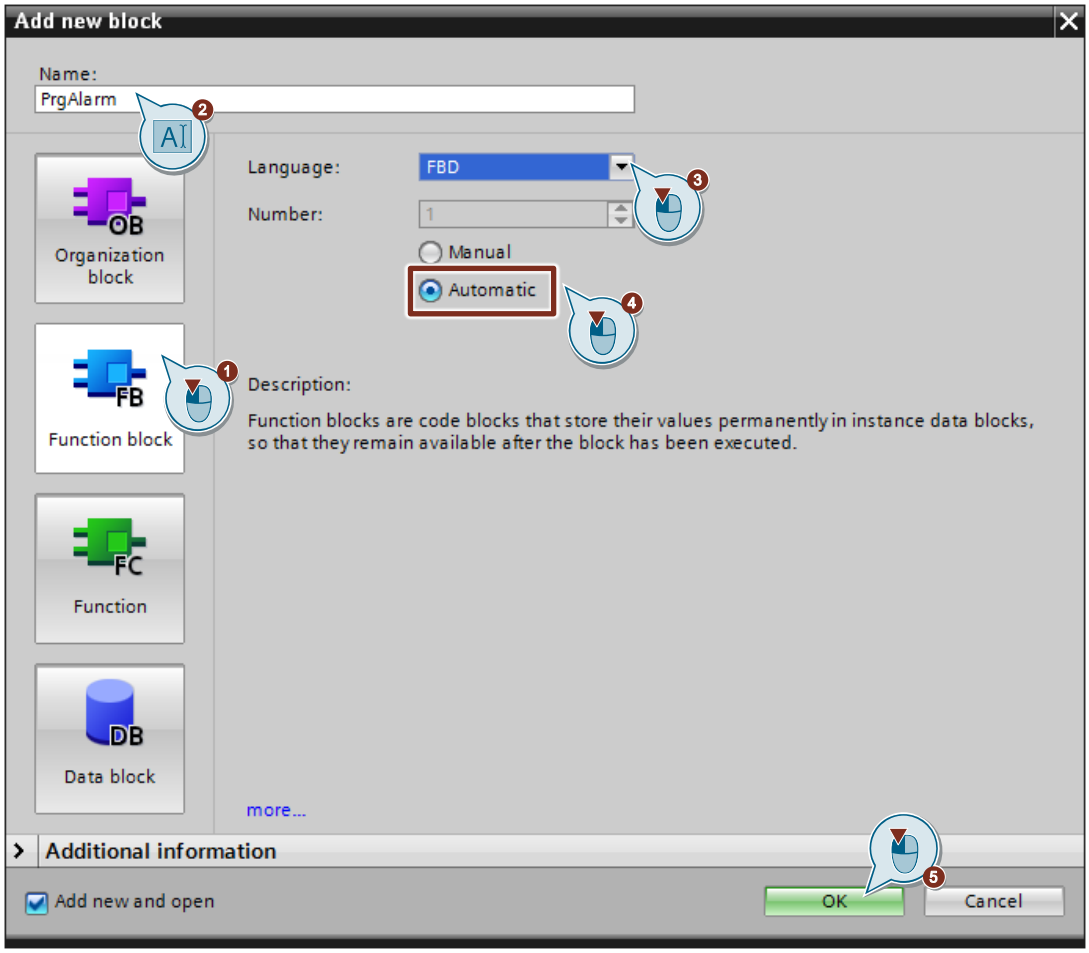
Insert a function block (FB) to call the "Program_Alarm" and "Get_AlarmState" instructions.

1. In the project tree, navigate to the device folder of the S7-1500 CPU.
2. Open the "Program blocks" folder.
3. Double-click the "Add new block" command.



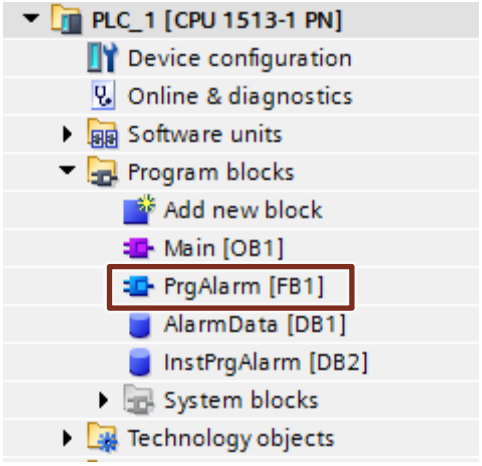
The dialog "Add new block" opens.

4. Make the following settings:



- Click on the "Function block" button.
- Enter the name of the FB, e. g. "PrgAlarm".
- Select the programming language, e. g. "FBD".
- Select the "Automatic" radio button for automatic number assignment. The number of the FB will be assigned by TIA Portal.
- Click "OK" to confirm the settings.

The inserted FB “PrgAlarm" is displayed in the project tree.



Create PLC data type "typePrgAlarmVar"

Create a PLC data type, e. g. "typePrgAlarmVar", to define the parameters of the FB "PrgAlarm" and populate it with tags.

The following table shows the structure of the PLC data type "typePrgAlarmVar".

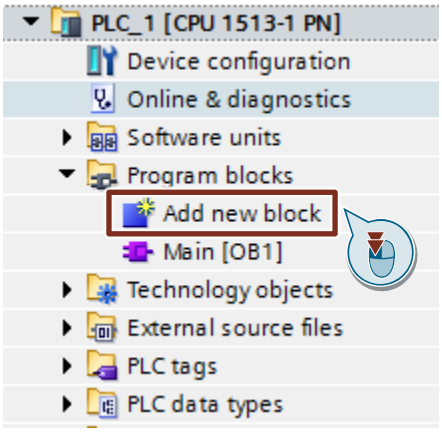
Table 2-1

Tag	Data type	Description
createAlarm	Bool	The signal to be monitored. • Positive signal edge: An incoming program alarm is generated • Negative signal edge: An outgoing program alarm is generated
SD1Value	String	Associated value 1, for example a character string Up to 10 associated values can be assigned to a program alarm.
SD2Value	Real	Associated value 2, for example a floating-point number Up to 10 associated values can be assigned to a program alarm.
errPrgAlarm	Bool	Status parameter to detect an error in the processing of the "Program_Alarm" instruction.
stateProgAlarm	Word	Status parameter to store the error information of the instruction "Program_Alarm" in case of an error.
alarmState	Byte	Status of the message as a bit field: • Bit 0: S - S=1: incoming - S=0: outgoing • Bit 1: A_C (Status of the message) - $_{AC=1}$: Incoming alarm was acknowledged • Bit 2: A_G (Status of the message) - $_{AG=1}$: Outgoing alarm was acknowledged • Bit 3: O_C (overflow) - O_C=1: Overflow for incoming messages • Bit 4: OG (overflow) - OG=1: Overflow for outgoing messages • Bit 5: Reserved • Bit 6: Reserved • Bit 7: V (status message information) - V=0: Message information invalid - V=1: Message information valid
errGetAlarmState	Bool	Status parameter to detect an error when processing the "Get_AlarmState" instruction.
stateGetAlarm	Word	Status parameter to store the error information of the instruction "Get_AlarmState" in case of an error.

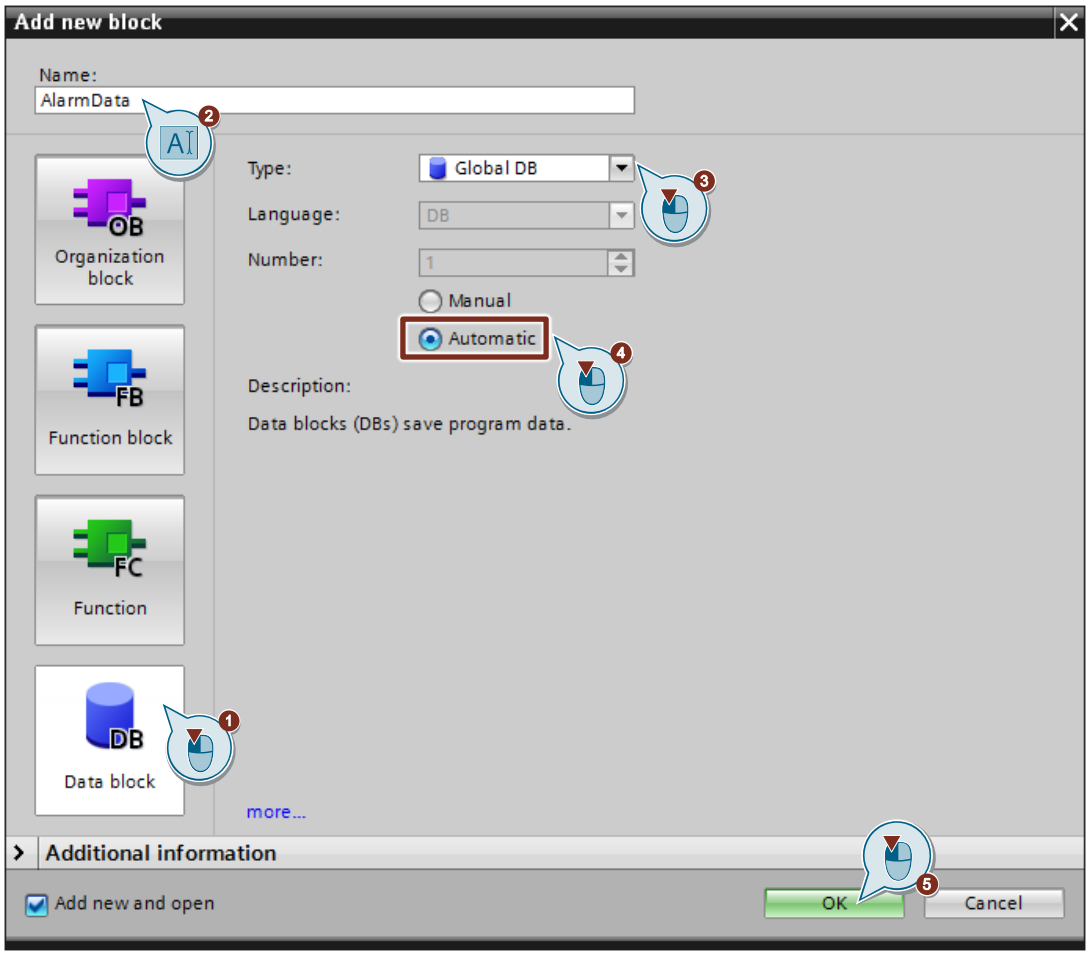
Create tags for the parameters of FB "PrgAlarm"

Insert a data block (DB) and create tags to parameterize the FB "PrgAlarm".

1. In the project tree, navigate to the device folder of the S7-1500 CPU.
2. Open the "Program blocks" folder.
3. Double-click the "Add new block" command.
   The dialog "Add new block" opens.



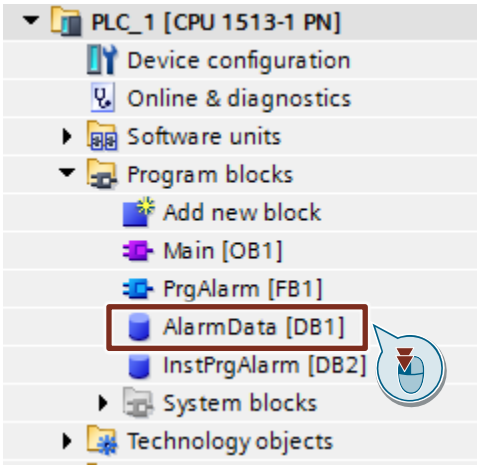
4. Make the following settings.



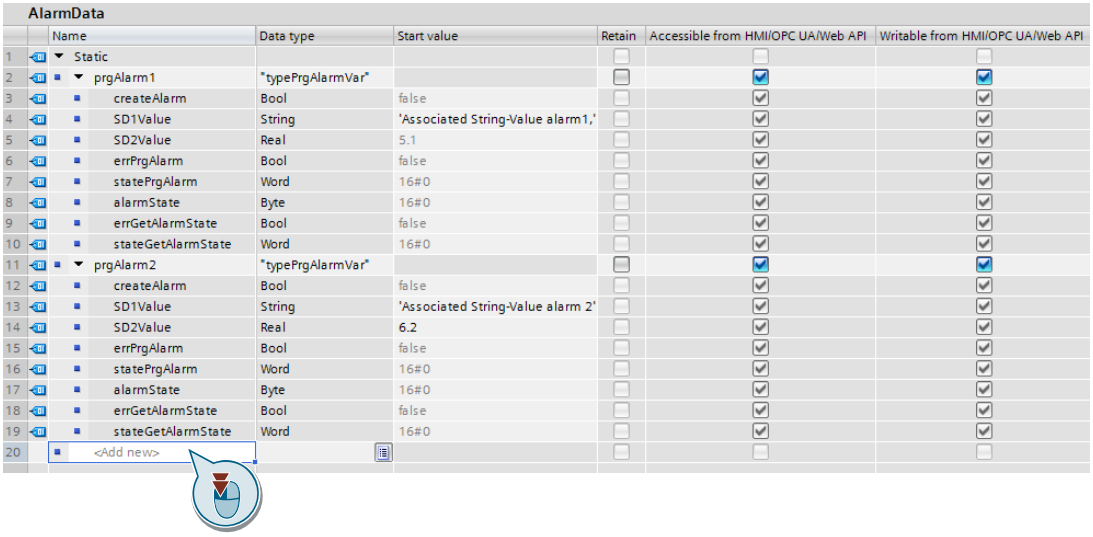
- Click the "Data block" button.
- Enter the name of the DB, e. g. "AlarmData".
- Select the "Global DB" type.
- Select the "Automatic" radio button for automatic number assignment. The number of the global DB will be assigned by TIA Portal.
- Click "OK" to confirm the settings.

The inserted DB "AlarmData" is displayed in the project tree.

5. Double-click on the DB "AlarmData" in the project tree.
The data block opens.



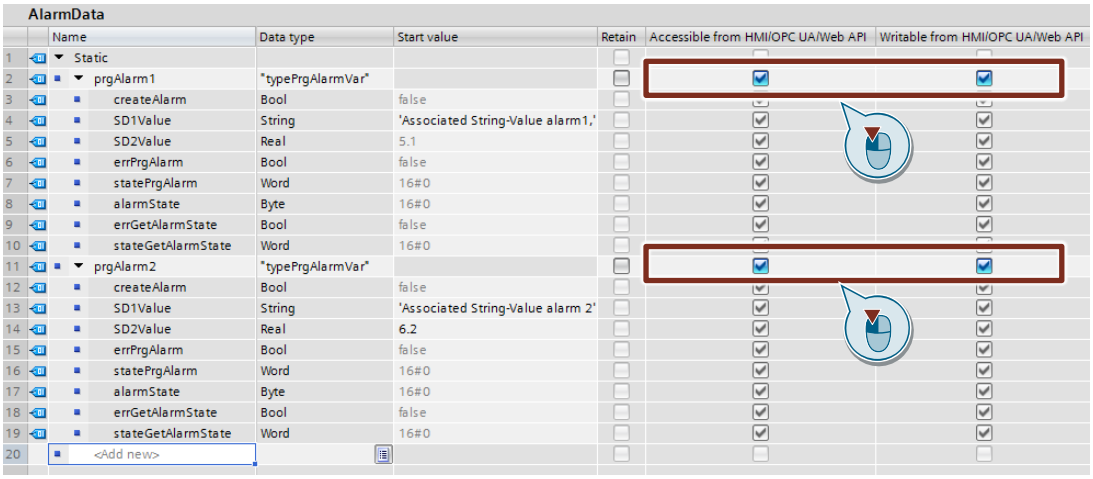
6. Double-click "<Add new>" to create tags.



7. Create the following tags to assign the parameters of the FB "PrgAlarm". The PLC data type "typePrgAlarmVar" is used as data type.

Tag	PLC data type	Description
prgAlarm1	typePrgAlarmVar	Tags for the parameterization of the program alarm with acknowledgement required and 2 associated values
prgAlarm2	typePrgAlarmVar	Tags for parameterization of the program alarm, for information purposes only, without associated values

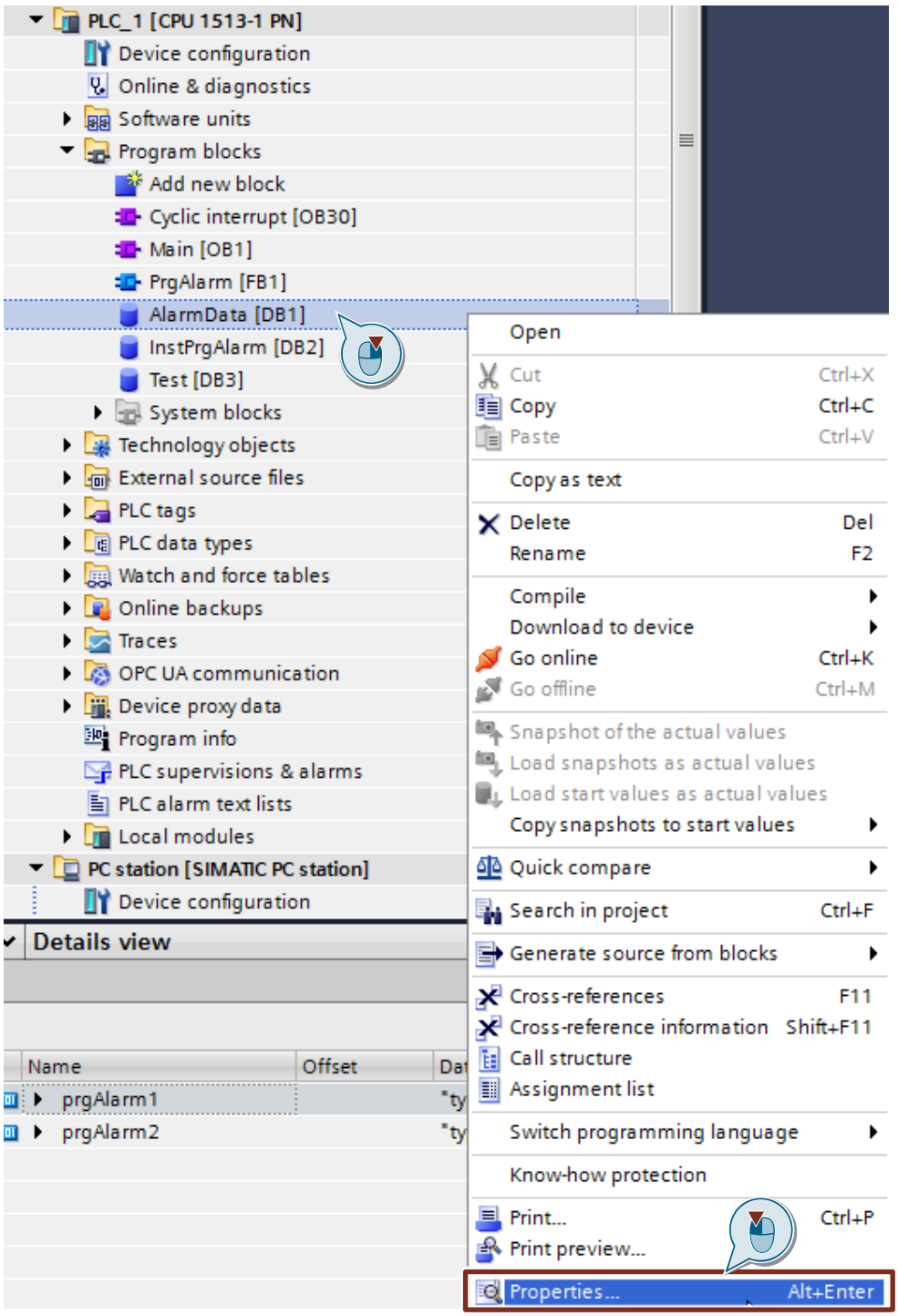
8. Enable the following options for the tags that you created:
   - "Accessible from HMI/OPC UA/Web API"
   - "Writable from HMI/OPC UA/Web API"



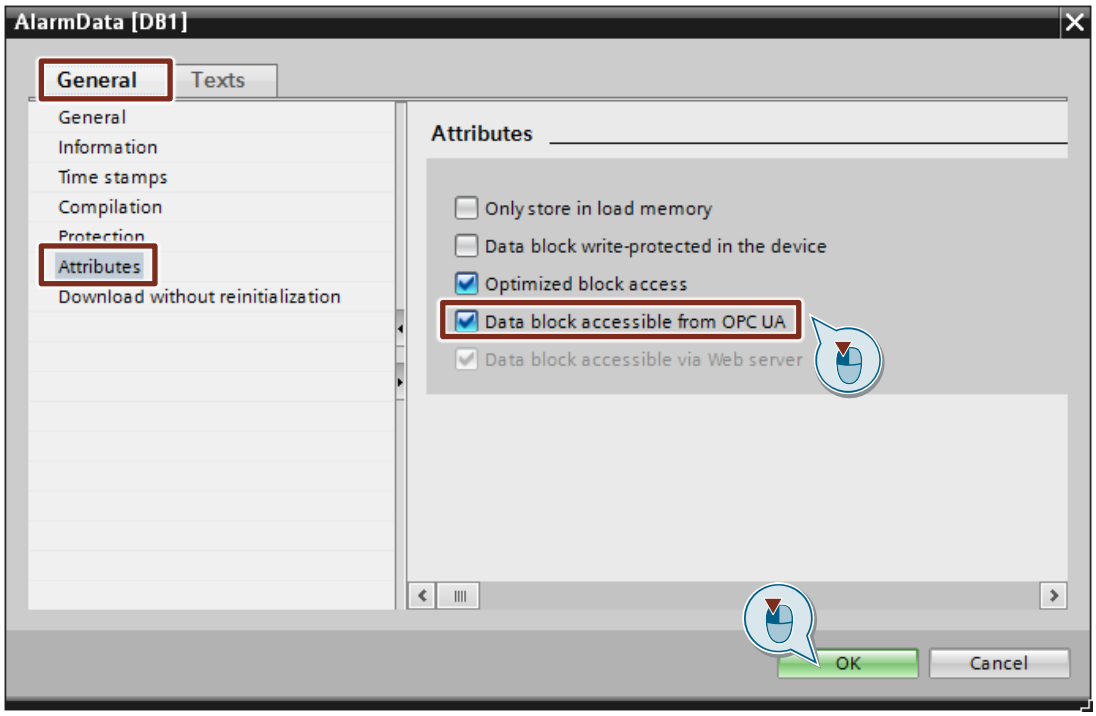
AlarmData

	Name	Data type	Start value	Retain	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API
1	Static					
2	prgAlarm1	"typePrgAlarmVar"			☑	☑
3	createAlarm	Bool	false		☑	☑
4	SD1Value	String	'Associated String-Value alarm1,'		☑	☑
5	SD2Value	Real	5.1		☑	☑
6	errPrgAlarm	Bool	false		☑	☑
7	statePrgAlarm	Word	16#0		☑	☑
8	alarmState	Byte	16#0		☑	☑
9	errGetAlarmState	Bool	false		☑	☑
10	stateGetAlarmState	Word	16#0		☑	☑
11	prgAlarm2	"typePrgAlarmVar"			☑	☑
12	createAlarm	Bool	false		☑	☑
13	SD1Value	String	'Associated String-Value alarm 2'		☑	☑
14	SD2Value	Real	6.2		☑	☑
15	errPrgAlarm	Bool	false		☑	☑
16	statePrgAlarm	Word	16#0		☑	☑
17	alarmState	Byte	16#0		☑	☑
18	errGetAlarmState	Bool	false		☑	☑
19	stateGetAlarmState	Word	16#0		☑	☑
20	<Add new>				☐	☐

9. In the project tree, right-click the DB "AlarmData".
   The context menu opens.
10. Select "Properties".
    The Properties dialog box for the DB "AlarmData" will open.



11. In the "General" tab under "Attributes", enable the function "Data block accessible from OPC UA".



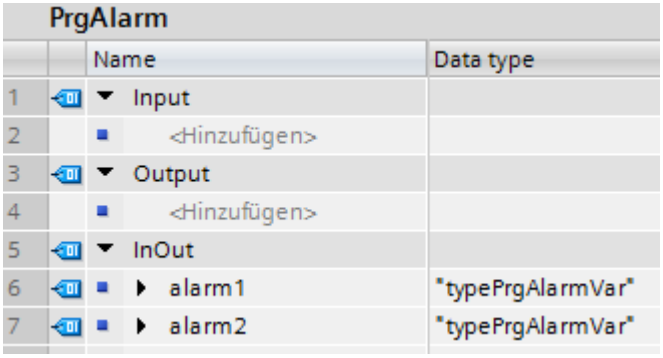
Call the instructions "Program_Alarm" and "Get_AlarmState"

Two program alarms are generated in FB "PrgAlarm":

- Program alarm with required acknowledgement and two associated values
- Program alarm for information purposes only, without associated values

Create two "InOut" parameters of the data type "typePrgAlarmVar" in the interface of the FB "PrgAlarm".

