SIEMENS

Application Example • 10/2016

OPC UA .NET Client for the SIMATIC S7-1500 OPC UA Server

S7-1500 / OPC UA

https://support.industry.siemens.com/cs