- alarm1
- alarm2



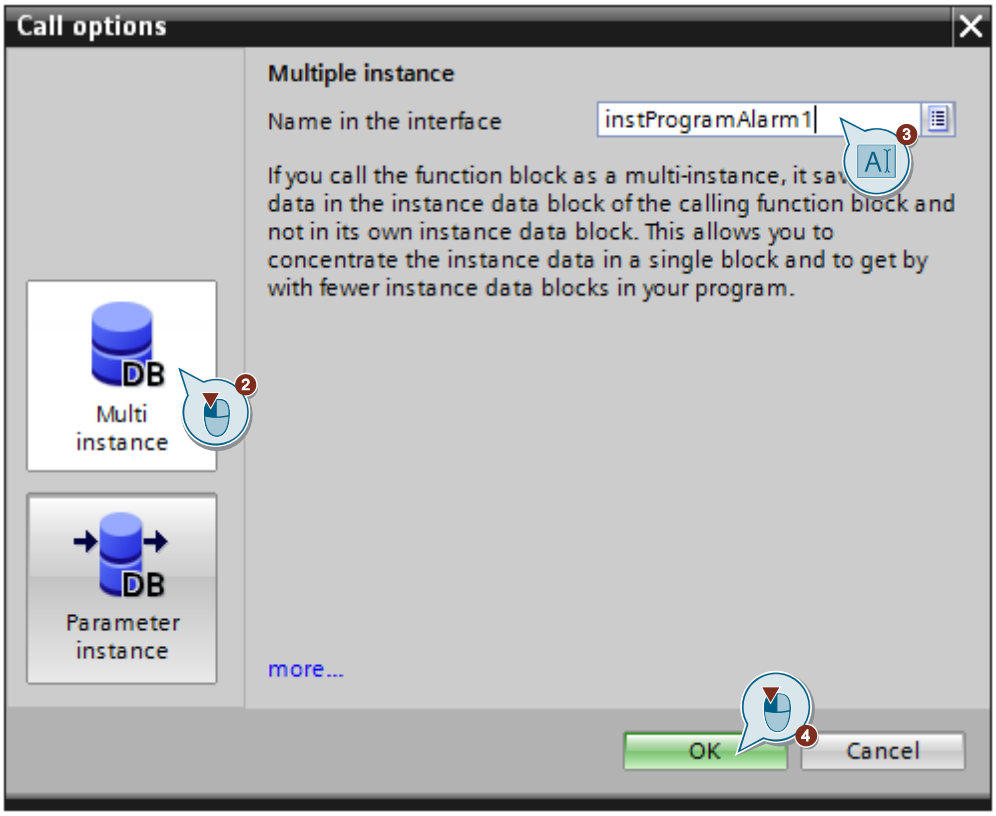
Generate program alarm with required acknowledgement and two associated values

1. Call the "ProgramAlarm" instruction in the FB "PrgAlarm".
   The "Call options" dialog opens automatically to create the instance DB of the "Program_Alarm" instruction.

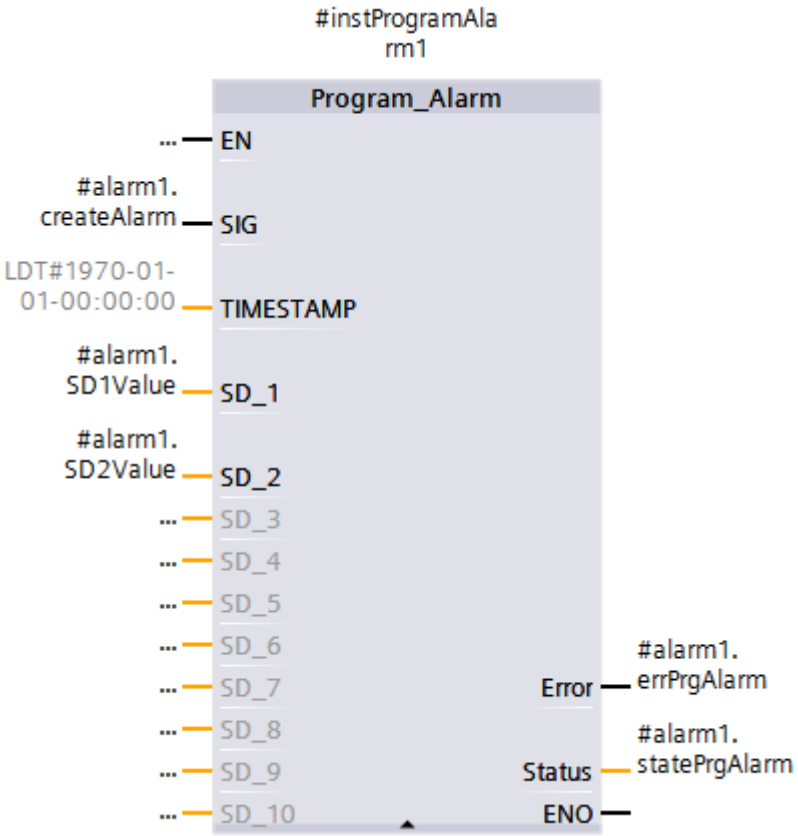
Note

You will find the "ProgramAlarm" instruction in the "Instructions" task card in the "Extended instructions" palette under "Alarming".

2. Click the "Multi instance" button.
3. Enter the name of the multi-instance, e. g. "instProgramAlarm1".
4. Click "OK" to confirm the settings.



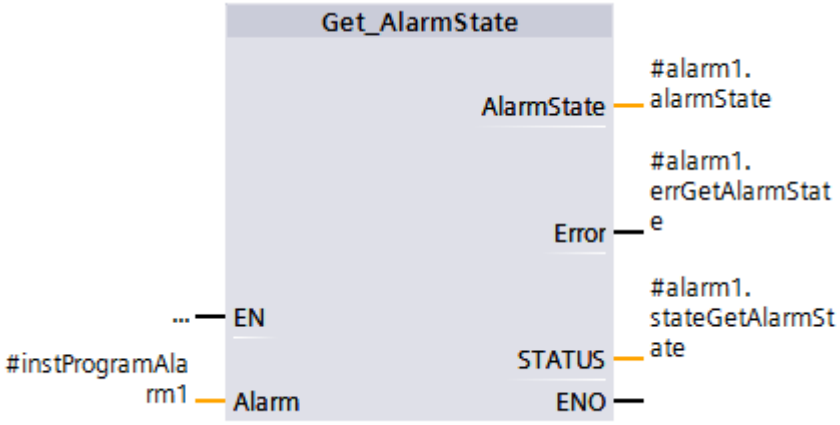
5. Interconnect the parameters of the instance "#instProgramAlarm1" with the tags of the "InOut" parameter "alarm1".
   - SIG: #alarm1.createAlarm (triggers an alarm on a positive edge)
   - SD_1: #alarm1.SD1Value (alarm accompanying value 1)
   - SD_2: #alarm1.SD2Value (alarm accompanying value 2)
   - Error: #alarm1.errPrgAlarm
   - Status: #alarm1.statePrgAlarm



6. To output the alarm state of the program alarm, call the "Get_AlarmState" instruction.

Note You will find the "Get_AlarmState" instruction in the "Instructions" task card in the "Extended instructions" palette under "Alarming".

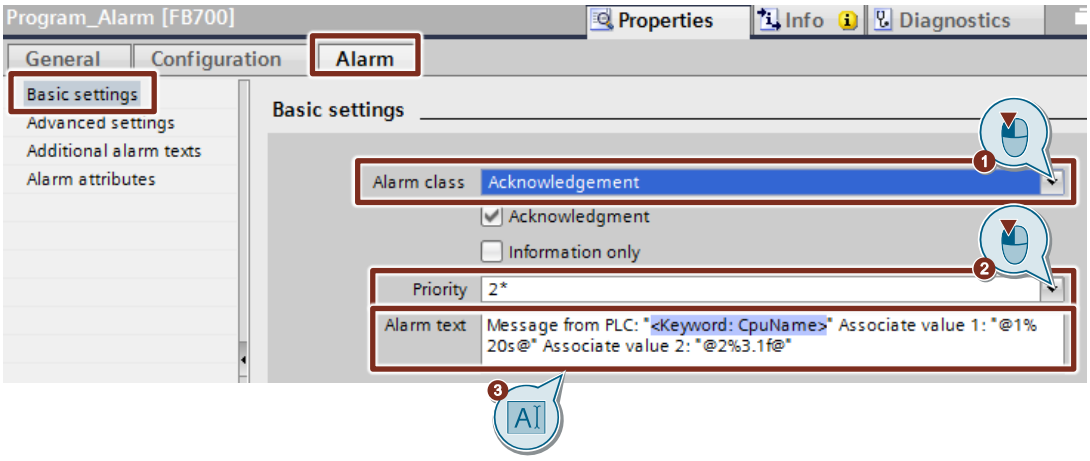
7. At the "Alarm" input parameter, specify the instance DB "#instProgramAlarm1" of the triggering program alarm.
8. Connect the output parameters of the "Get_AlarmState" instruction with the tags of the "InOut" parameter "alarm1".
   - AlarmState: #alarm1.alarmState
   - Error: #alarm1.errGetAlarmState
   - State: #alarm1.stateGetAlarmState



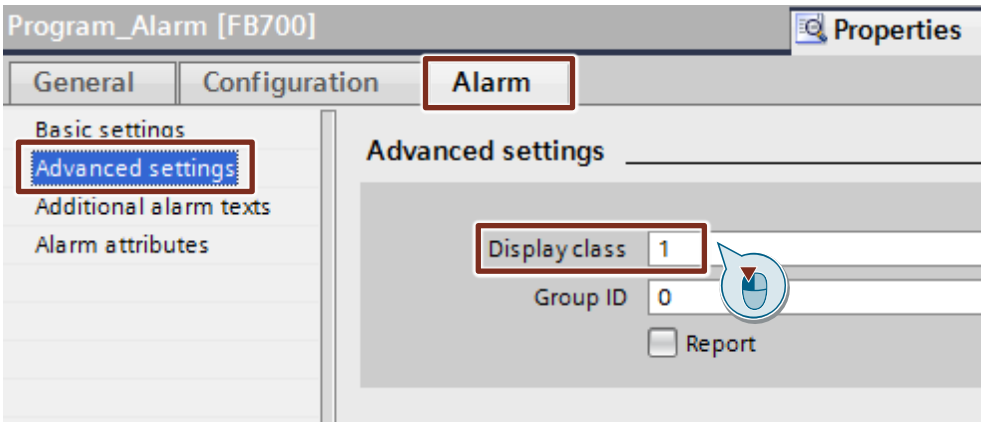
9. Select the instruction "Program_Alarm".
   The properties of the program alarm are displayed in the Inspector window.
10. Configure the following settings in the "Alarm" tab under "Basic settings":
    - "Alarm class": "Acknowledgement", i. e. this program alarm requires an acknowledgement.

Note The "Acknowledgment" function will be activated automatically.

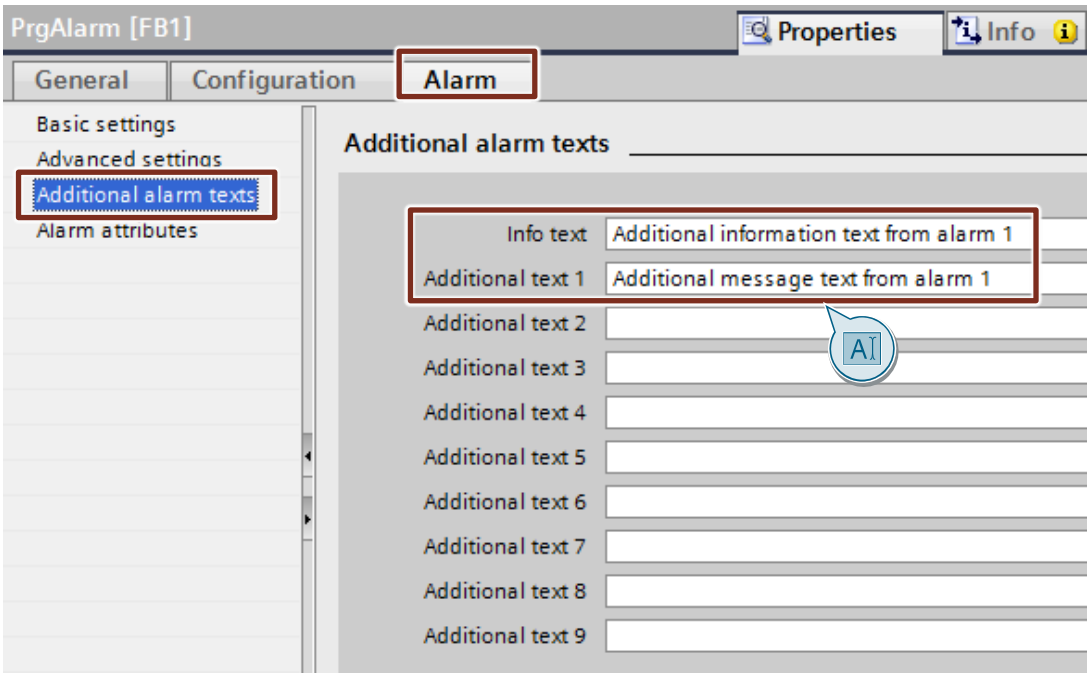
- "Priority": 2
- "Alarm text"



11. Set the "Display class", e. g. 1, in the "Alarm" tab under "Advanced settings".



12. Enter any informational text and additional texts for the program alarm in the "Alarm" tab under "Additional alarm texts".



Note

To insert a dynamic tag in the message text, right-click in the "Message text" field. Select "Insert keyword…" and specify the appropriate keyword. In this example, the name of the PLC that triggers the program alarm is displayed.

It is also possible to enter dynamic keywords in the additional message texts.

You can include the associated values in the alarm text in the following format:

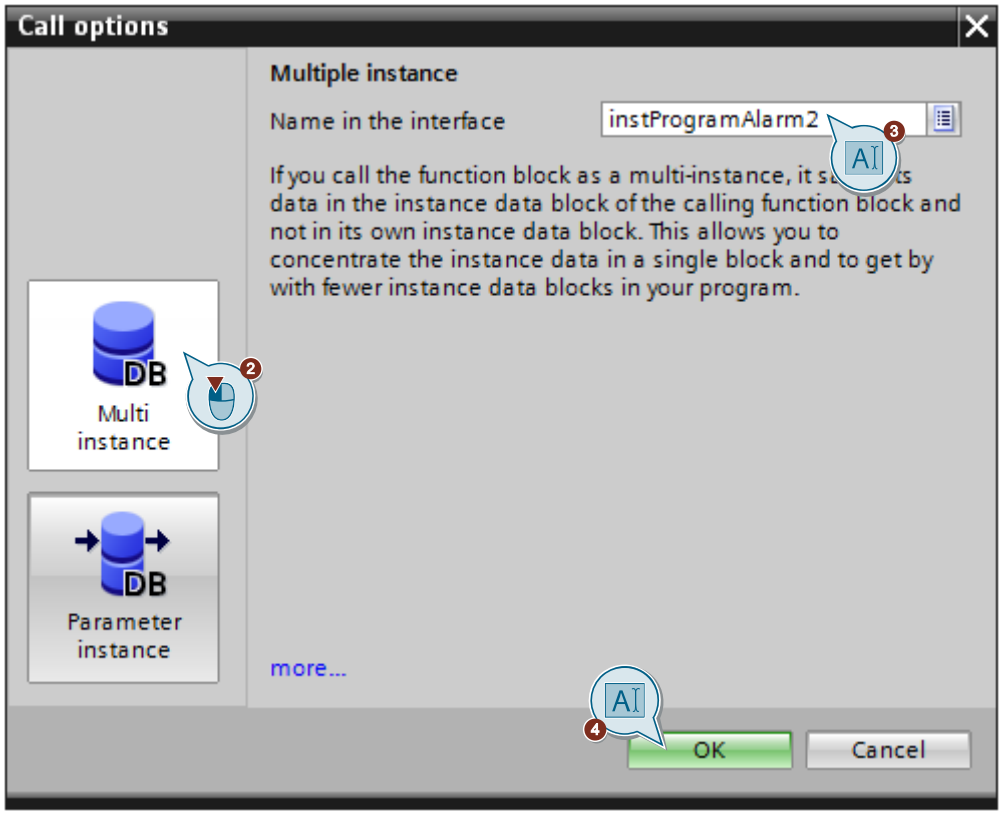
@<Associated value number>%<Format specification>@

Example:

- "@1%3.1f@" for the formatting of the associated value SD_1 (real number with 3 digits and 1 decimal place) in the alarm text.
- "@2%20s@" for the formatting of the associated value SD_2 (string tag) in the alarm text.

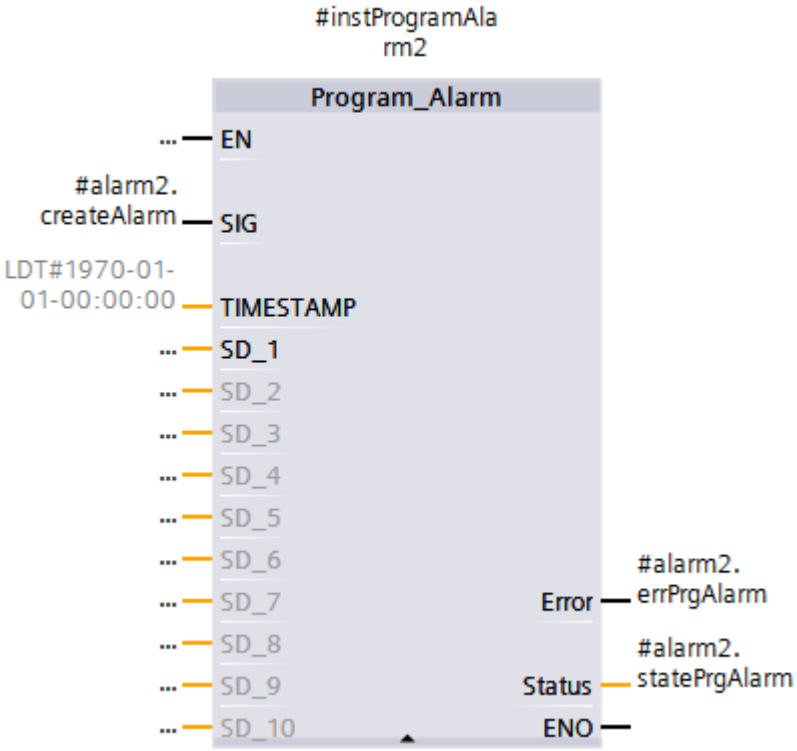
Generate a program alarm for informational purposes only, without any accompanying values

1. Call the "ProgramAlarm" instruction in the FB "PrgAlarm".
   The "Call options" dialog opens automatically to create the instance DB of the "Program_Alarm" instruction.



2. Click the "Multi instance" button.
3. Enter the name of the multi-instance, e. g. "instProgramAlarm2".
4. Click "OK" to confirm the settings.

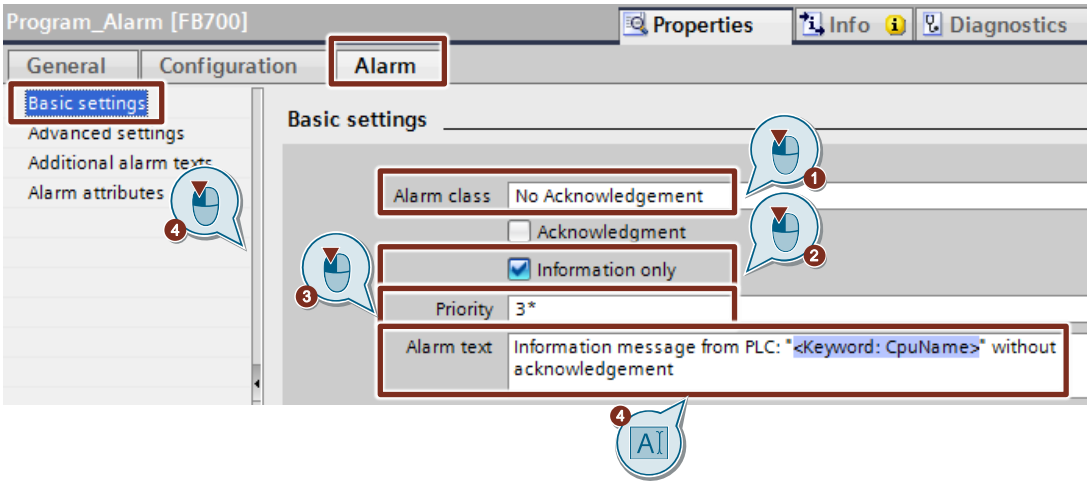
5. Interconnect the parameters of the instance "#instProgramAlarm2" with the tags of the "InOut" parameter "alarm2".
   - SIG: #alarm2.createAlarm (triggers an alarm on a positive edge)
   - Error: #alarm2.errPrgAlarm
   - Status: #alarm2.statePrgAlarm



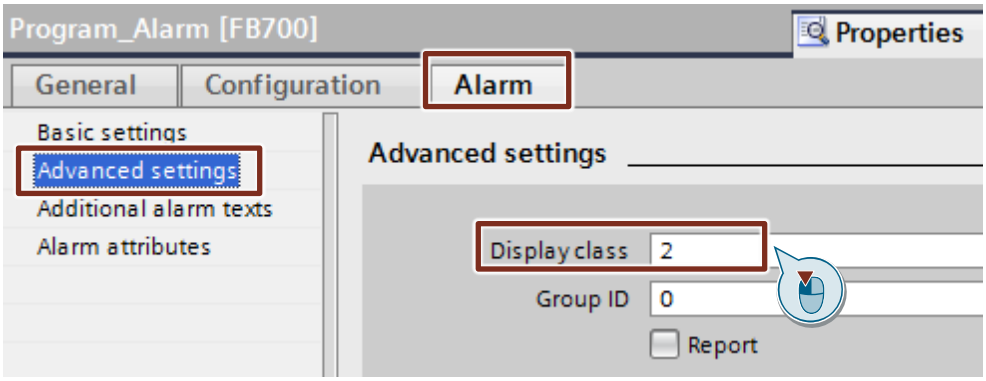
6. Select the instruction "Program_Alarm".
   The properties of the program alarm are displayed in the Inspector window.
7. Configure the following settings in the "Alarm" tab under "Basic settings":
   - "Alarm class": "No Acknowledgement", i. e. this program alarm does not require an acknowledgement

Note The "Acknowledgment" function is automatically disabled.

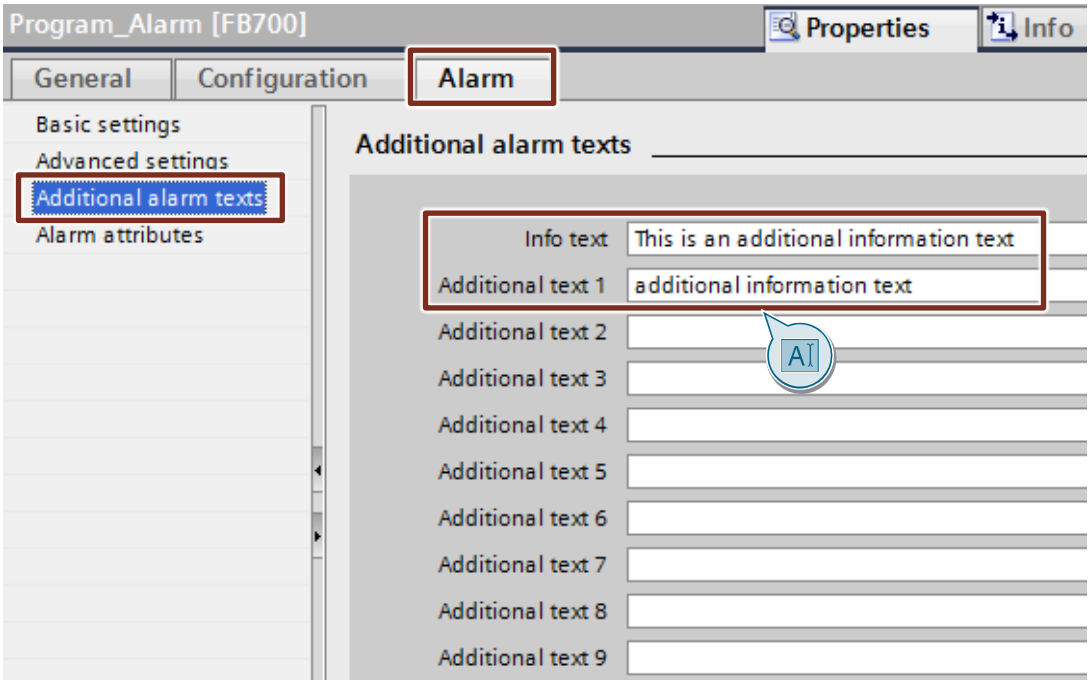
   - Enable the function "Information only".
   - "Priority": 3
   - "Alarm text":



8. In the "Alarm" tab under "Advanced settings", set the display class, e. g. 2.



9. Enter any informational text and additional texts for the program alarm in the "Alarm" tab under "Additional alarm texts".



Note

For program alarms that are only used for information purposes, it is not necessary to output the message state with the "Get_AlarmState" instruction.

If a program alarm is generated without accompanying values, it is not necessary to assign the input parameters "SD_1" to "SD_2".

To insert a dynamic tag in the message text, right-click in the "Message text" field. Select "Insert keyword…" and specify the appropriate keyword. In this example, the name of the PLC that triggers the program alarm is displayed.

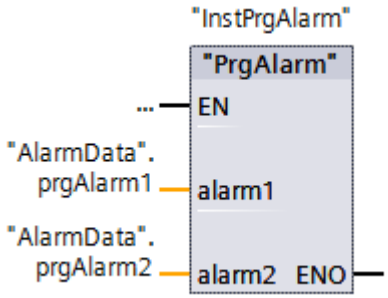
It is also possible to enter dynamic keywords in the additional message texts.

Parameterization of FB "PrgAlarm"

Call the FB "PrgAlarm" in the user program of the S7-1500 CPU, for example in OB 1.

The following figure shows the call of the FB "PrgAlarm" in OB 1.

Figure 2-11



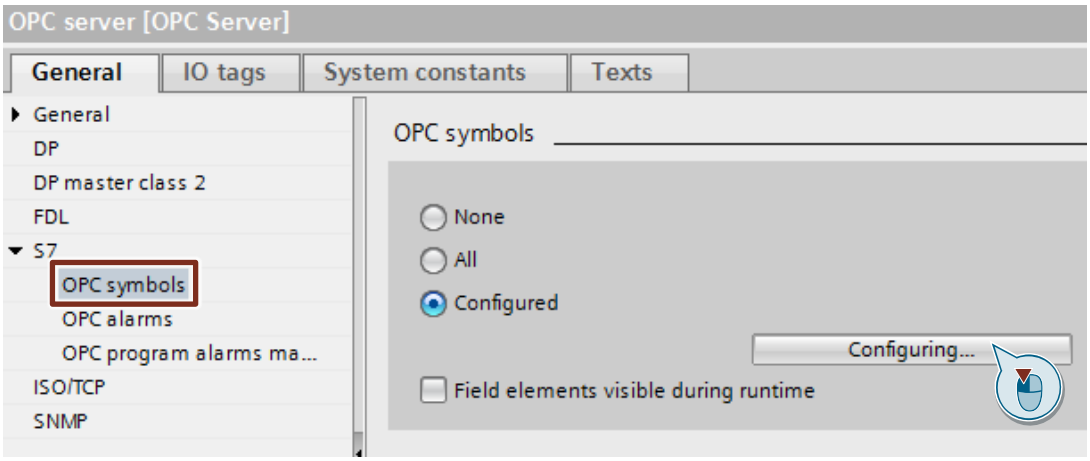
The following table shows the parameters of the FB "PrgAlarm".

Table 2-2

Parameter	Declaration	Data type	Description
alarm1	InOut	typePrgAlarmVar	Detailed information about the data type "typePrgAlarmVar" can be found in Table 2-1.
alarm2	InOut	typePrgAlarmVar	Detailed information about the data type "typePrgAlarmVar" can be found in Table 2-1.

2.5.5 Declaring S7 symbols to the OPC server

1. Open the "Device view" of the PC station.
2. Select the OPC server.
   The properties of the OPC server are displayed in the Inspector window.
3. In the "General" tab, navigate to "S7 > OPC symbols".
4. To access configured symbolic S7 tags in the OPC server, enable the option "Configured" and click the "Configuring" button.
   The "Symbol Configuration" dialog opens.



5. Select the S7 tags to make the following settings:
   - Visibility:
     You can enable or disable visibility for the selected S7 tags.
     If the selected S7 tags need to be visible in the OPC server, it is necessary to enable the "Visible" option. This is necessary so that the OPC client can access the S7 tags.

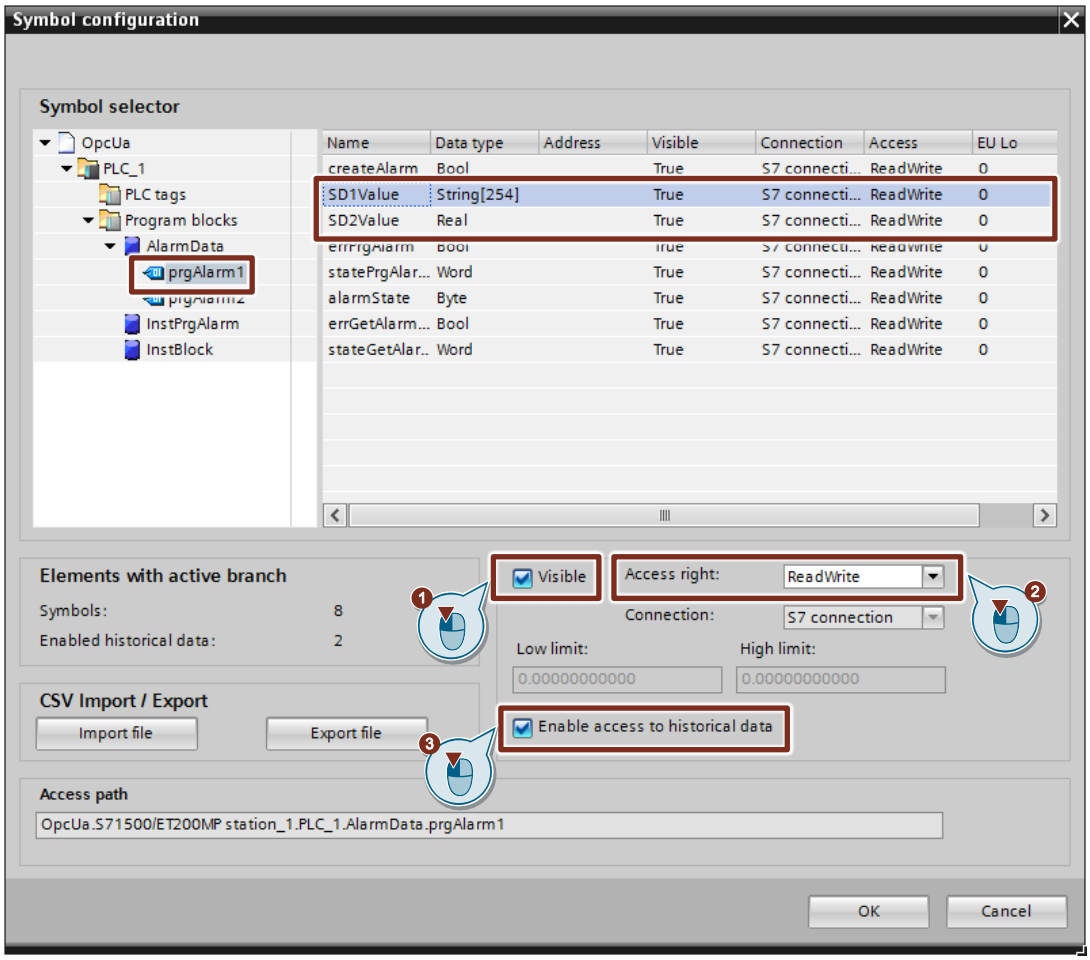
Note The "Visible" option is enabled by default.

   - Access permissions:
     Set the access permission that the OPC server has to the selected S7 tags.

Note The "ReadWrite" access permission is pre-set by default, i. e. the OPC server has read and write access to the S7 tags.

   - Access to historical data:
     You can enable or disable access to historical data for the selected S7 tags.
     In this example, the "Enable access to historical data" function is enabled for the associated values of the program alarm with required acknowledgement.

Note The function "Enable access to historical data" is disabled by default.



6. Click "OK" to apply the settings.

2.6 Configuring the "Station Configuration Editor"

This chapter demonstrates how to configure the "Station Configuration Editor".

You have the following options for configuring the "Station Configuration Editor":

- Manual configuration (see chapter 2.6.1)
- Configure in TIA Portal (see chapter 2.6.2)
- XDB export: Export XDB from TIA Portal (see chapter 2.6.3)

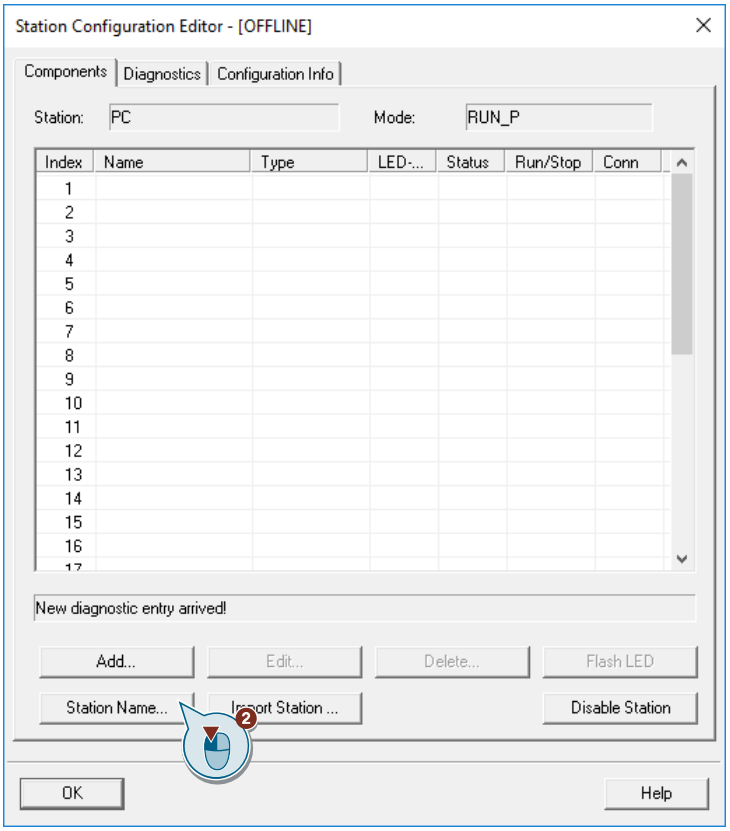
2.6.1 Manual configuration

Note

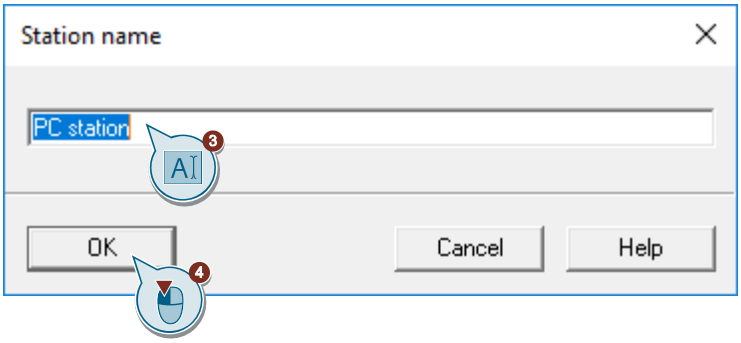
Insert the components in the same order as in the component image that you created in TIA Portal in the PC station "Device view". If the configuration differs, the configuration data that you download from TIA Portal to the PC station will not be adopted correctly.

When configuring for the first time it is necessary to enter the station name.

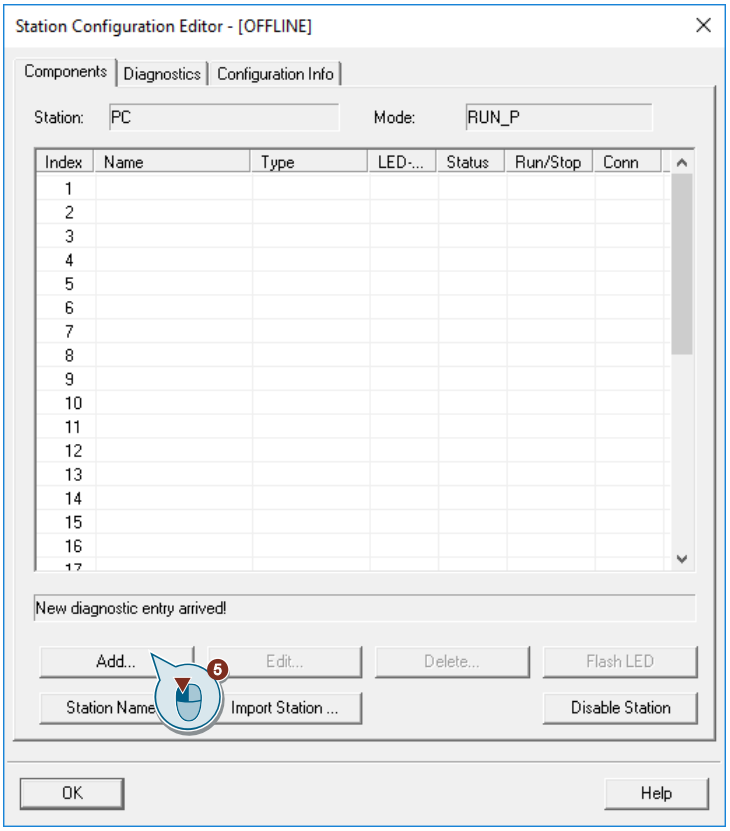
1. Double-click the corresponding icon on your desktop to start the "Station Configuration Editor".
2. Click the "Station Name" button.
   The "Station name" dialog will open.



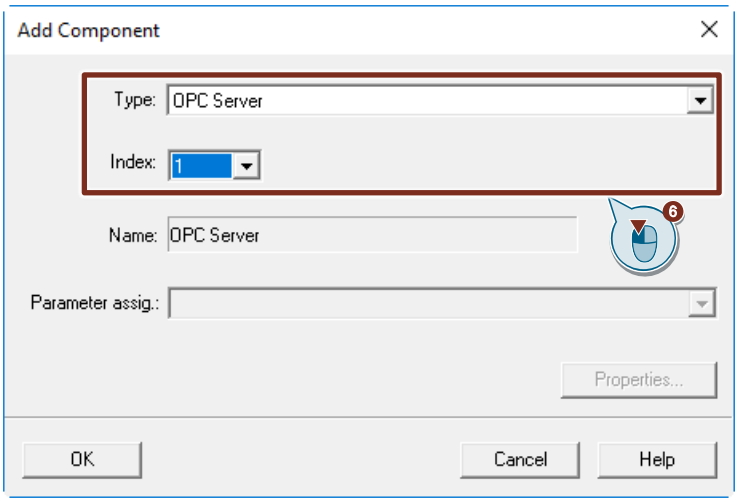
3. Enter the station name, e. g. "PC station".
   It is imperative that the name in the "Station Configuration Editor" matches the name that you assigned when configuring the PC station with TIA Portal.
4. Click "OK" to confirm the settings.



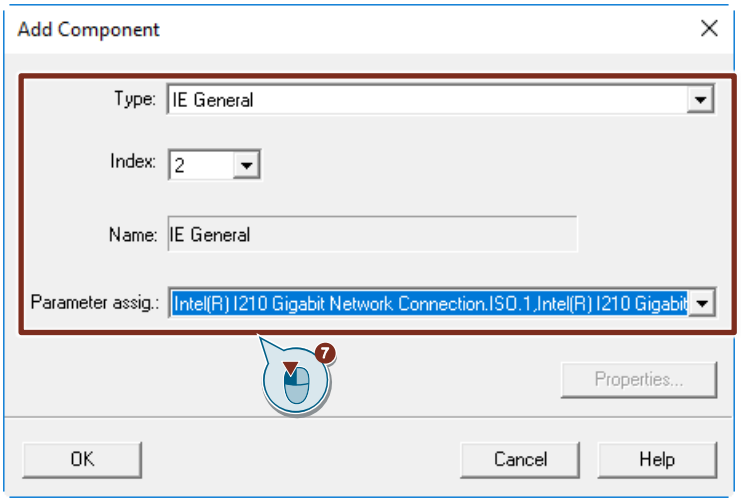
5. Click the "Add" button.
   The "Add Component" dialog box opens.



6. Configure the following settings to add the "OPC server" user application.
   - "Type": "OPC Server"
   - "Index": 1



7. Make the following settings to add the "IE General" component.
   - "Type": "IE General"
   - "Index": 2
   - "Parameter assig.":
     Select the network adapter via which the PC station is connected to communicates with the S7 CPU.

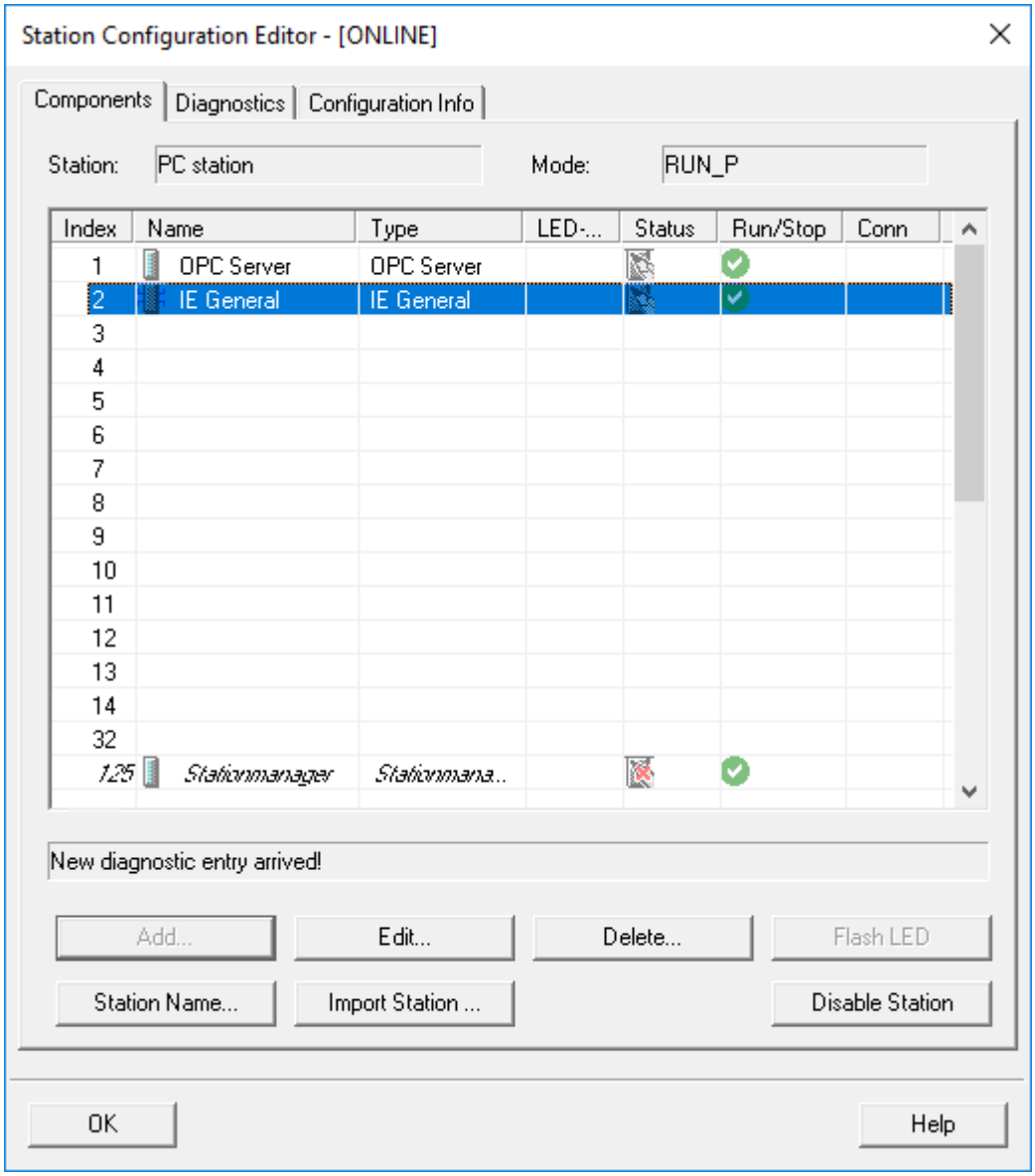


Result

The added components and the station name will be displayed in the "Station Configuration Editor":

- Station: "PC station"
- Index 1: "OPC server"
- Index 2: "IE General"
- Index 125: "Stationmanager"
  "Stationmanager" will be automatically added at this index by the system.

Figure 2-12



The following status icons for the components show that the configuration data are not yet loaded:

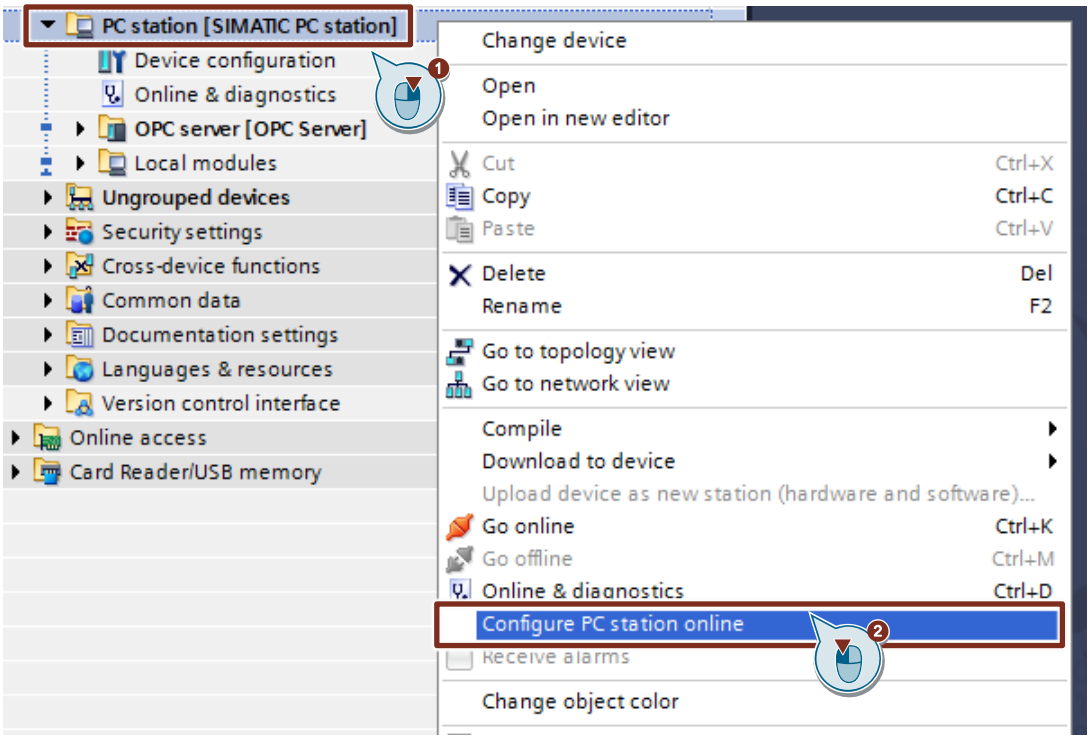
Table 2-3

Status icon	Meaning
	• The component is present in the current configuration of the PC station. • The component has a configuration that is derived from a default parameter set. The default parameter set allows a component to be accessible via network without further configuration immediately after its installation. Make sure that the default parameter set you use has parameters that match the other network parameter settings.
	• The component exists in the current configuration of the PC station, but it was not created in the project engineering. Depending on the intended application, you still might have to configure the component in TIA Portal and load the configuration.

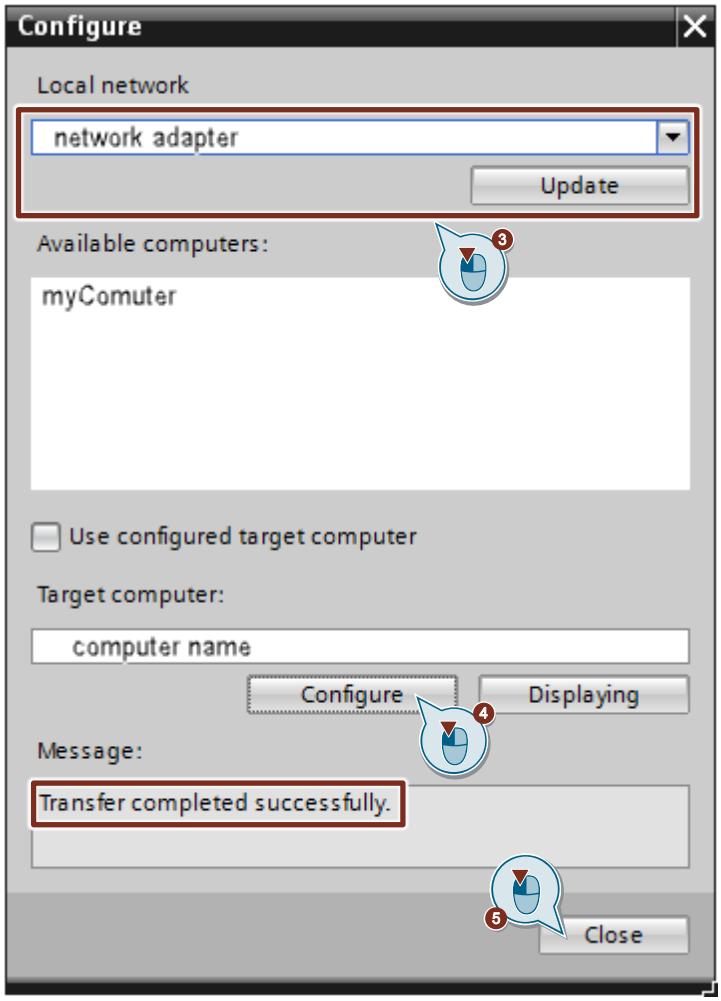
After you have manually configured the "Station Configuration Editor", load the configuration into the PC station (see chapter 2.7.1)

2.6.2 Configure in TIA Portal

1. Right-click on the device folder of the PC station.
   The context menu opens.
2. Select "Configure PC station online". The "Configure" dialog will open.



3. Select the network adapter via which the PC station communicates with the S7 CPU, then click "Update".
4. Click "Configure" to transfer the configuration of the PC station to the Station Configuration Editor.
   The message "Transfer completed successfully" will appear once the transfer has completed successfully.
5. Click "Close" to finish the dialog.

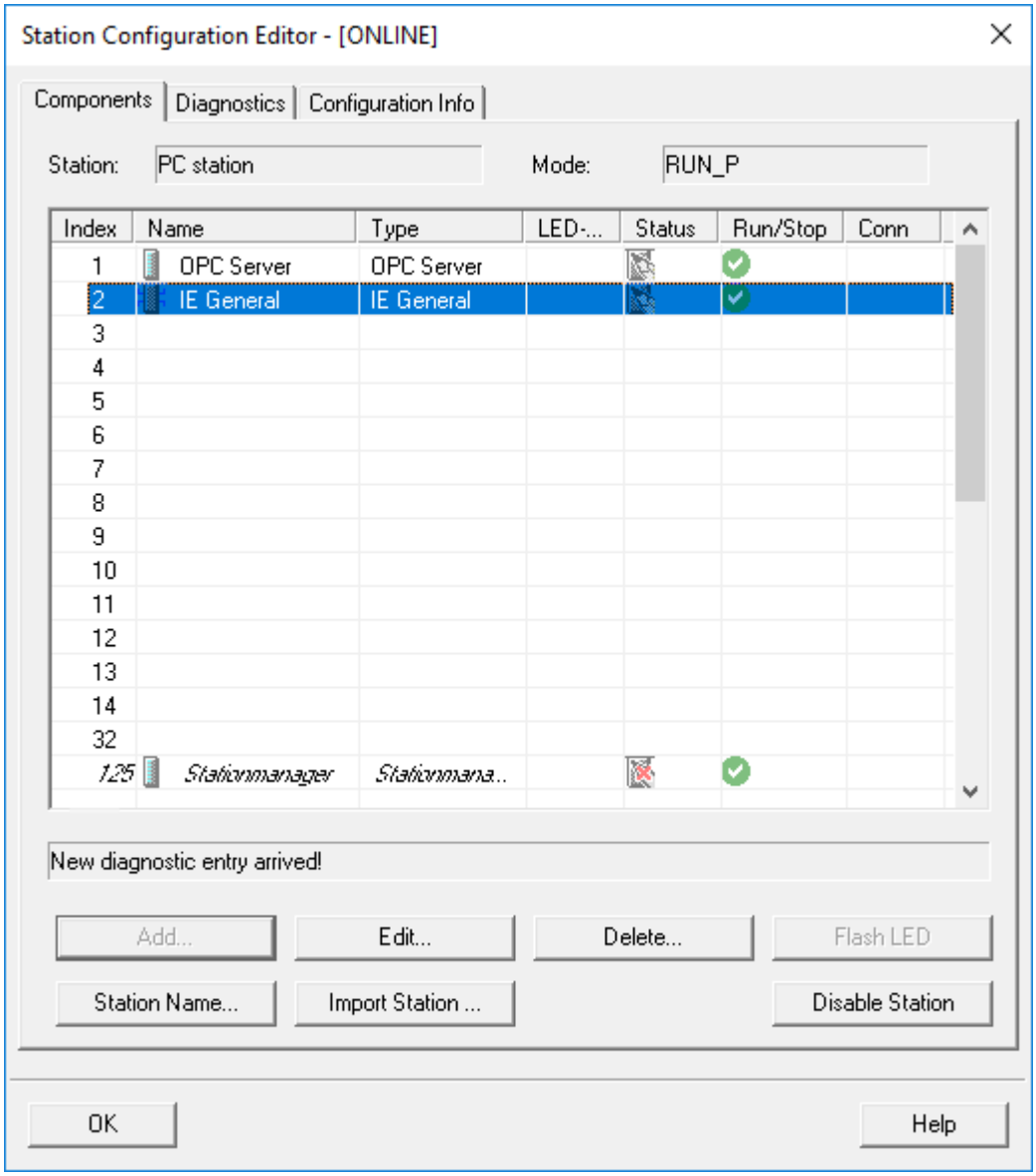


Result

In the "Station Configuration Editor", the components and the station name are created according to the configuration in TIA Portal:

- Station: "PC station"
- Index 1: "OPC server"
- Index 2: "IE General"
- Index 125: "Stationmanager"
  "Stationmanager" will be automatically added at this index by the system.

Figure 2-13



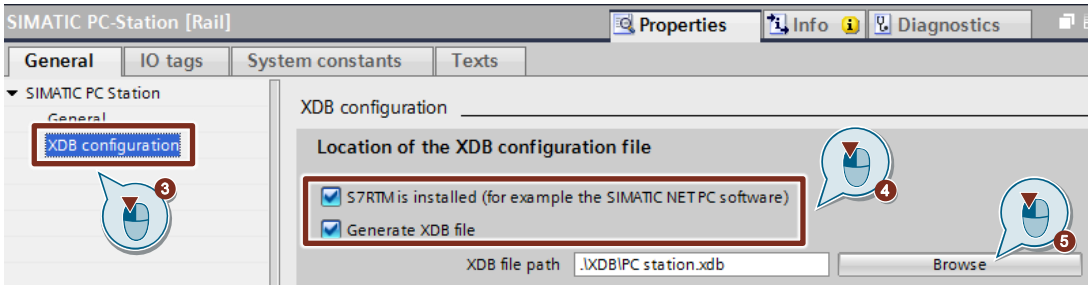
The following status symbols for components show that the configuration is not yet loaded:
Table 2-4

Status icon	Meaning
	• The component is present in the current configuration of the PC station. • The component has a configuration that is derived from a default parameter set. The default parameter set allows a component to be accessible via network without further configuration immediately after its installation. Make sure that the default parameter set you use has parameters that match the other network parameter settings.
	• The component exists in the current configuration of the PC station, but it was not created in the project engineering. Depending on the intended application, you still might have to configure the component in TIA Portal and load the configuration.

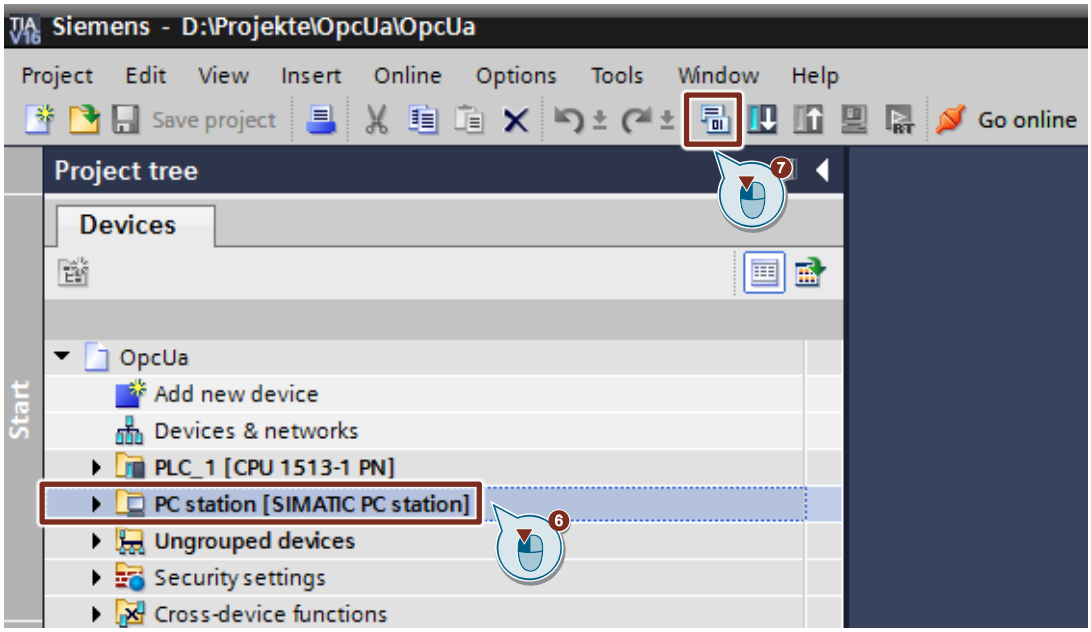
After you have configured the "Station Configuration Editor" in TIA Portal, load the configuration into the PC station (see chapter 2.7.1).

2.6.3 XDB export: Exporting XDB from TIA Portal

1. Open the "Device view" of the PC station.
2. Select the PC station.
   The Inspector window displays the properties of the PC station.
3. In the "General" tab, navigate to "XDB configuration".
4. Enable the following functions:
   - "S7RTM is installed (for example SIMATIC NET PC software)"
   - "Generate XDB file"
5. Click on the "Browse" button to set the path where the XDB file will be stored.



6. Select the PC station in the project tree.
7. Click on the "Compile" button in the function bar.



Result

The XDB configuration file will be generated and saved in the directory that you set when configuring the PC station.

Once the XDB configuration file has been exported, it is necessary to import it into the "Station Configuration Editor" (see chapter 2.7.2.2).

2.7 Loading the configuration

This chapter demonstrates how to load the configuration into the PC station and the S7 CPU.

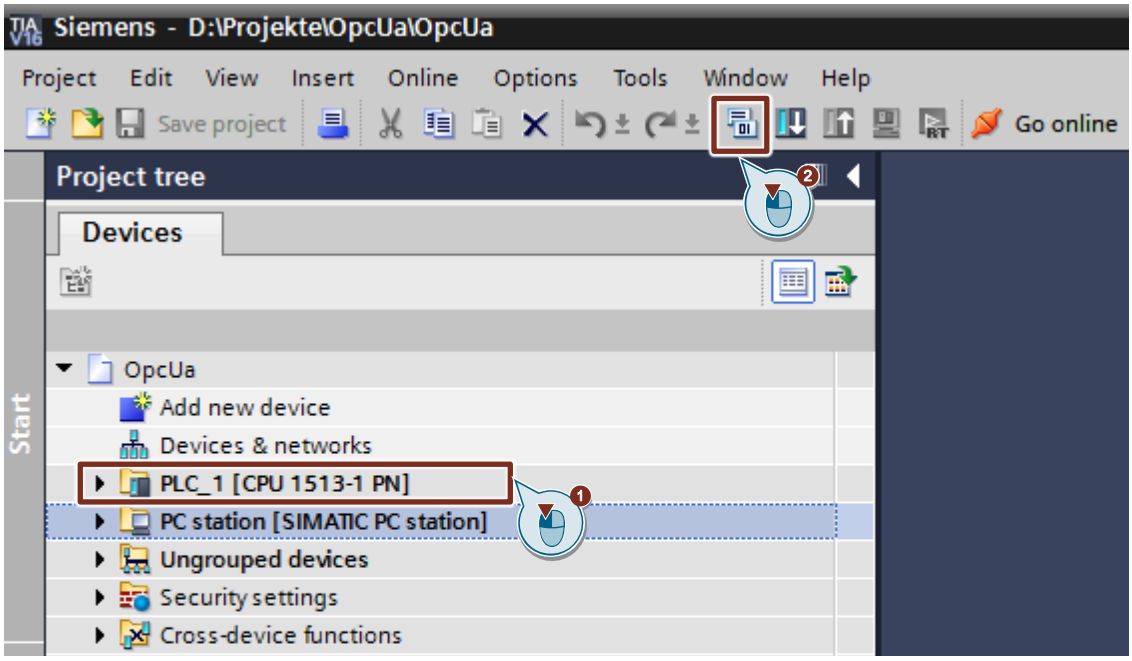
2.7.1 Load configuration into S7 CPU

Requirements

- Engineering PC and S7 CPU are in the same subnet.
- You set the same IP address and subnet mask for the S7 CPU as you did in the hardware configuration (see chapter 2.2.2).

Compile

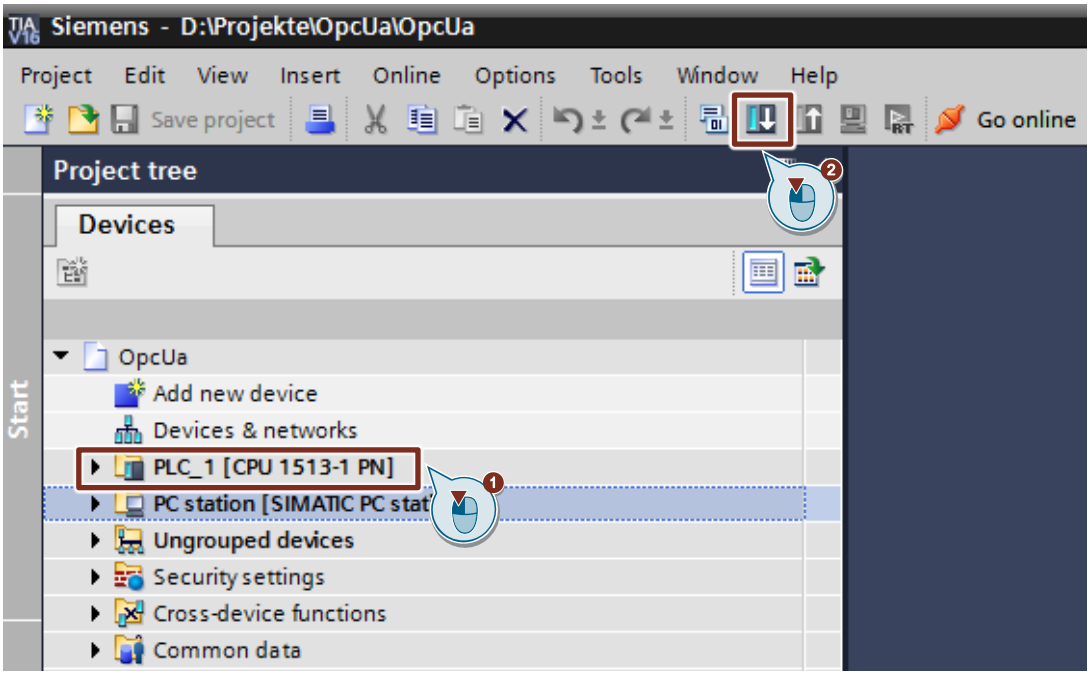
Figure 2-14



1. Select the S7 CPU in the project tree.
2. Click on the "Compile" button in the function bar.

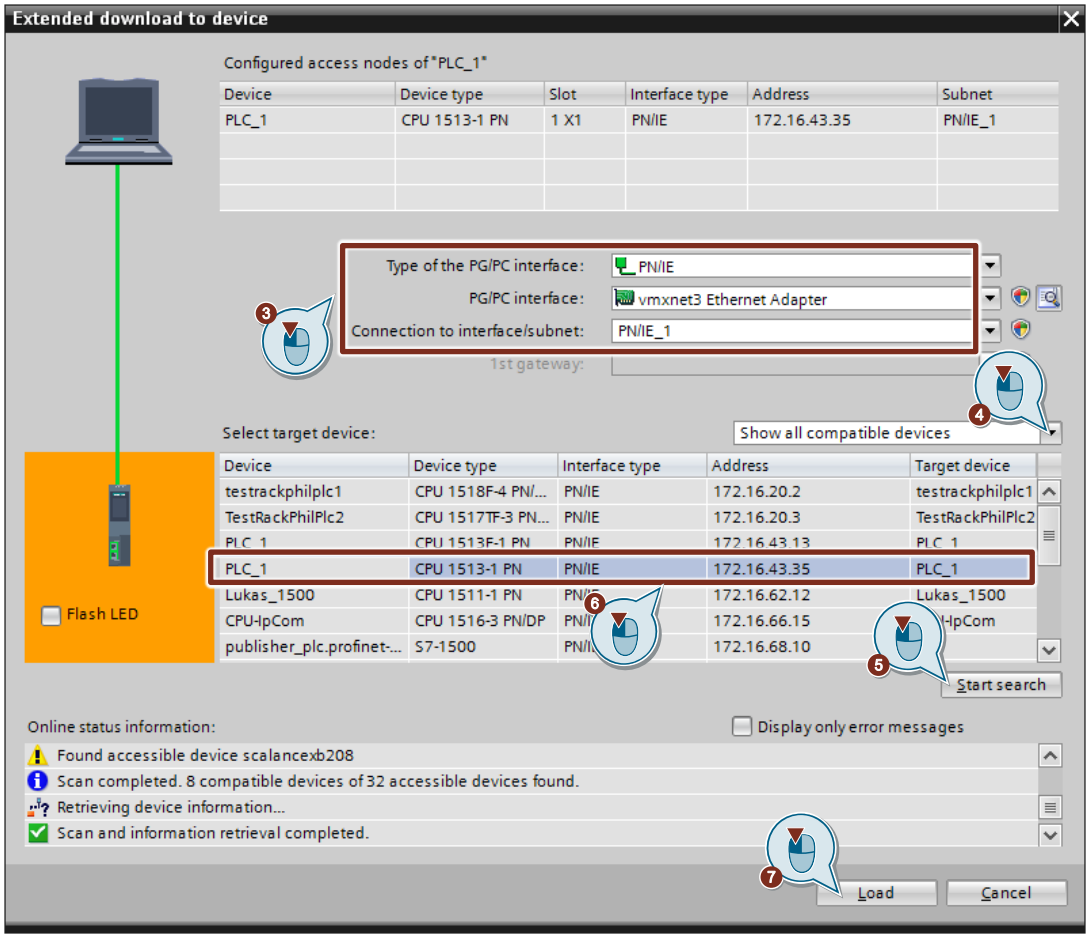
Downloading

1. Select the S7 CPU in the project tree.
2. Click on the "Download to device" button in the function bar.
   The "Extended download to device" or "Load preview" dialog opens automatically.

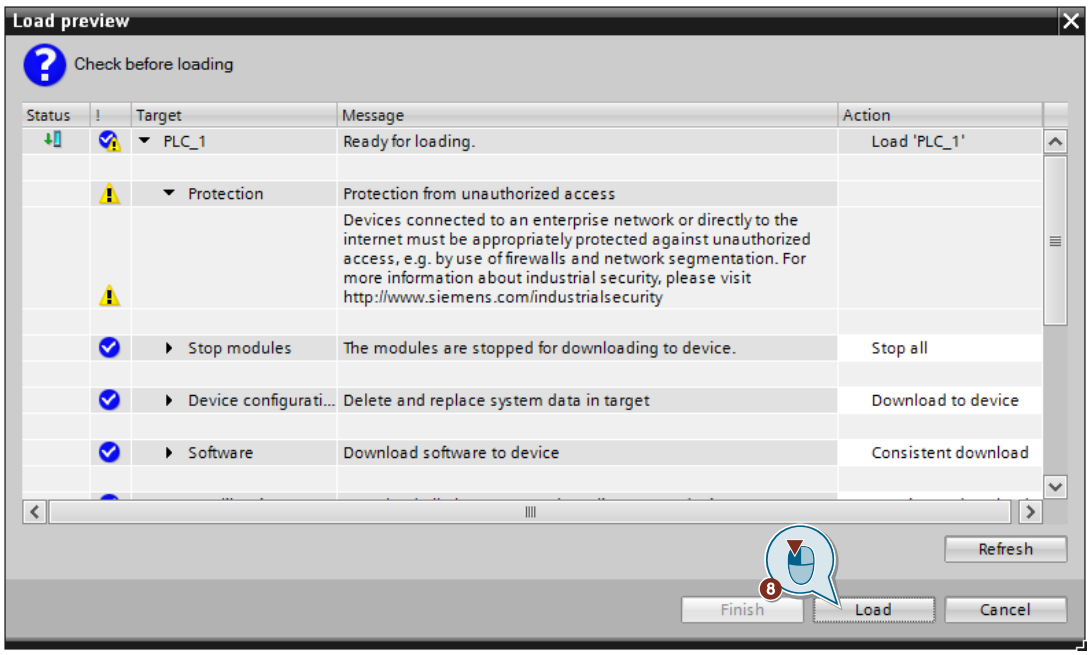


Note The "Extended download to device" dialog is only opened automatically if the access path from the PG/PC to the S7 CPU must be reset.

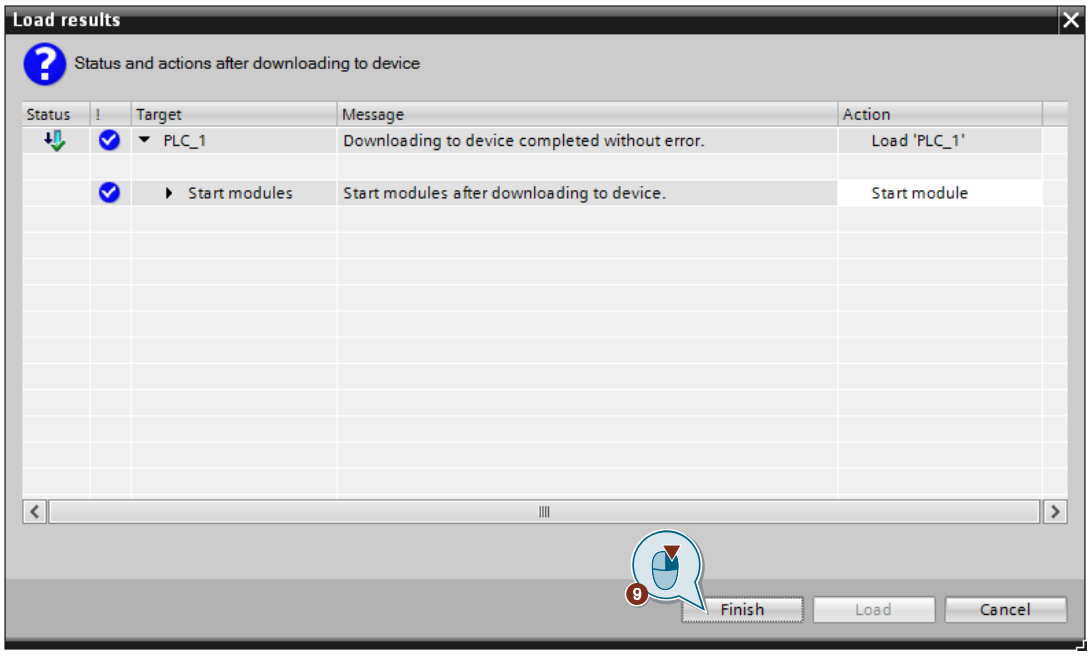
3. In the "Extended download to device" dialog, make the following settings to access the S7 CPU via TCP/IP:
   - "Type of the PG/PC interface": PN/IE
   - "PG/PC interface": PG/PC network adapter
   - "Connection to interface/subnet": Subnet of the S7 CPU, e. g. PN/IE_1
4. Select the "Show all compatible devices" option.
5. Click the "Start search" button.
6. Select the S7 CPU as the target device.
7. Click "Load".
   The "Load preview" dialog window opens.



8. Click the "Load" button to start the load process.
The "Load results" dialog opens.



9. Click the "Finish" button.



Result

The download sequence is complete.

2.7.2 Load configuration into PC station

For production operation, in addition to the component configuration, you need to configure the communication links and, if necessary, the symbols of tags.

You have the following options for loading the configuration into the PC station:

- Loading via TIA Portal in online mode (see chapter 2.7.2.1)
- XDB import: Import XDB in the "Station Configuration Editor" (see 2.7.2.2)

2.7.2.1 Loading via TIA Portal in online mode

Online operation enables direct loading of the configuration into the network-connected PC station, or into the local PC station if that PC station is also used as an engineering PC.

Note

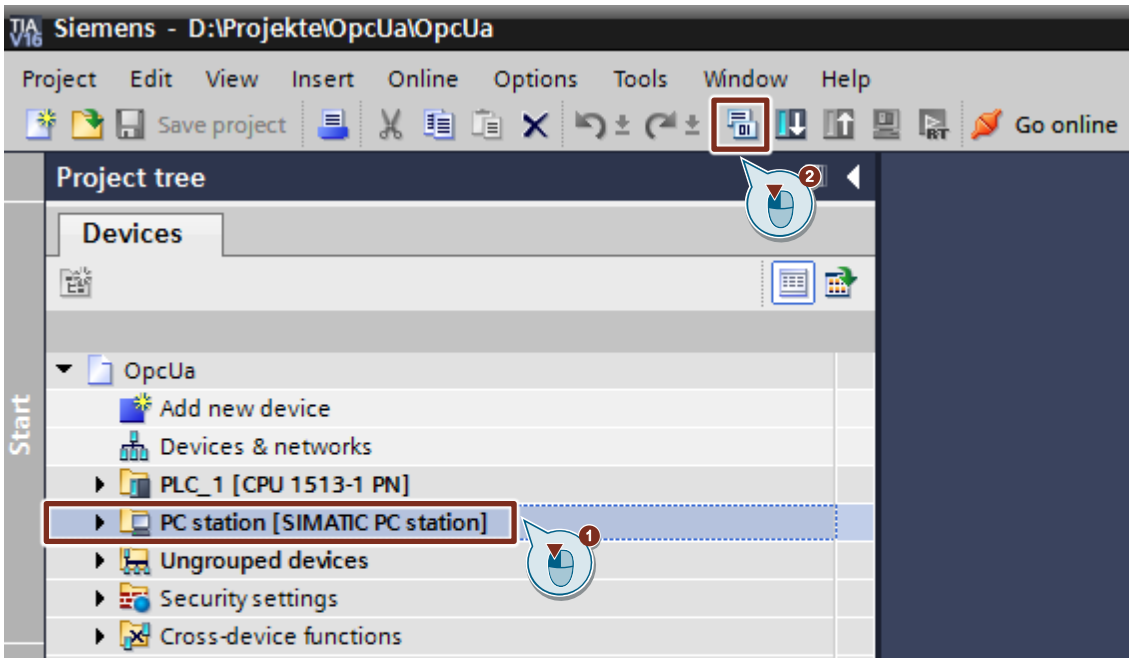
Loading via the TIA Portal in online mode only leads to successful installation of the communication services on your PC station if the component arrangement in the configuration is identical to the arrangement in the configuration data on the PC station.

Requirements

- Engineering PC and PC station are in the same subnet
- You set the same IP address and subnet mask for the PC station network adapter as you did in the hardware configuration (see chapter 2.2.1).

Compile

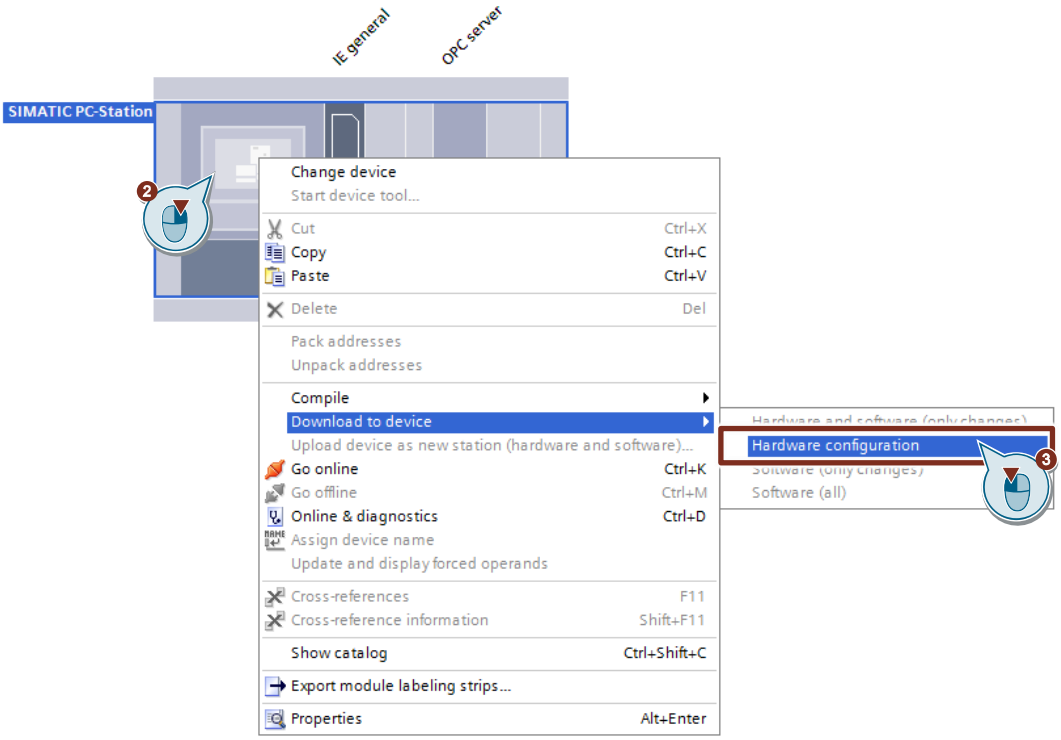
Figure 2-15



1. Select the PC station in the project tree.
2. Click on the "Compile" button in the function bar.

Downloading

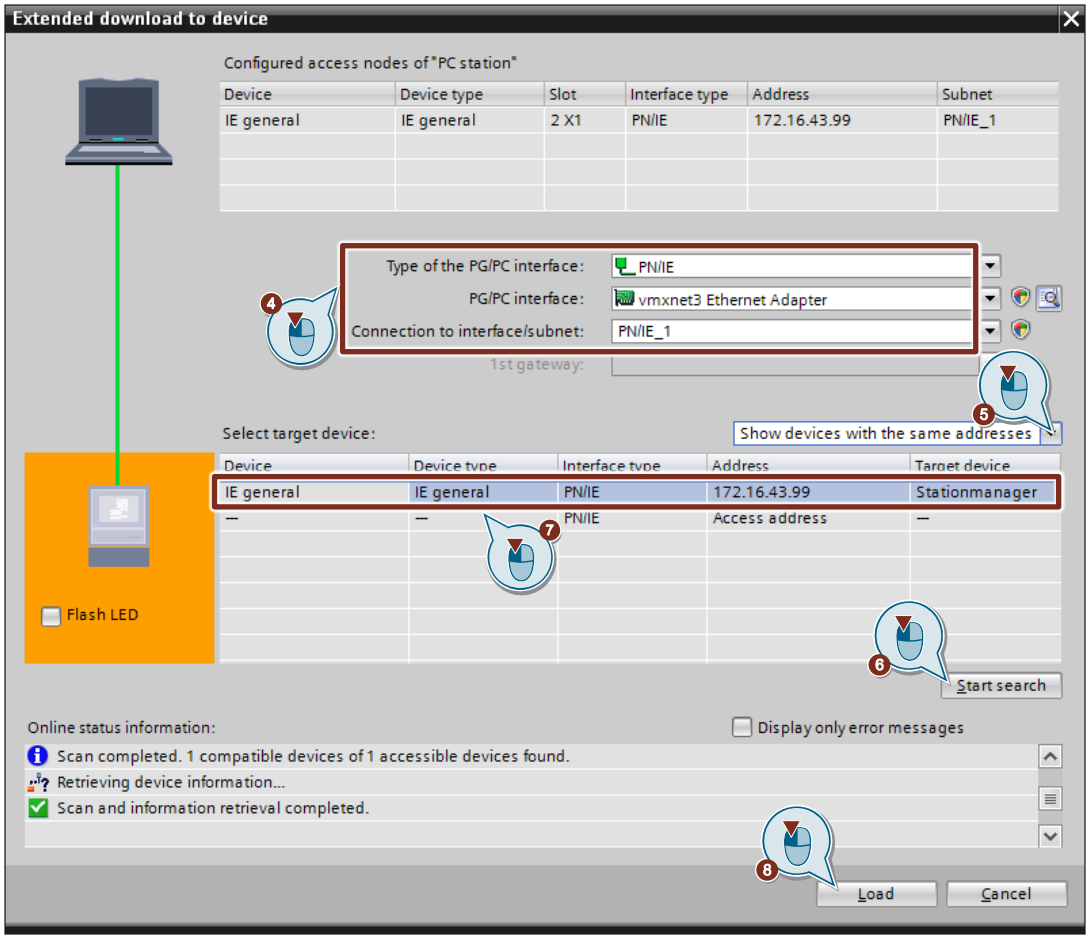
1. Open the "Device view" of the PC station.



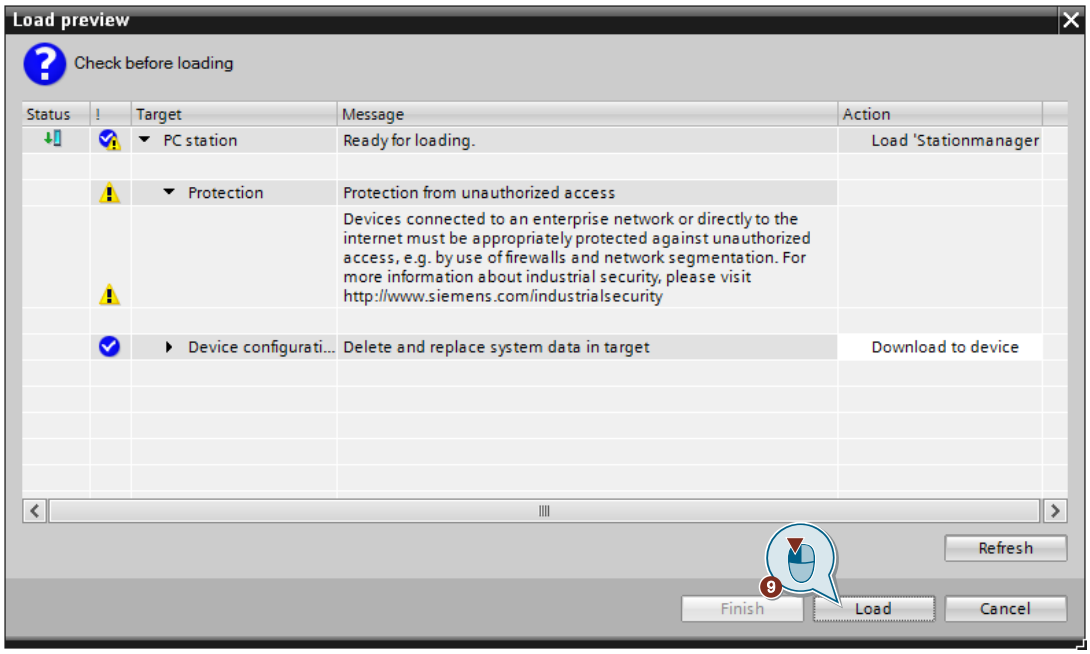
2. Right-click the PC station.
   The context menu opens.
3. Select the "Download to device > Hardware configuration" command.
   The "Extended download to device" or "Load preview" dialog will open.

Note The "Extended download to device" dialog only opens if the access path to the PC station must be reset.

4. In the "Extended download to device" dialog, make the following settings:
   - "Type of the PG/PC interface": PN/IE
   - "PG/PC interface": Network adapter of the PC station
   - "Connection to interface/subnet": Subnet of the PC station, e. g. PN/IE_1
5. Select the option "Show devices with the same addresses".
6. Click the "Start search" button.
7. Select the Station Manager as target device.
8. Click "Load".
   The "Load preview" dialog window opens.



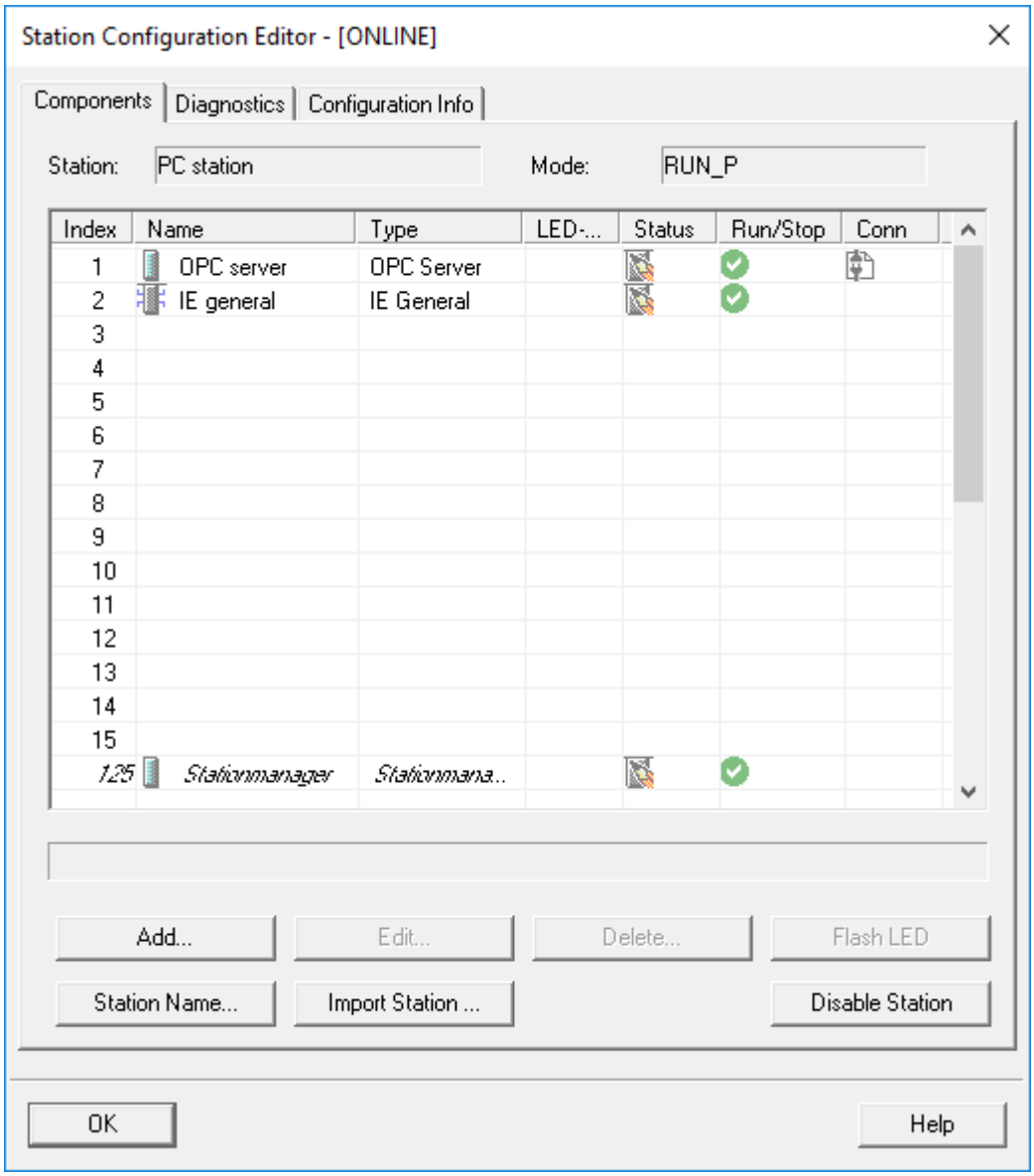
9. Click the "Load" button to start the load process.



Result

The configuration of the PC station was loaded successfully.

Figure 2-16



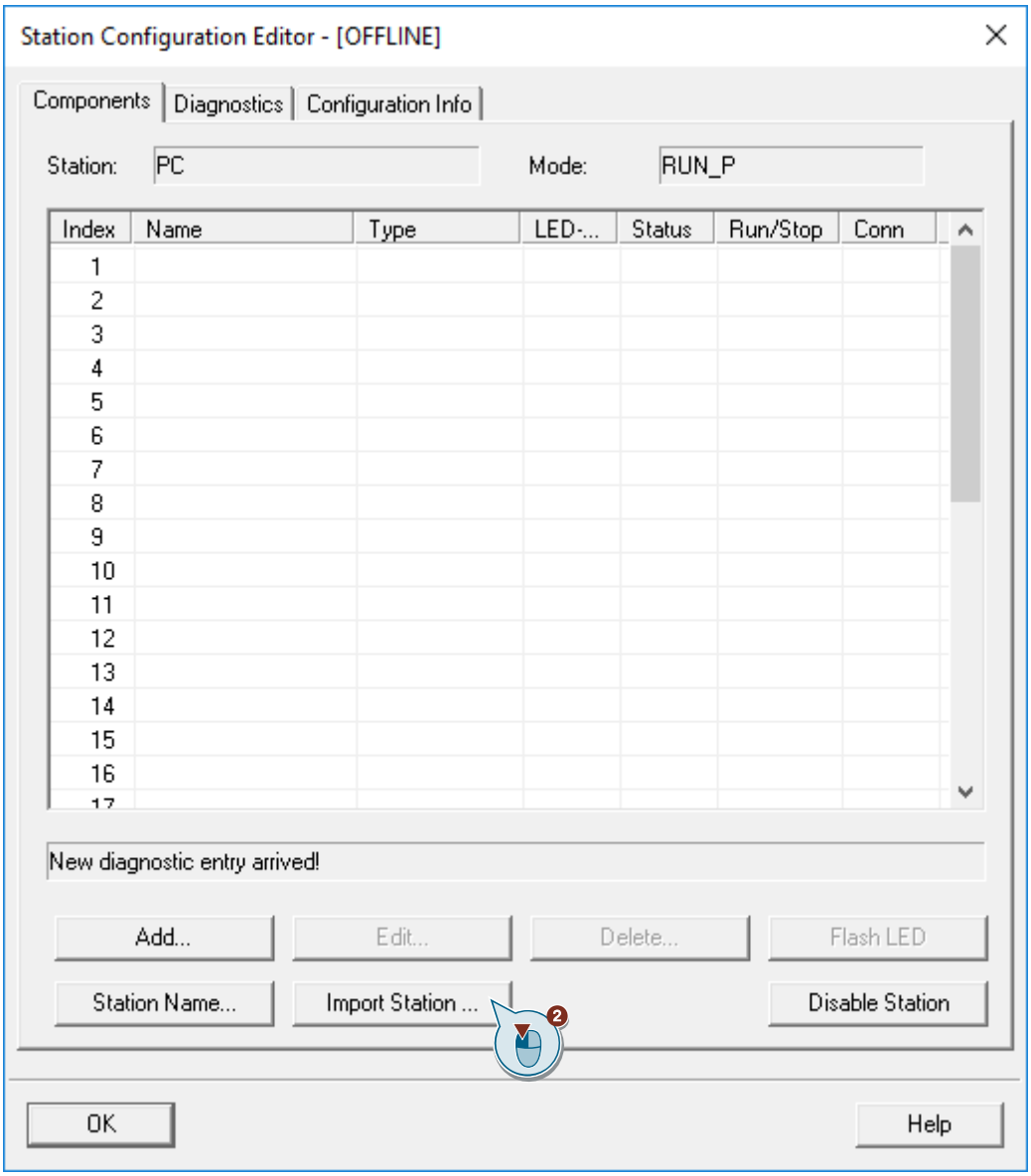
- The components are in "RUN" mode. This is shown with the icon in the "Run/Stop" column.
- The following status icon for the component shows that the configuration data have been loaded successfully.

Status icon	Meaning
	• The component is present and configured in the current configuration of the PC station. • The component is ready for operation!

- The configured S7 connection is loaded. This is shown with the icon in the "Conn" column.

2.7.2.2 XDB import: Import XDB in the "Station Configuration Editor"

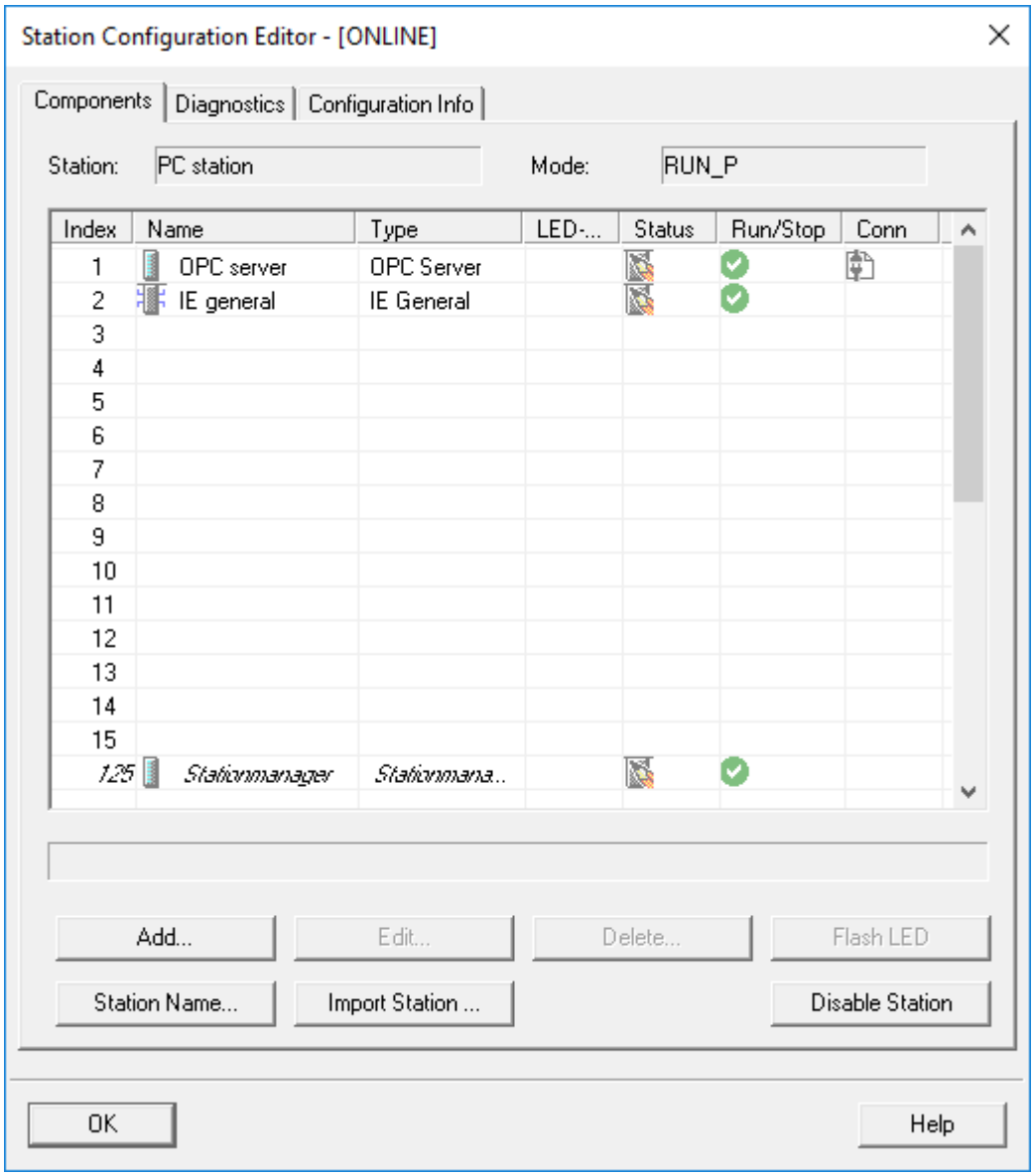
1. Open the "Station Configuration Editor".
2. Click on the "Import Station" button to load the configuration into the PC station.



Result

The configuration of the PC station was loaded successfully.

Figure 2-17



- The station has the same name as in the component image that you generated in TIA Portal in the "Device view" for the PC station.
- The components are in "RUN" mode. This is shown with the icon in the "Run/Stop" column.
- The following status icon for the component shows that the configuration data have been loaded successfully.

Status icon	Meaning
	• The component is present and configured in the current configuration of the PC station. • The component is ready for operation!

- The configured S7 connection is loaded. This is shown with the icon in the "Conn" column.

2.8 Operation

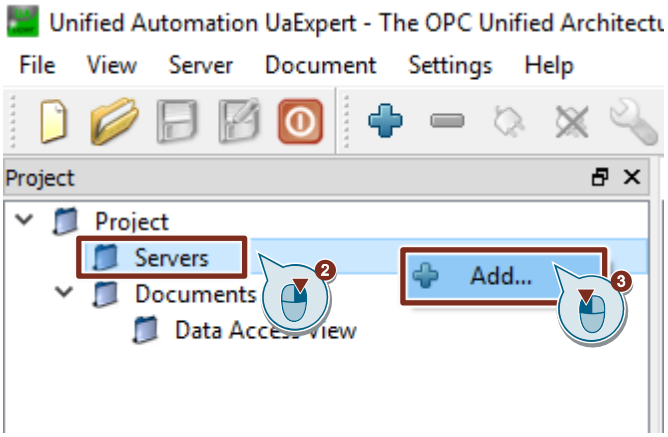
You need an OPC client to access the following objects of the S7OPT OPC UA Server:

- OPC UA event and alarm types
- Process values of archived S7 tags.

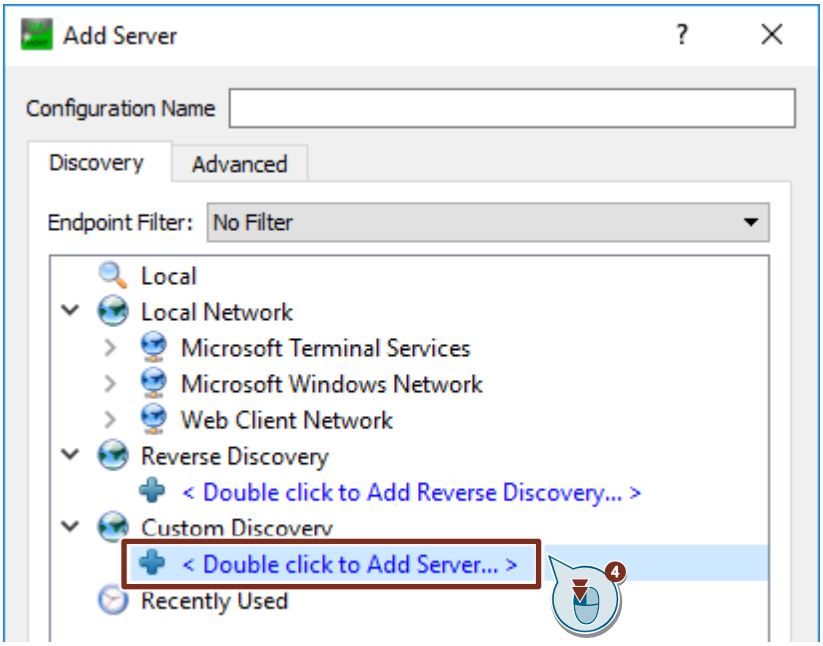
In this example we will use UA Expert as an OPC client.

Establish a connection from UA Expert to S7OPT OPC UA Server

1. Start UA Expert via the Windows start menu "Unified Automation > UaExpert".
2. In the "Project" window under "Project", right-click "Servers".
   The context menu opens.
3. Click "Add".
   The "Add Server" dialog opens.



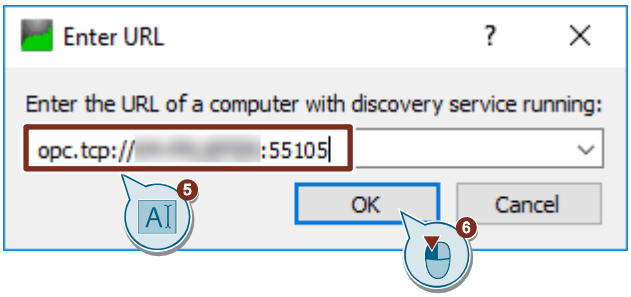
4. Under "Custom Discovery", double-click on "<Double click to Add Server>".
   The "Enter URL" dialog opens.



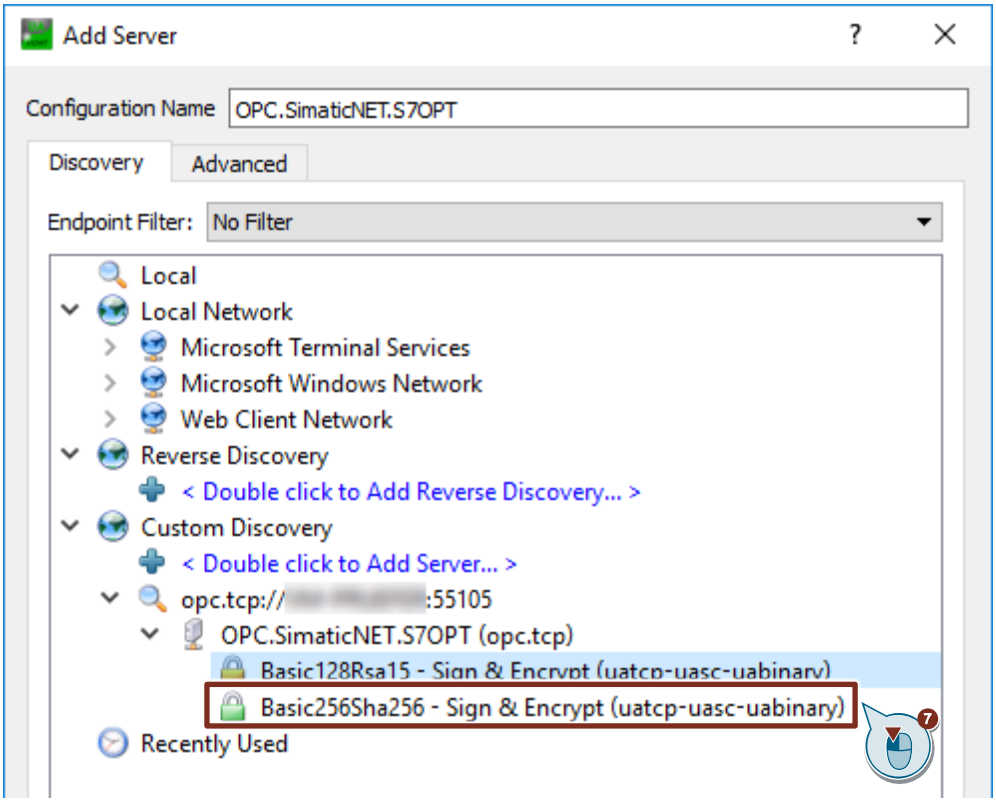
5. Enter the URL of the S7OPT OPC UA server.
   URL: opc.tcp://<PC name>:55105

Note Port 55105 is preset in the "Communication settings". The port can be changed.

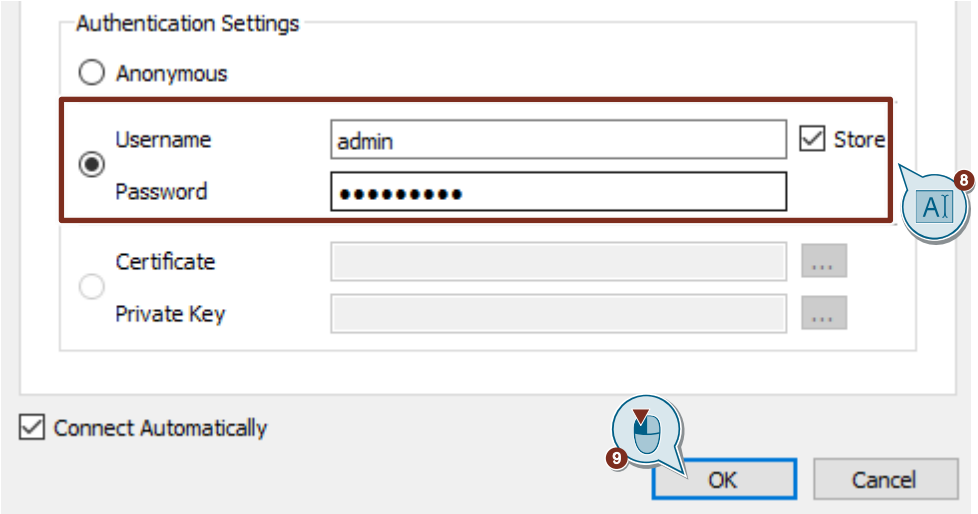
6. Click the "OK" button to apply the setting.



7. Under "Custom Discovery > [URL of the S7OPT OPC UA server] > OPC.SimaticNET.S7 (opc.tcp)", click one of the visible S7 connections.

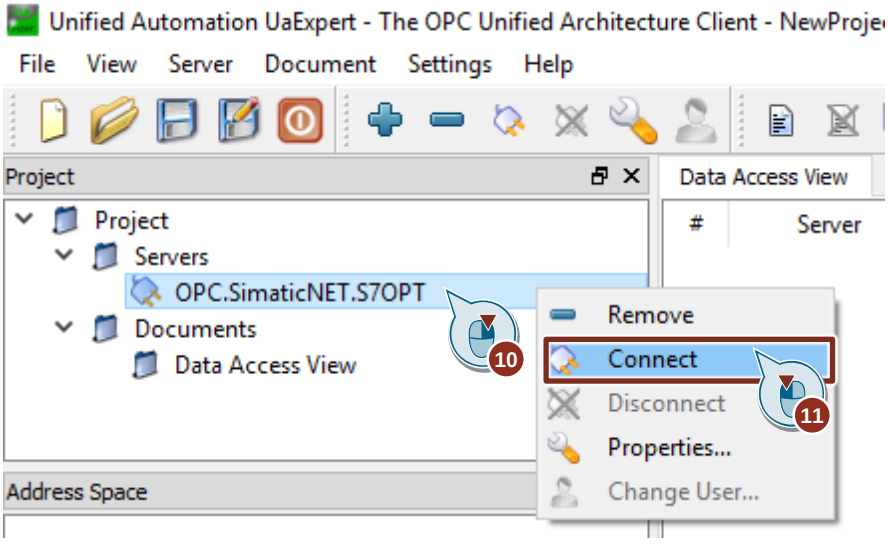


8. A user authentication with Windows login and password will be needed to establish the S7 connection.
9. Click "OK" to apply the settings.



Note It is possible to log in anonymously if you enabled the option "Allow anonymous logins to the OPC UA server" in the "Communication Settings".

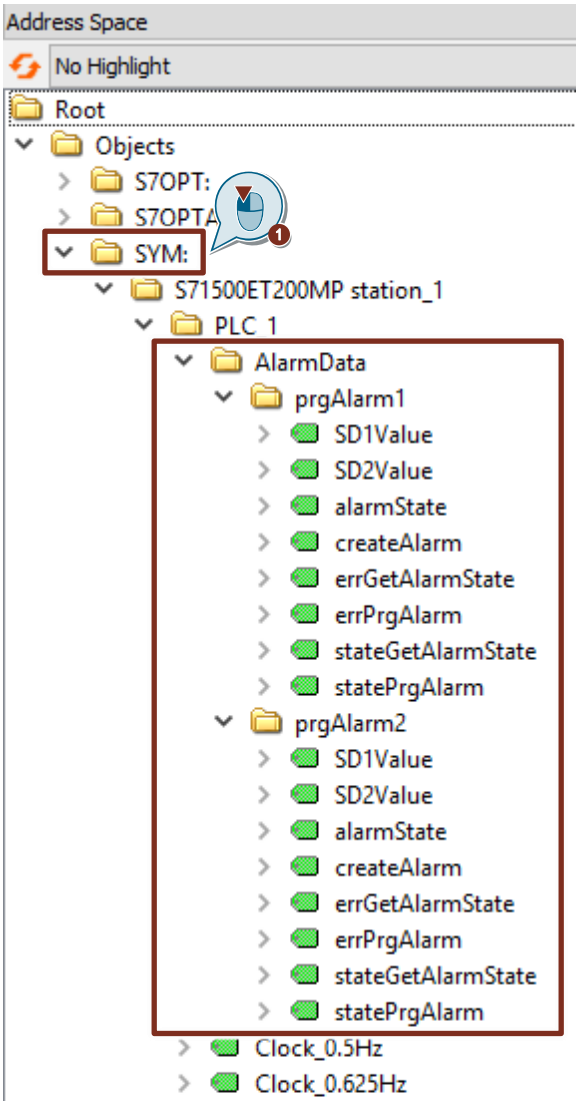
10. In the "Project" window under "Project > Servers", right-click the entry "OPC.SimaticNET.S7OPT".
    The context menu opens.
11. Click "Connect" in order to establish the connection to the SIMATIC NET S7OPT OPC UA server.



Note If only secured connections are allowed, it is necessary to accept the certificate of the OPC client "UA Expert" in the "Communication settings" (see Figure 2-7).

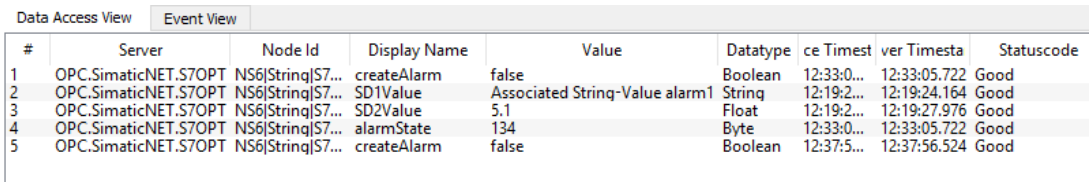
Access the S7 tags in the S7 CPU via symbol names

1. In the "Address Space" window, navigate to "Root > Objects > SYM".
   A symbol table with the existing S7 tags will be displayed.



2. Drag and drop to add the following S7 tags from the object "prgAlarm1" to the "Data Access View" of UA Expert.
   - SD1Value
   - SD2Value
   - alarmState
   - createAlarm

3. Drag and drop to add the S7 tag "createAlarm" from the object "prgAlarm2" to the "Data Access View" of UA Expert.

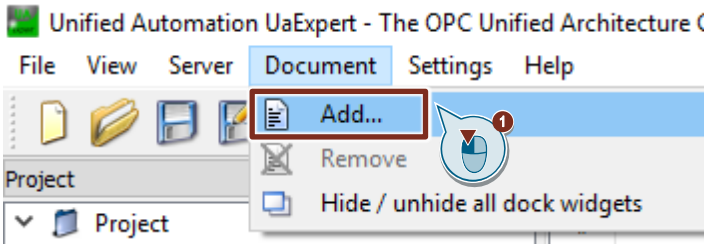


#	Server	Node Id	Display Name	Value	Datatype	ce Timest	ver Timesta	Statuscode
1	OPC.SimaticNET.S7OPT	NS6|String|S7...	createAlarm	false	Boolean	12:33:0...	12:33:05.722	Good
2	OPC.SimaticNET.S7OPT	NS6|String|S7...	SD1Value	Associated String-Value alarm1	String	12:19:2...	12:19:24.164	Good
3	OPC.SimaticNET.S7OPT	NS6|String|S7...	SD2Value	5.1	Float	12:19:2...	12:19:27.976	Good
4	OPC.SimaticNET.S7OPT	NS6|String|S7...	alarmState	134	Byte	12:33:0...	12:33:05.722	Good
5	OPC.SimaticNET.S7OPT	NS6|String|S7...	createAlarm	false	Boolean	12:37:5...	12:37:56.524	Good

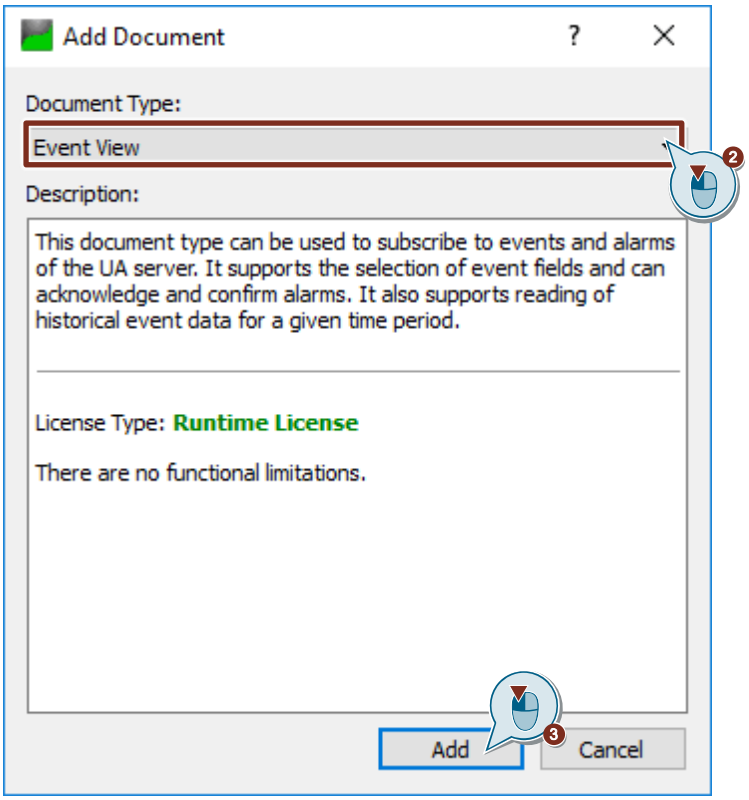
Set up the "Event View"

The "Event View" is used to display the events reported by the S7OPT OPC UA server. Event messages requiring acknowledgement can be acknowledged in the "Event View".

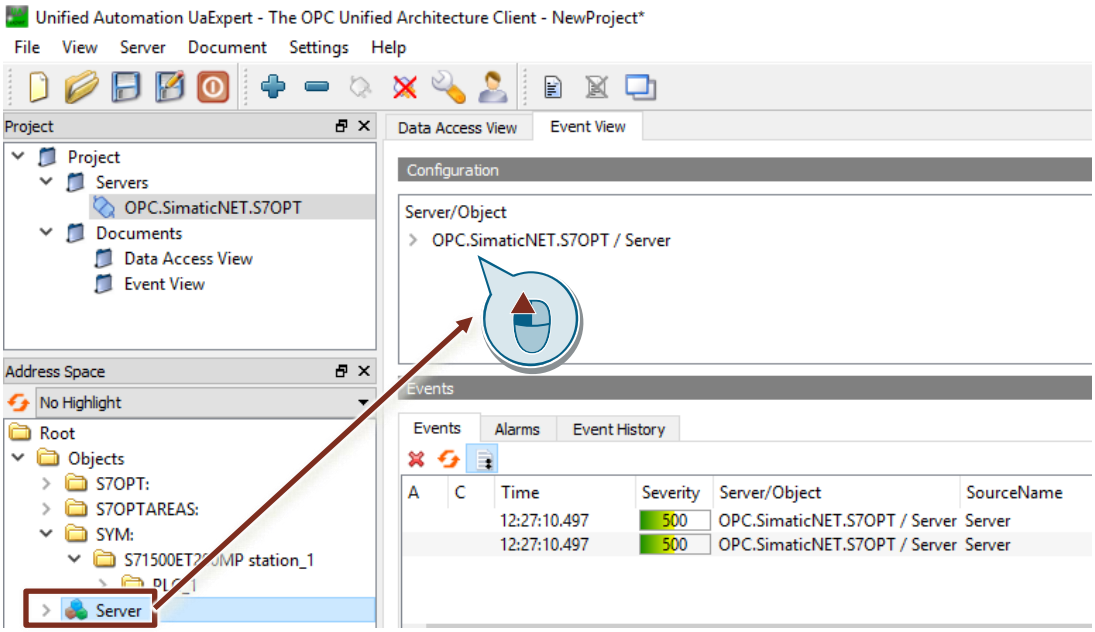
1. Click on "Add" in the "Document" menu.
   The "Add Document" dialog opens.



2. Select the document type "Event View".
3. Click the "Add" button.
   The "Event View" will be added to UA Expert.



4. Drag & drop the server from the "Address Space" window into the "Configuration" area of the "Event View".
   The server responds with two initialization events.

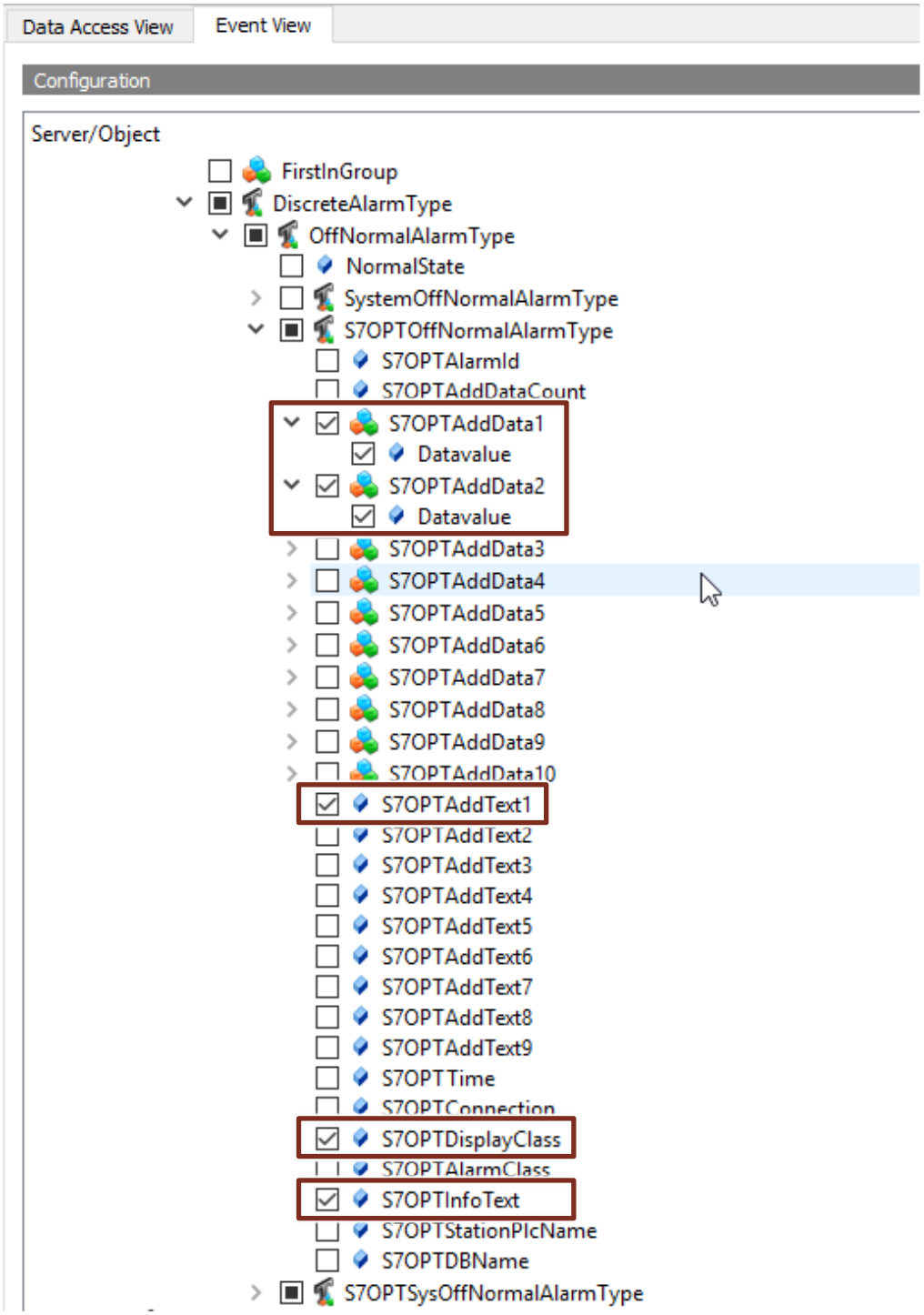


Display attributes of the program alarm via the S7OPT event type "S7OPTOffNormalAlarmType"

To display the configured attributes of the program alarm via the S7OPT event type "S7OPTOffNormalAlarmType", make the following settings:

1. In the "Configuration" section of the "Event View", navigate to the node "Condition Type > AcknowledgeableConditionType > AlarmConditonType > DiscreteAlarmType > OffNormalAlarmType > S7OPTOffNormalAlarmType".
2. Select the following attributes:
   - "S7OPTAddData1 > Datavalue" (associated value SD_1)
   - "S7OPTAddData2 > Datavalue" (associated value SD_2)
   - "S7OPTAddText1" (additional text 1)
   - "S7OPTDisplayClass" (display class of the alarm)
   - "S7OPTInfoText" (additional info text)

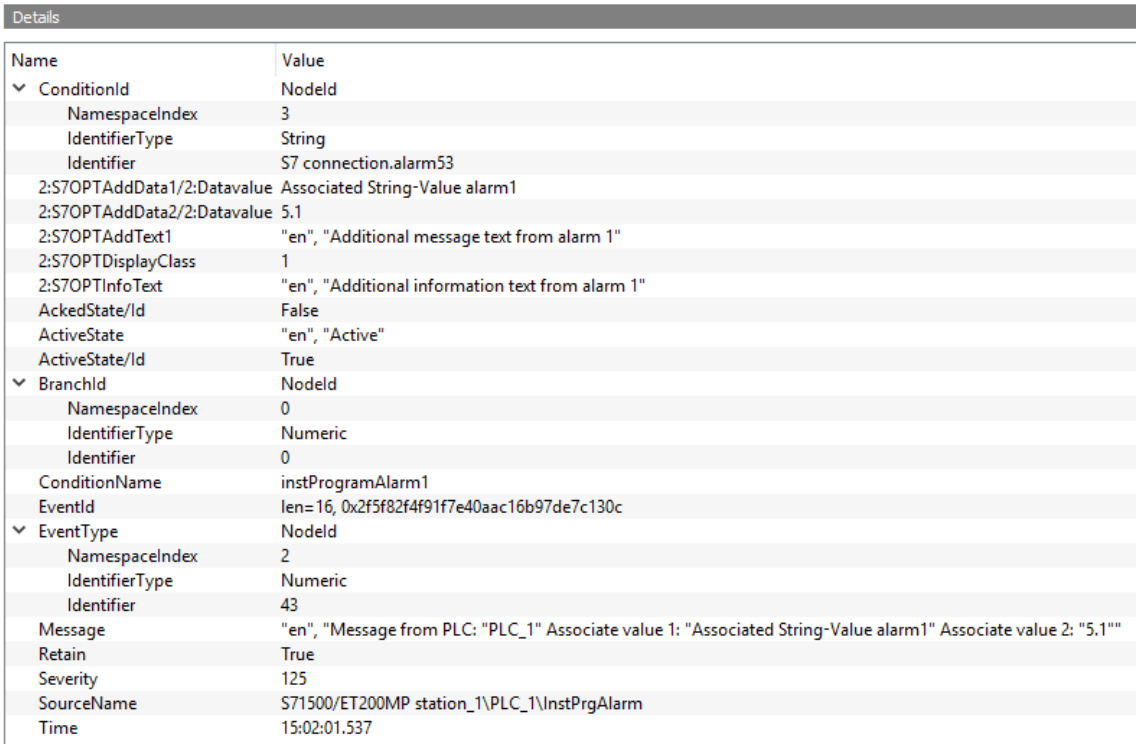
Figure 2-18



Result

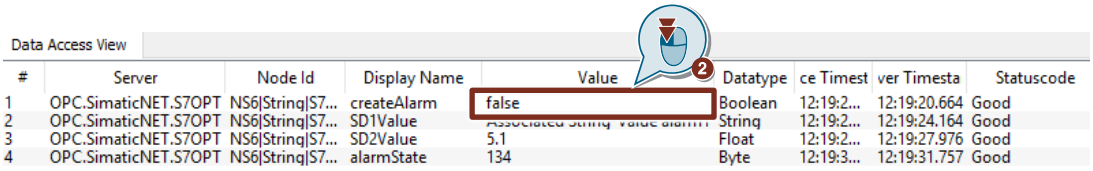
When a program alarm is triggered, the selected attributes will be displayed in the "Details" section.

Figure 2-19

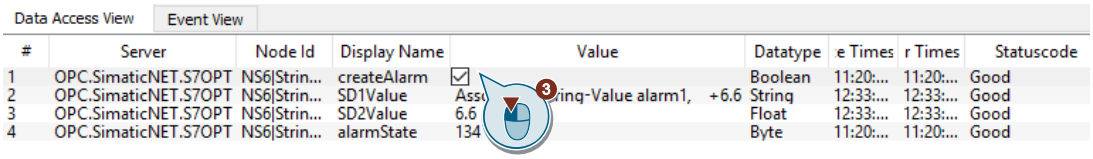


Enable a program alarm with required acknowledgement in the PLC

1. Open the "Data Access View".
2. In the "Value" column, double-click on the tag "createAlarm" of the object "prgAlarm1".

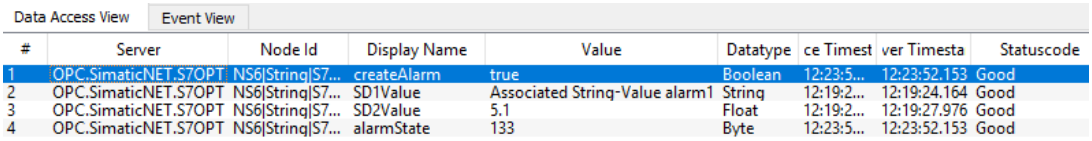


3. Set the tag "createAlarm" of the "prgAlarm1" object to the value "true".



Result

- The value of the "createAlarm" tag of the object "prgAlarm1" changes to "true".
- The value of the "alarmState" tag of the object "prgAlarm1" changes from "134" to "133".
- The values "Good" appear in the "Statuscode" column.



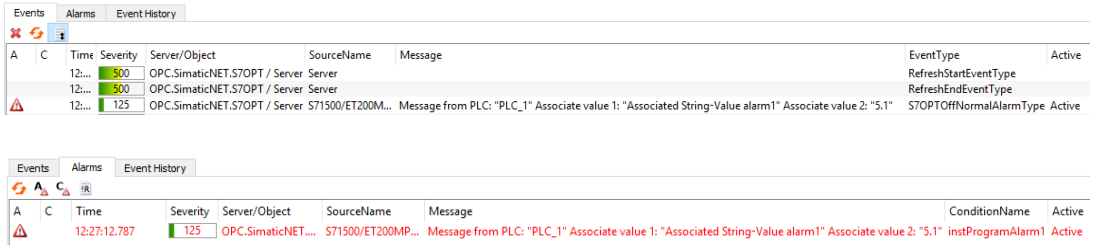
Data Access View | Event View

#	Server	Node Id	Display Name	Value	Datatype	ce Timest	ver Timesta	Statuscode
1	OPC.SimaticNET.S7OPT	NS6|String|S7...	createAlarm	true	Boolean	12:23:5...	12:23:52.153	Good
2	OPC.SimaticNET.S7OPT	NS6|String|S7...	SD1Value	Associated String-Value alarm1	String	12:19:2...	12:19:24.164	Good
3	OPC.SimaticNET.S7OPT	NS6|String|S7...	SD2Value	5.1	Float	12:19:2...	12:19:27.976	Good
4	OPC.SimaticNET.S7OPT	NS6|String|S7...	alarmState	133	Byte	12:23:5...	12:23:52.153	Good

- With a rising edge in the tag "createAlarm", a program alarm is activated in the PLC and sent to the S7OPT OPC UA server.

Receive program alarm with required acknowledgement in the "Event View"

1. Open the "Event View".
   The program alarm (with required acknowledgement) of S7OPT event type "S7OPTOffNormalAlarmType" with the status "Active" and "acknowledgement required (alarmState = 133)" will appear in the "Events" and "Alarms" tabs.



Events | Alarms | Event History

A	C	Time	Severity	Server/Object	SourceName	Message	EventType	Active
		12:...	500	OPC.SimaticNET.S7OPT / Server	Server		RefreshStartEventType	
		12:...	500	OPC.SimaticNET.S7OPT / Server	Server		RefreshEndEventType	
⚠		12:...	125	OPC.SimaticNET.S7OPT / Server	S71500/ET200M...	Message from PLC: "PLC_1" Associate value 1: "Associated String-Value alarm1" Associate value 2: "5.1"	S7OPTOffNormalAlarmType	Active

Events | Alarms | Event History

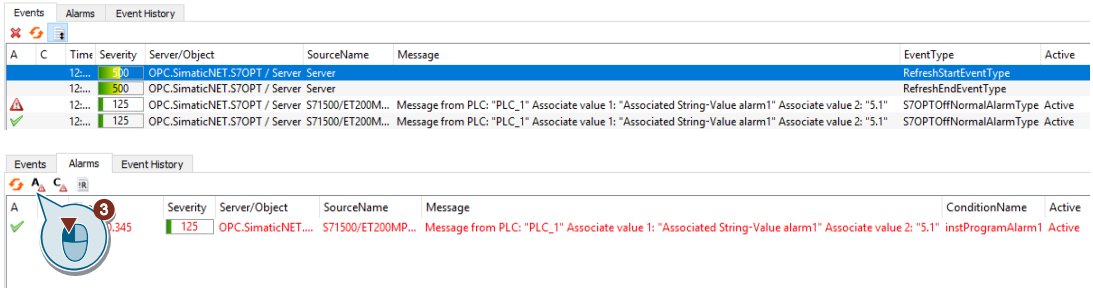
A	C	Time	Severity	Server/Object	SourceName	Message	ConditionName	Active
⚠		12:27:12.787	125	OPC.SimaticNET....	S71500/ET200MP...	Message from PLC: "PLC_1" Associate value 1: "Associated String-Value alarm1" Associate value 2: "5.1"	instProgramAlarm1	Active

2. Select the program alarm with required acknowledgement S7OPT event type "S7OPTOffNormalAlarmType" in the "Events" or "Alarms" tab.
   The configured attributes of the program alarm appear in the "Details" section.

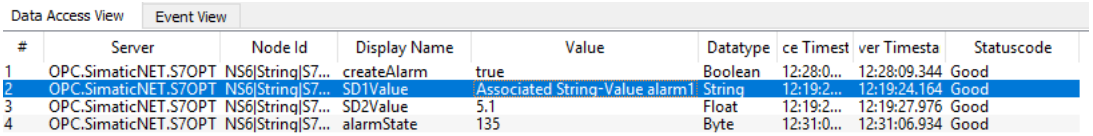
Details

Name	Value
ConditionId	NodeId
NamespaceIndex	3
IdentifierType	String
Identifier	S7 connection.alarm53
2:S7OPTAddData1/2:Datavalue	Associated String-Value alarm1
2:S7OPTAddData2/2:Datavalue	5.1
2:S7OPTAddText1	"en", "Additional message text from alarm 1"
2:S7OPTDisplayClass	1
2:S7OPTInfoText	"en", "Additional information text from alarm 1"
AckedState/Id	False
ActiveState	"en", "Active"
ActiveState/Id	True
BranchId	NodeId
NamespaceIndex	0
IdentifierType	Numeric
Identifier	0
ConditionName	instProgramAlarm1
EventId	len=16, 0x2f5f82f4f91f7e40aac16b97de7c130c
EventType	NodeId
NamespaceIndex	2
IdentifierType	Numeric
Identifier	43
Message	"en", "Message from PLC: "PLC_1" Associate value 1: "Associated String-Value alarm1" Associate value 2: "5.1""
Retain	True
Severity	125
SourceName	S71500/ET200MP station_1\PLC_1\InstPrgAlarm
Time	15:02:01.537

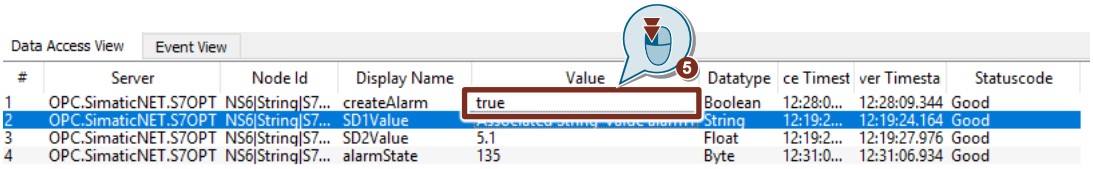
3. In the "Alarms" tab, click the "Acknowledge All" icon.
   In the tabs "Events" and "Alarms", the program alarm with required acknowledgement and of S7OPT event type "S7OPTOffNormalAlarmType" will appear with the state "Active" and "acknowledged (alarmState = 135)".



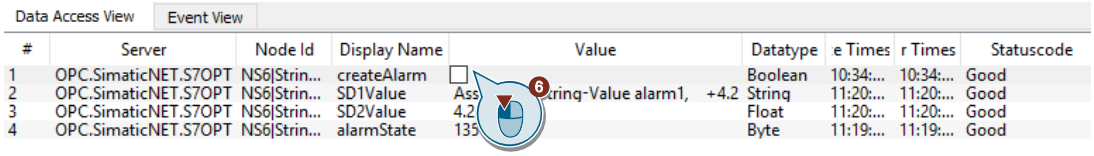
4. Open the "Data Access View" and check whether the "alarmState" tag of the object "prgAlarm1" has the value "135".



5. In the "Value" column, double-click on the tag "createAlarm" of the object "prgAlarm1".

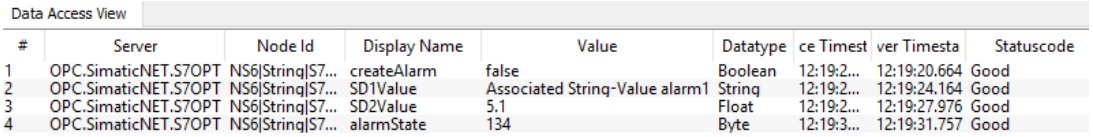


6. Reset the tag "createAlarm" of the "prgAlarm1" object to the value "false".

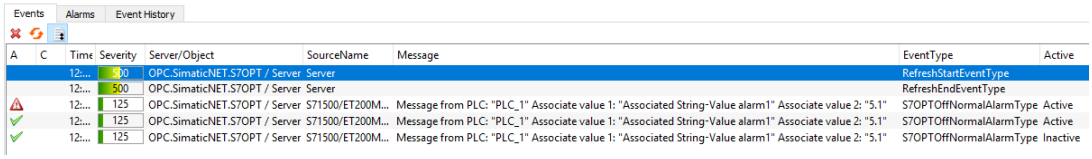


Result

- In the "Data Access View", the value of the tag "createAlarm" of the object "prgAlarm1" changes to "false".
- In the "Data Access View", the value of the tag "alarmState" of the object "prgAlarm1" changes from "135" to "134".

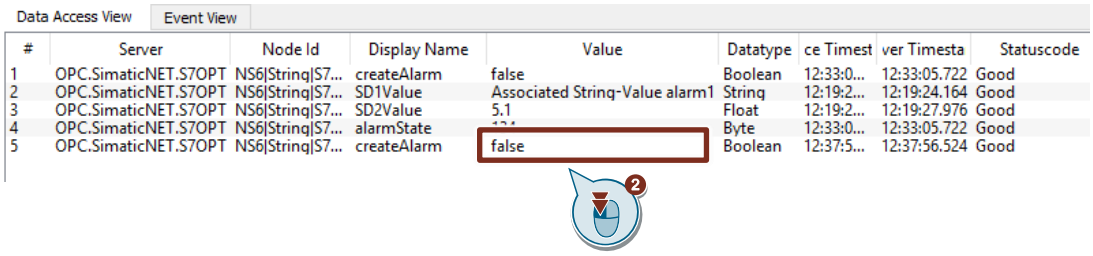


- UA Expert has received a new alarm state change for this object. In the "Event View", the alarm has changed to the state "Inactive" and "acknowledged (alarmState = 134)".

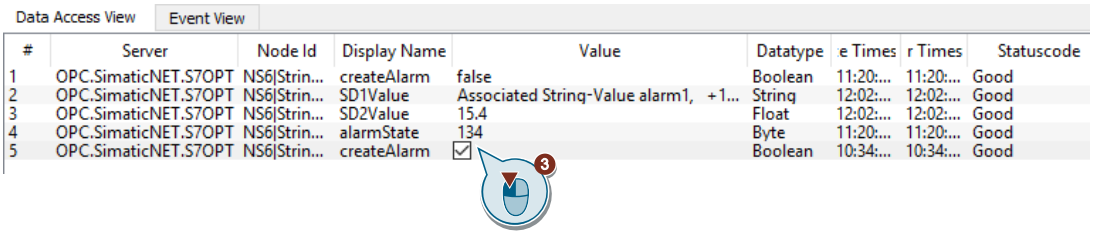


Enable information-only program alarm in the PLC

1. Open the "Data Access View".
2. In the "Value" column, double-click on the "createAlarm" tag of the object "prgAlarm2".

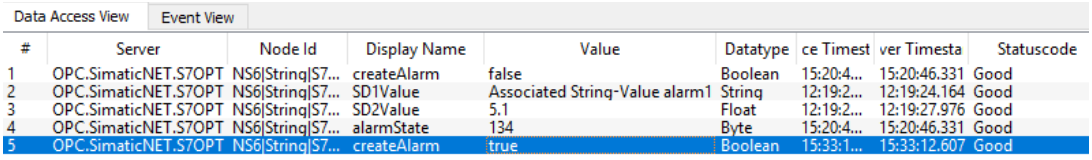


3. In the Data Access View, set the tag "createAlarm" of the object "prgAlarm2" to the value "true".



Result

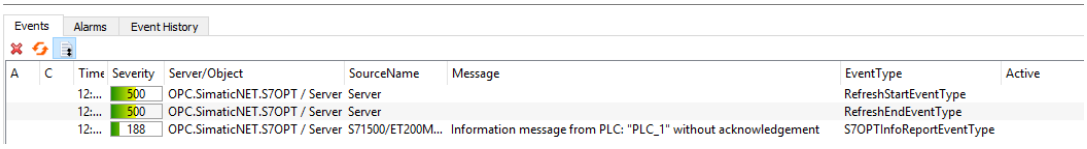
- The value of the "createAlarm" tag of the object "prgAlarm2" changes to "true".
- The values "Good" appear in the "Statuscode" column.



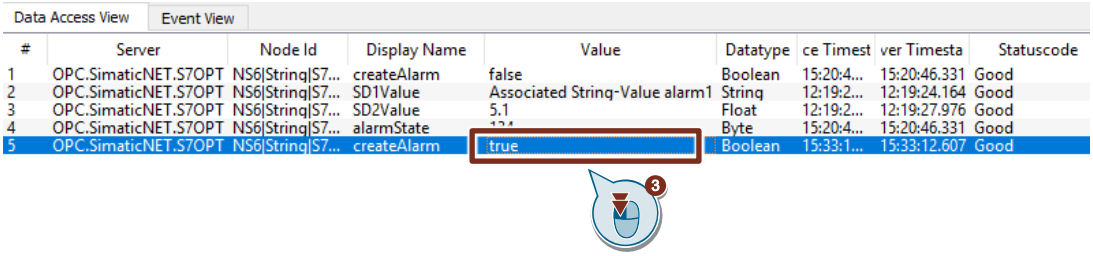
- With a rising edge of the tag "createAlarm" a program alarm is activated in the PLC and sent to the S7OPT OPC UA server.

Receive information-only program alarm in the "Event View"

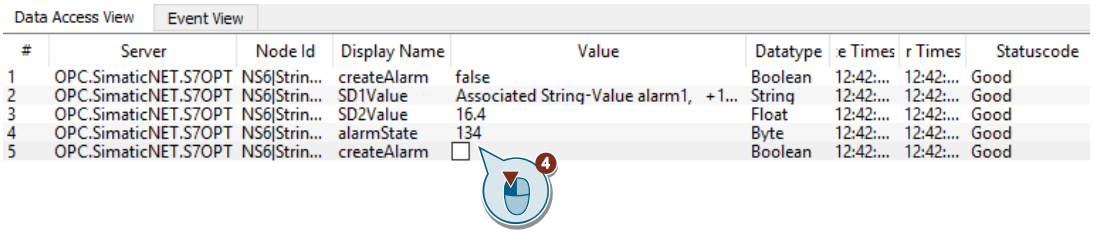
1. Open the "Event View".
   In the "Events" tab, the information-only program alarm will be shown by the S7OPT event type "S7OPTInfoReportEventType".



2. Open the "Data Access View".
3. In the "Value" column, double-click on the "createAlarm" tag of the object "prgAlarm2".

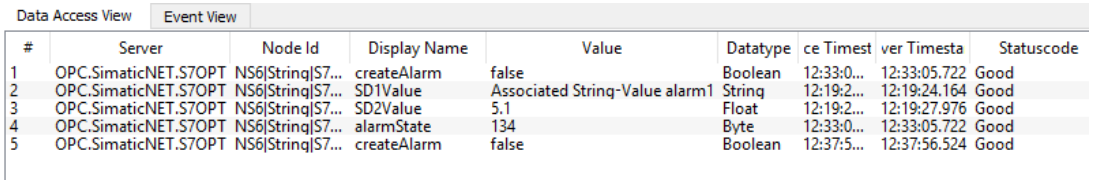


4. Reset the tag "createAlarm" of the object "prgAlarm2" to the value "false".



Result

- In the "Data Access View", the value of the tag "createAlarm" of the object "prgAlarm2" changes to "false".



- No more program alarm will be generated for the S7OPT event type "S7OPTInfoReportEventType".

Set up the "History Trend View"

The "History Trend View" is used to graphically display the process values of the S7 tags archived by the S7OPT OPC UA server.

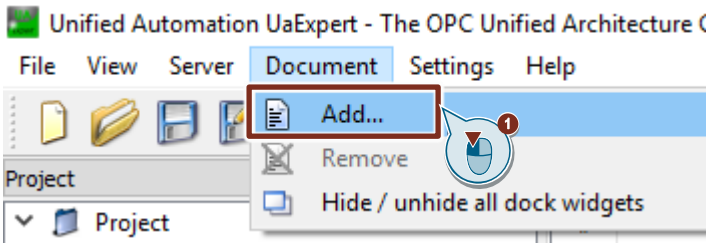
In this example, the following S7 tags are stored in the archive:

- "SD1Value" from the data structure "prgAlarm1" (associated value 1)
- "SD2Value" from the data structure "prgAlarm1" (associated value 2)

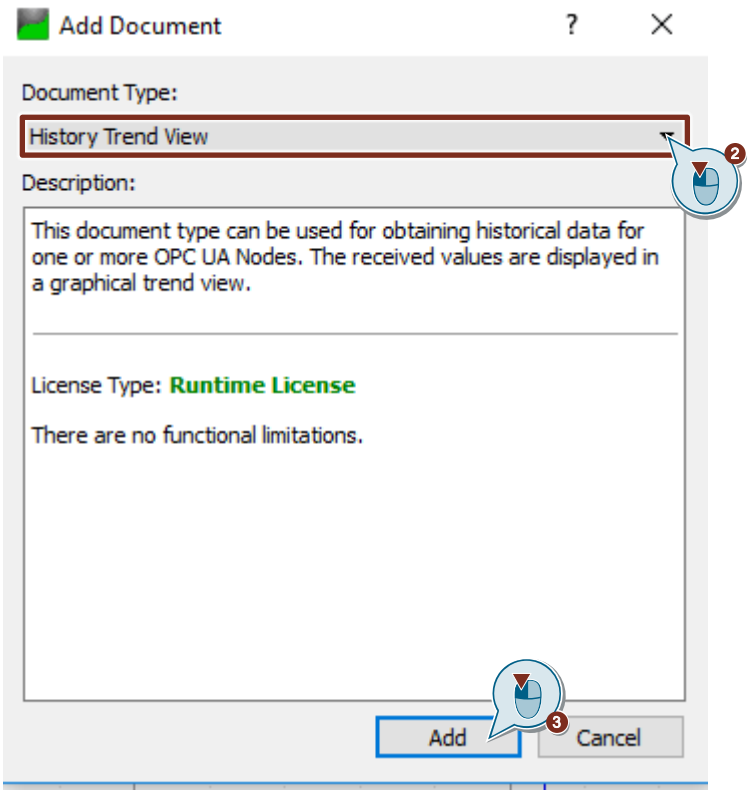
The timestamp and the quality characteristic of the S7 tags are stored together with the process value.

With the "History Trend View", it is possible to have read access to the values of the S7 tags stored in the archive.

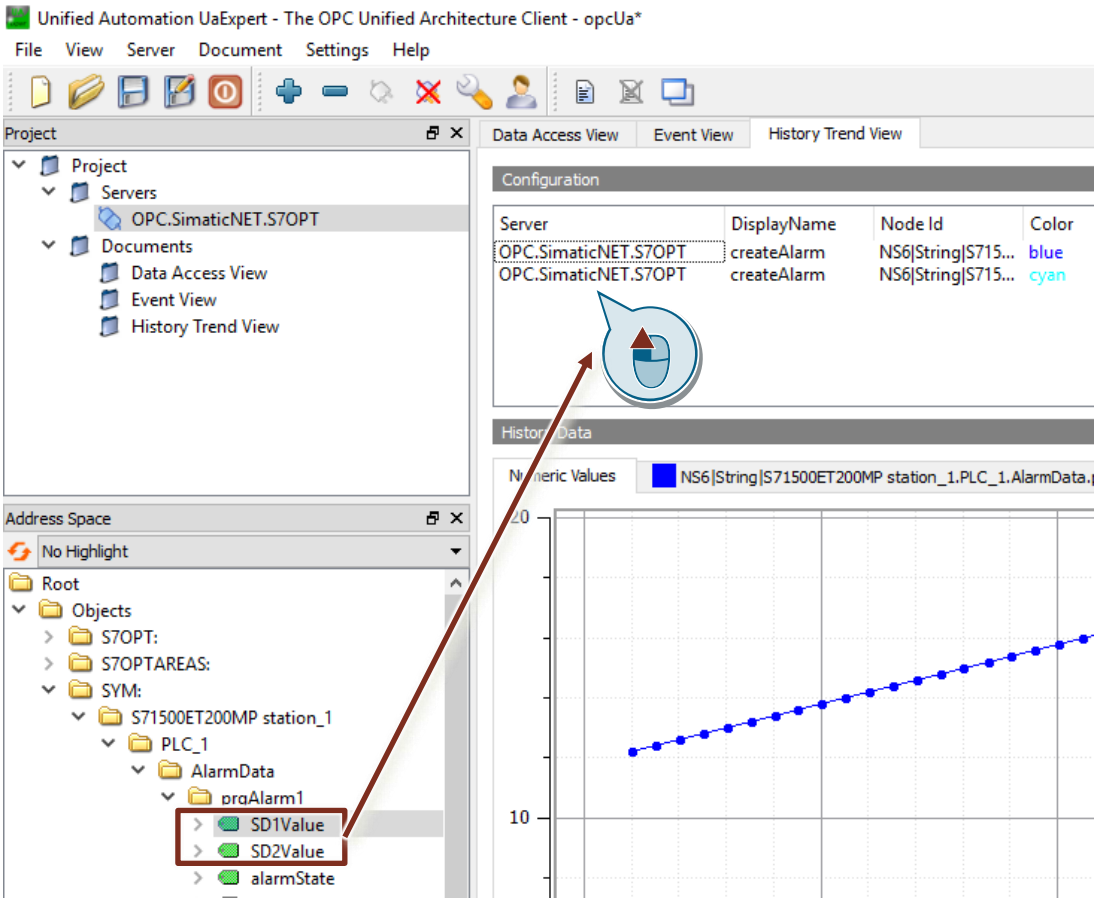
1. Click on "Add" in the "Document" menu.
   The "Add Document" dialog opens.



2. Select the document type "History Trend View".
3. Click the "Add" button.
   The "History Trend View" will be added in UA Expert.



4. Drag and drop to add the following S7 tags of the object "prgAlarm1" from the "Address Space" window to the "Configuration" section of the "History Trend View".
   - SD1Value
   - SD2Value



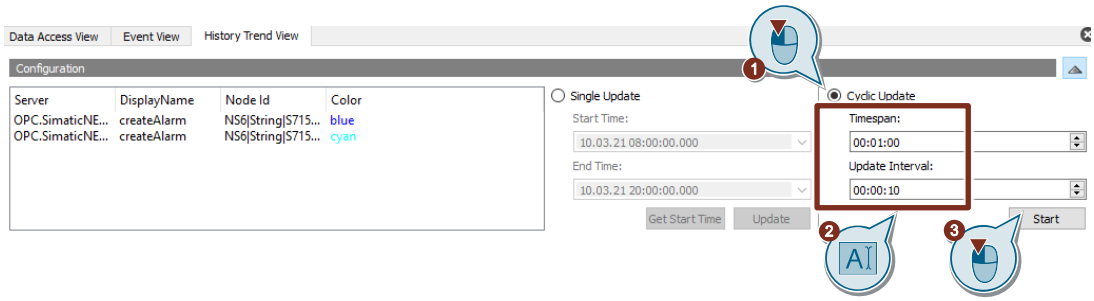
Display process values of archived S7 tags in the "History Trend View"

The following options are available for read access to the S7 tags stored in the archive:

- Single Update:
  The displayed range is defined by the time of start and end.
- Cyclic Update:
  The time range to be displayed is specified directly as the duration and the data is retrieved at an adjustable interval.

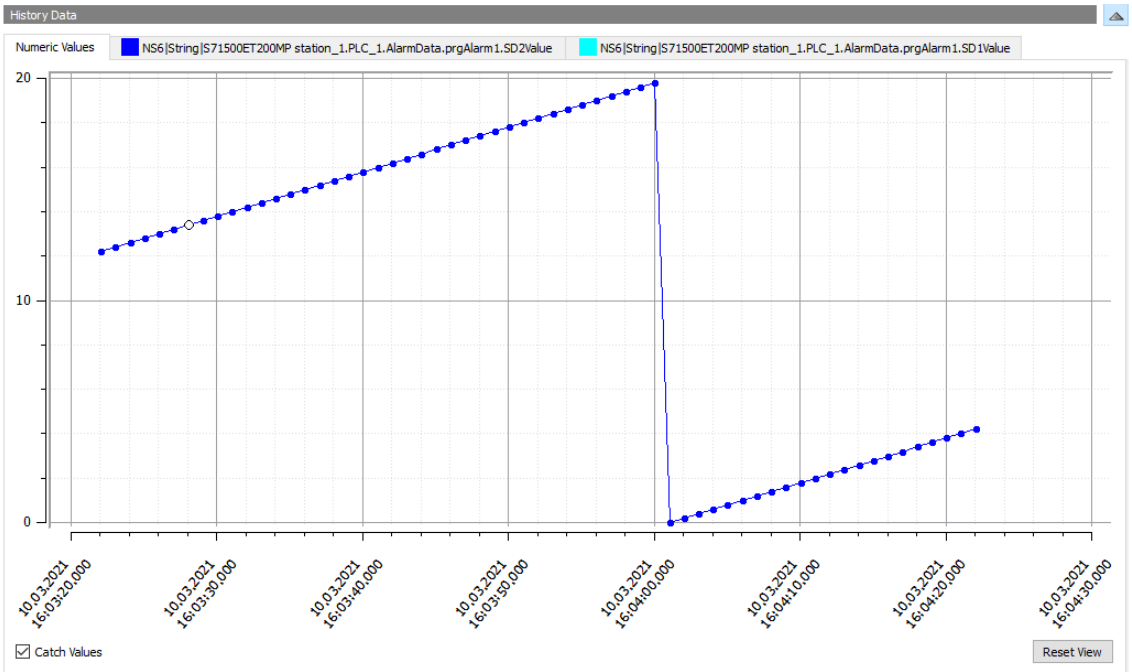
Cyclic Update

1. Enable the "Cyclic Update" function.
2. Enter the time span and update interval, for example:
   - "Timespan": 1 min
     The values that have been stored within 1 minute up to the current time are displayed.
   - "Update Interval": 10s
     The display of the values is updated every 10s.
3. Click the "Start" button to start the cyclic update.



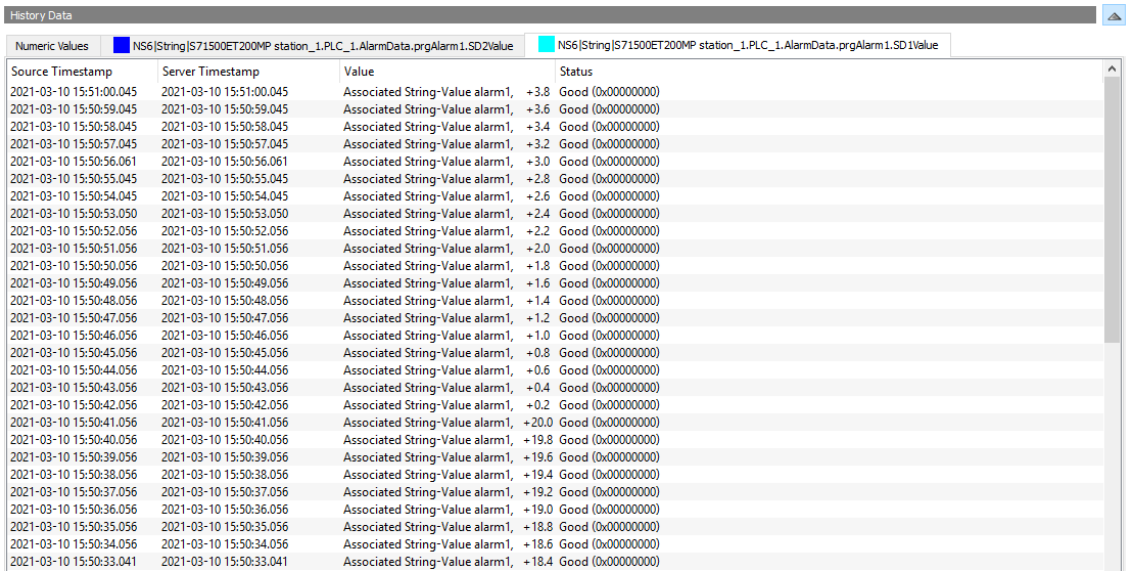
The values of the S7 tag "SD2Value" of the data type "Real" are displayed graphically in the "History Data" section of the "Numeric Values" tab.

Figure 2-20



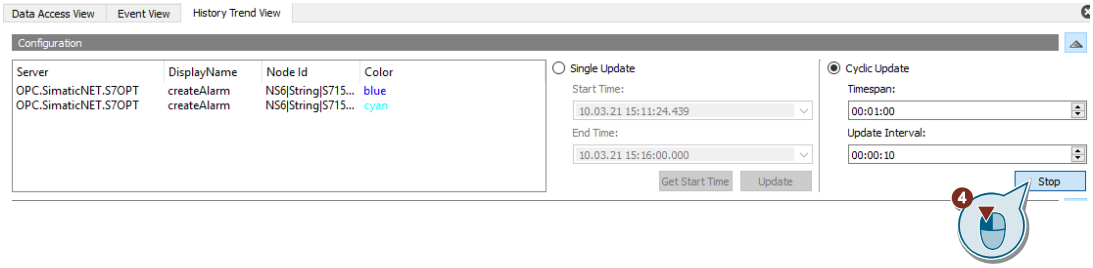
The values of the S7 tag "SD1Value" of the data type "String" are displayed in tabular form in the "History data" section.

Figure 2-21



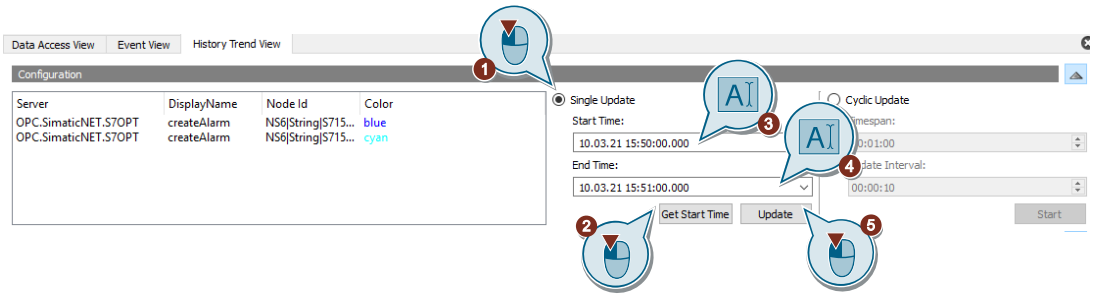
Source Timestamp	Server Timestamp	Value	Status
2021-03-10 15:51:00.045	2021-03-10 15:51:00.045	Associated String-Value alarm1, +3.8	Good (0x00000000)
2021-03-10 15:50:59.045	2021-03-10 15:50:59.045	Associated String-Value alarm1, +3.6	Good (0x00000000)
2021-03-10 15:50:58.045	2021-03-10 15:50:58.045	Associated String-Value alarm1, +3.4	Good (0x00000000)
2021-03-10 15:50:57.045	2021-03-10 15:50:57.045	Associated String-Value alarm1, +3.2	Good (0x00000000)
2021-03-10 15:50:56.061	2021-03-10 15:50:56.061	Associated String-Value alarm1, +3.0	Good (0x00000000)
2021-03-10 15:50:55.045	2021-03-10 15:50:55.045	Associated String-Value alarm1, +2.8	Good (0x00000000)
2021-03-10 15:50:54.045	2021-03-10 15:50:54.045	Associated String-Value alarm1, +2.6	Good (0x00000000)
2021-03-10 15:50:53.050	2021-03-10 15:50:53.050	Associated String-Value alarm1, +2.4	Good (0x00000000)
2021-03-10 15:50:52.056	2021-03-10 15:50:52.056	Associated String-Value alarm1, +2.2	Good (0x00000000)
2021-03-10 15:50:51.056	2021-03-10 15:50:51.056	Associated String-Value alarm1, +2.0	Good (0x00000000)
2021-03-10 15:50:50.056	2021-03-10 15:50:50.056	Associated String-Value alarm1, +1.8	Good (0x00000000)
2021-03-10 15:50:49.056	2021-03-10 15:50:49.056	Associated String-Value alarm1, +1.6	Good (0x00000000)
2021-03-10 15:50:48.056	2021-03-10 15:50:48.056	Associated String-Value alarm1, +1.4	Good (0x00000000)
2021-03-10 15:50:47.056	2021-03-10 15:50:47.056	Associated String-Value alarm1, +1.2	Good (0x00000000)
2021-03-10 15:50:46.056	2021-03-10 15:50:46.056	Associated String-Value alarm1, +1.0	Good (0x00000000)
2021-03-10 15:50:45.056	2021-03-10 15:50:45.056	Associated String-Value alarm1, +0.8	Good (0x00000000)
2021-03-10 15:50:44.056	2021-03-10 15:50:44.056	Associated String-Value alarm1, +0.6	Good (0x00000000)
2021-03-10 15:50:43.056	2021-03-10 15:50:43.056	Associated String-Value alarm1, +0.4	Good (0x00000000)
2021-03-10 15:50:42.056	2021-03-10 15:50:42.056	Associated String-Value alarm1, +0.2	Good (0x00000000)
2021-03-10 15:50:41.056	2021-03-10 15:50:41.056	Associated String-Value alarm1, +20.0	Good (0x00000000)
2021-03-10 15:50:40.056	2021-03-10 15:50:40.056	Associated String-Value alarm1, +19.8	Good (0x00000000)
2021-03-10 15:50:39.056	2021-03-10 15:50:39.056	Associated String-Value alarm1, +19.6	Good (0x00000000)
2021-03-10 15:50:38.056	2021-03-10 15:50:38.056	Associated String-Value alarm1, +19.4	Good (0x00000000)
2021-03-10 15:50:37.056	2021-03-10 15:50:37.056	Associated String-Value alarm1, +19.2	Good (0x00000000)
2021-03-10 15:50:36.056	2021-03-10 15:50:36.056	Associated String-Value alarm1, +19.0	Good (0x00000000)
2021-03-10 15:50:35.056	2021-03-10 15:50:35.056	Associated String-Value alarm1, +18.8	Good (0x00000000)
2021-03-10 15:50:34.056	2021-03-10 15:50:34.056	Associated String-Value alarm1, +18.6	Good (0x00000000)
2021-03-10 15:50:33.041	2021-03-10 15:50:33.041	Associated String-Value alarm1, +18.4	Good (0x00000000)

4. Click the "Stop" button to stop the cyclic update.



Single Update

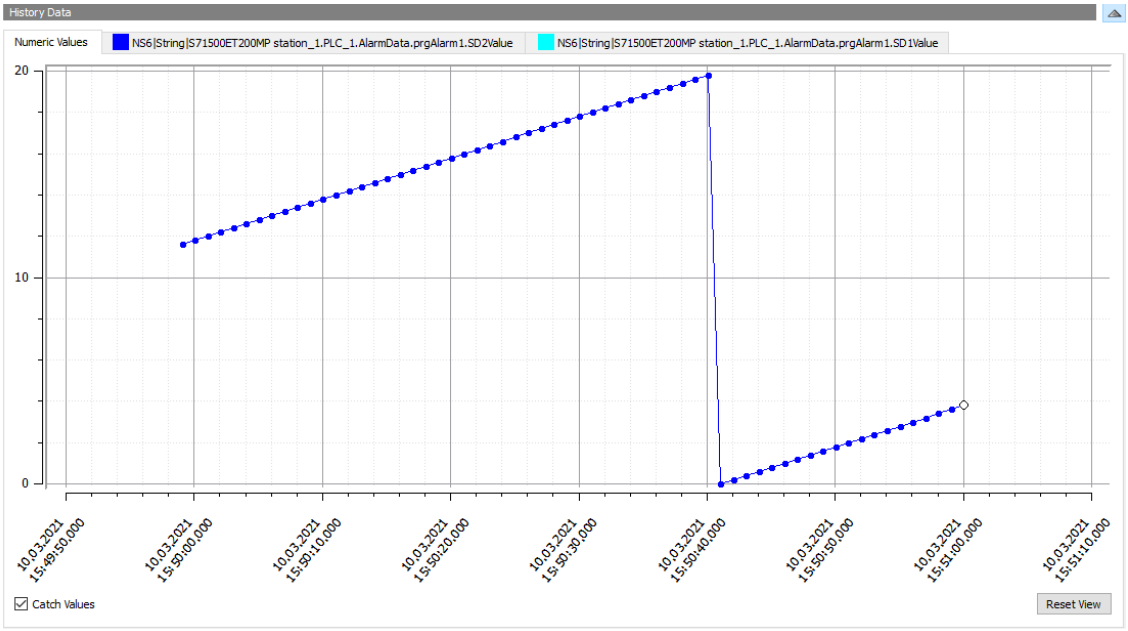
1. Enable the "Single Update" function.
2. Click the "Get Start Time" button.
   The possible start time will be found and entered in the "Start Time" field.
3. Optional: Adjust the start time in the "Start Time" field.
4. Enter the end time in the "End Time" field.
5. Click the "Update" button.



The values stored in the specified period are displayed.

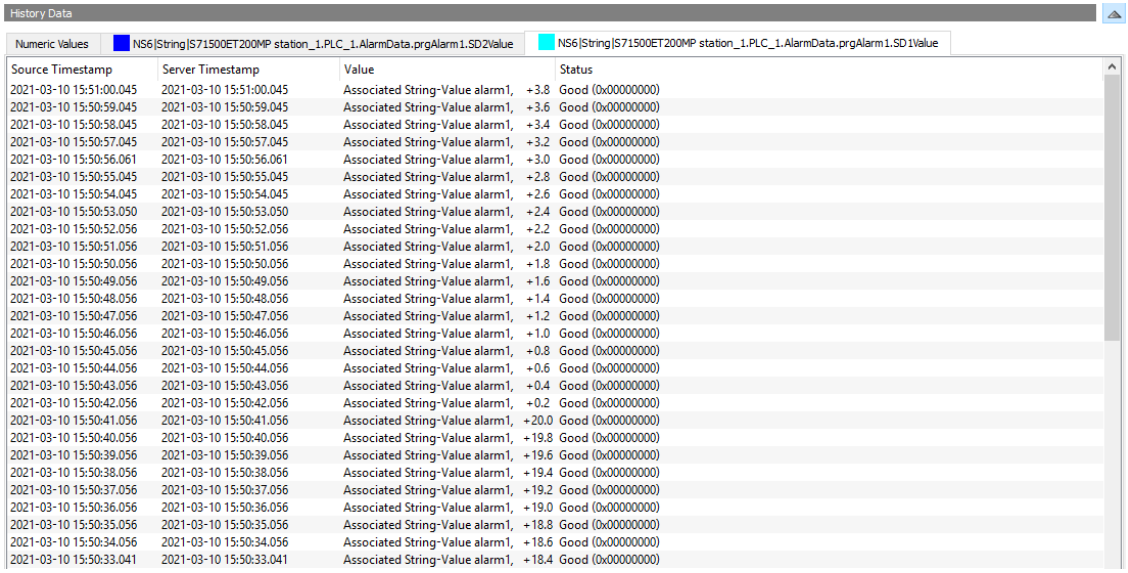
The values of the S7 tag "SD2Value" of the data type "Real" are displayed graphically in the "History Data" section of the "Numeric Values" tab.

Figure 2-22



The values of the S7 tag "SD1Value" of the data type "String" are displayed in tabular form in the "History data" section.

Figure 2-23



Source Timestamp	Server Timestamp	Value	Status
2021-03-10 15:51:00.045	2021-03-10 15:51:00.045	Associated String-Value alarm1, +3.8	Good (0x00000000)
2021-03-10 15:50:59.045	2021-03-10 15:50:59.045	Associated String-Value alarm1, +3.6	Good (0x00000000)
2021-03-10 15:50:58.045	2021-03-10 15:50:58.045	Associated String-Value alarm1, +3.4	Good (0x00000000)
2021-03-10 15:50:57.045	2021-03-10 15:50:57.045	Associated String-Value alarm1, +3.2	Good (0x00000000)
2021-03-10 15:50:56.061	2021-03-10 15:50:56.061	Associated String-Value alarm1, +3.0	Good (0x00000000)
2021-03-10 15:50:55.045	2021-03-10 15:50:55.045	Associated String-Value alarm1, +2.8	Good (0x00000000)
2021-03-10 15:50:54.045	2021-03-10 15:50:54.045	Associated String-Value alarm1, +2.6	Good (0x00000000)
2021-03-10 15:50:53.050	2021-03-10 15:50:53.050	Associated String-Value alarm1, +2.4	Good (0x00000000)
2021-03-10 15:50:52.056	2021-03-10 15:50:52.056	Associated String-Value alarm1, +2.2	Good (0x00000000)
2021-03-10 15:50:51.056	2021-03-10 15:50:51.056	Associated String-Value alarm1, +2.0	Good (0x00000000)
2021-03-10 15:50:50.056	2021-03-10 15:50:50.056	Associated String-Value alarm1, +1.8	Good (0x00000000)
2021-03-10 15:50:49.056	2021-03-10 15:50:49.056	Associated String-Value alarm1, +1.6	Good (0x00000000)
2021-03-10 15:50:48.056	2021-03-10 15:50:48.056	Associated String-Value alarm1, +1.4	Good (0x00000000)
2021-03-10 15:50:47.056	2021-03-10 15:50:47.056	Associated String-Value alarm1, +1.2	Good (0x00000000)
2021-03-10 15:50:46.056	2021-03-10 15:50:46.056	Associated String-Value alarm1, +1.0	Good (0x00000000)
2021-03-10 15:50:45.056	2021-03-10 15:50:45.056	Associated String-Value alarm1, +0.8	Good (0x00000000)
2021-03-10 15:50:44.056	2021-03-10 15:50:44.056	Associated String-Value alarm1, +0.6	Good (0x00000000)
2021-03-10 15:50:43.056	2021-03-10 15:50:43.056	Associated String-Value alarm1, +0.4	Good (0x00000000)
2021-03-10 15:50:42.056	2021-03-10 15:50:42.056	Associated String-Value alarm1, +0.2	Good (0x00000000)
2021-03-10 15:50:41.056	2021-03-10 15:50:41.056	Associated String-Value alarm1, +20.0	Good (0x00000000)
2021-03-10 15:50:40.056	2021-03-10 15:50:40.056	Associated String-Value alarm1, +19.8	Good (0x00000000)
2021-03-10 15:50:39.056	2021-03-10 15:50:39.056	Associated String-Value alarm1, +19.6	Good (0x00000000)
2021-03-10 15:50:38.056	2021-03-10 15:50:38.056	Associated String-Value alarm1, +19.4	Good (0x00000000)
2021-03-10 15:50:37.056	2021-03-10 15:50:37.056	Associated String-Value alarm1, +19.2	Good (0x00000000)
2021-03-10 15:50:36.056	2021-03-10 15:50:36.056	Associated String-Value alarm1, +19.0	Good (0x00000000)
2021-03-10 15:50:35.056	2021-03-10 15:50:35.056	Associated String-Value alarm1, +18.8	Good (0x00000000)
2021-03-10 15:50:34.056	2021-03-10 15:50:34.056	Associated String-Value alarm1, +18.6	Good (0x00000000)
2021-03-10 15:50:33.041	2021-03-10 15:50:33.041	Associated String-Value alarm1, +18.4	Good (0x00000000)

3 Useful information

3.1 S7OPT event types

3.1.1 Overview

The SIMATIC NET S7OPT OPC UA server supports the following OPC UA event and alarm types:

- Statepath alarm
  Alarms for the S7 connection status
- Consistency alarm
  Alarm for an inconsistent alarm configuration
- Program alarms
  At a signal change, the "Program_Alarm" alarm block will generate a program alarm with or without required acknowledgement and with up to ten associated values.
- System messages
  System messages are triggered independently by the PLC and cannot be configured or changed by the user.
  The following system messages are available:
  - System diagnostics alarms:
    The scope of the system diagnostics is derived from the relevant hardware configurations. Conditions such as device failure, block error, peripheral access error, channel error, parameterization error, external auxiliary power failure, and hardware configuration changes (such as unplugging and plugging in of modules) are reported.
  - Overload messages:
    Special system diagnostic messages for resource bottlenecks
  - Security messages:
    Reporting of access violations in case of, e. g. incorrect password entry

Note The S7OPT OPC UA server only supports program alarms to the S7-1500.

3.1.2 Statepath alarm

This S7OPT event type maps the inverse state of an S7 connection ("Inactive" if S7 connection is established ("UP"); and "Active" if S7 connection is not established ("DOWN" or "RECOVERY")).

The status is only determined on the PC side and can, therefore, be reported even if there is no physical connection to the PLC.

In the "Active" state, no further program alarms can be received.

Display name

"S7OPTStatepathAlarmType"

3.1.3 Consistency alarm

This S7OPT event type has no acknowledgement requirement. It indicates inconsistent alarm configuration between a PLC and the PC station. Such inconsistent program alarms are not reported to the OPC client. In this case, the condition instance "consistency" is set to "Active" once for this PLC. It is recommended to update the alarm configuration first on the PLC and then on the PC station.

Display name

"S7OPTConsistencyAlarmType"

3.1.4 Program alarms

Display name

- "S7OPTOffNormalAlarmType":
  This S7OPT event type displays the configured program alarms with or without required acknowledgement and with up to ten associated values. The program alarms of this type have a state or condition. These can assume the status "incoming" or "outgoing".
- "S7OPTInfoReportEventType":
  This S7OPT event type displays the configured information-only program alarms with up to ten associated values. To do this, the checkbox in the "Information only" column in the TIA Portal alarms editor must be enabled.

3.1.5 System messages

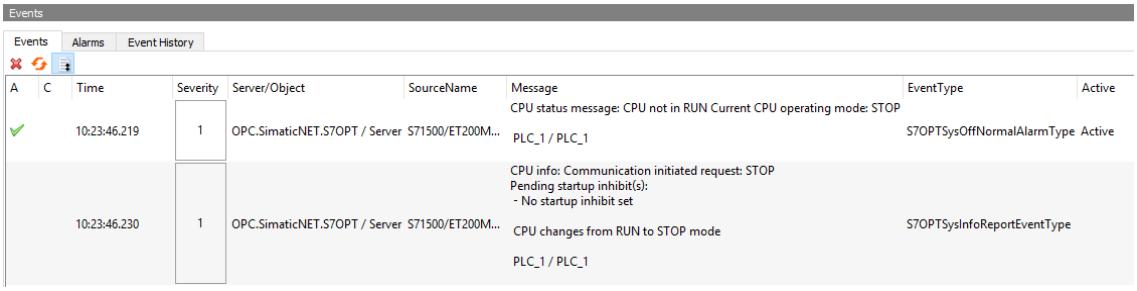
Display name

- "S7OPTSysOffNormalAlarmType"
  This S7OPT event type displays the system messages with or without acknowledgement obligation with an associated value. The contents of this associated value are the 20 bytes of diagnostic data. The system messages of this type have a state or condition. These can assume the status "incoming" or "outgoing". To accomplish this, the checkbox in the "Acknowledgement" column for the module's alarm settings in TIA Portal must be enabled.
- "S7OPTSysInfoReportEventType"
  This S7OPT event type displays the system messages, which are for information purposes only, with an associated value. The contents of this associated value are the 20 bytes of diagnostic data.

Receive system messages in the OPC client

System messages are automatically displayed in UA Expert in the Event View when they are incoming or outgoing. No user program is required in the S7 CPU.

Figure 3-1



3.2 Access to historical data of S7 Tags

Historical data

Historical data services enable storage and read access to the S7 tags of automation devices stored in an archive. The timestamp and the quality characteristic of the S7 tags are stored together with the process value.

Enable historical data

Archiving can only be activated for symbolic data tags via the "Symbol Editor" of the SIMATIC PC station in TIA Portal.

Options for OPC UA clients to access historical data

OPC UA clients, such as UA Expert from Unified Automation, can access the process values of archived S7 tags using the "HistoryRead" function. The archive consists of a maximum of 360 files. Each file stores the data of the symbols configured for the archive. Each file covers a period of 1 hour. Beginning at system startup, the maximum number of 360 files is reached after a little more than two weeks. When new archive files are created, the oldest files are successively deleted in the order in which they were first created.

Maximum storage of S7 tags

A maximum of 1000 S7 tags can be archived by the S7OPT OPC UA server.

Data types

The following table shows an overview of the data types that the S7OPT OPC UA server can archive.

Table 3-1

Type identifier	S7 data type	OPC UA data type	Description
b	BYTE	Byte	8 Bit (bit string)
	USINT	Byte	8 Bit (unsigned)
c	CHAR	SByte	8 Bit (character)
	SINT	SByte	8 Bit (signed)
wc	WCHAR	UInt16	16 Bit (character, UTF-8)
w	WORD	UInt16	16 Bit (bit string)
	UINT	UInt16	16 Bit (unsigned)
dw	DWORD	UInt32	32 Bit (Bitstring)
	UDINT	UInt32	32 Bit (unsigned)
lw	LWORD	UInt64	64 Bit (Bitstring) only available for S7-1500
	ULINT	UInt64	64 Bit (unsigned) only available for S7-1500
I	INT	Int16	16 Bit (signed)
di	DINT	Int32	32 Bit (signed)
li	LINT	Int64	64 Bit (signed) only available for S7-1500
R	REAL	Float	Floating point (4 bytes) IEEE 754
lr	LREAL	Double	Floating point (8 bytes) IEEE 754
dt	DATE_TIME	DateTime	Date and time Value range as of 01.01.1990; only available for S7-1500
ldt	LDT	DateTime	Date and time accurate to nanoseconds, Value range as of 01.01.1990; only available for S7-1500 The OPC UA server rounds the time by representing it as DateTime. This limits the resolution to 100 nanoseconds.
dtl	DTL	DateTime	Date and time accurate to nanoseconds, Value range 01.01.1970–31.12.2553; only available for S7-1500 The OPC UA server rounds the time by representing it as DateTime. This limits the resolution to 100 nanoseconds. The individual components of the S7 data type "DTL" are not archived.
date	DATE	DateTime	Date and time (8 bytes) (where the time is always 00:00:00); value range starting at 01.01.1990. Image of the CPU data type "DATE" (unsigned, 16 bit).
t	TIME	Int32	Signed time value in milliseconds
lt	LTIME	Int64	Signed time value in nanoseconds; only available for S7-1500
tod	TOD	UInt32	Time of day, 0–86399999 ms from midnight

Type identifier	S7 data type	OPC UA data type	Description
ltod	LTOD	UInt64	Time of day, 0–86399999999999 ns from midnight; only available for S7-1500
s5tbcd	S5TIME	UInt16	Mapping of the CPU data type "S5TIME" to UInt 16 (unsigned, 16 bit) with restricted value range, 0...9990000 ms; only available for S7-1500
x <bit address>	BOOL	Boolean	Bit (bool) In addition to the byte offset in the range, the <bit address> must also be specified in the respective byte. Value range 0–7
s <string length>	STRING	String (UTF-8)	The <string length reserved for the STRING> must be specified. Value range 1–254 When writing, it is also possible to write shorter STRING, whereby the transmitted data length is always the reserved string length in bytes plus 2 bytes. The bytes that are not required are filled with the value 0. The reading and writing of STRING and STRING arrays is internally mapped to the reading and writing of byte arrays. The STRING must be initialized on the S7 with valid values.
ws <string length>	WSTRING	String (UTF-8)	The <string length> reserved for the WSTRING must be specified in WCHAR. Value range 1–16382. When writing, shorter WSTRING can also be written, although the transmitted data length is always the reserved <string length> in WCHAR plus 4 bytes. The bytes that are not required are filled with the value 0. The reading and writing of WSTRING and WSTRING arrays is internally mapped to the reading and writing of byte arrays. The WSTRING must be initialized on the S7 with valid values.

Furthermore, arrays of these elementary S7OPT data types are also supported for archiving. Each array or data tag counts as an archivable S7 tag. The configured number of archived S7 tags can be determined in the TIA Portal "Symbol Editor" at the time of configuration.

User-specific data types (UDT), structures, timers, and counters cannot be archived by the S7OPT OPC UA server.

Note The configured S7 connections, which are necessary for monitoring archived S7 tags, are established after the PC and the S7OPT OPC UA server start up. This ensures seamless archiving of process values from the S7 tags.

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

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

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

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

support.industry.siemens.com

Technical Support

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

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

SITRAIN – Digital Industry Academy

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

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

siemens.com/sitrain

Service offer

Our range of services includes the following:

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

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

support.industry.siemens.com/cs/sc

Industry Online Support app

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

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

4.2 Industry Mall

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

4.3 Links and literature

Table 4-1

No.	Subject
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/67295801
\3\	SIMATIC NET: PC software Industrial Communication with PG/PC Volume 2 - Interfaces https://support.industry.siemens.com/cs/ww/en/view/77378184
\4\	SIMATIC NET: PC Software Industrial Communication with PG/PC Volume 1 – Fundamentals https://support.industry.siemens.com/cs/ww/en/view/77376110
\5\	SIMATIC NET: PC software Commissioning PC Stations - Manual and Quick Start https://support.industry.siemens.com/cs/ww/en/view/77377601

4.4 Change documentation

Table 4-2

Version	Date	Change
V1.0	07/2021	First version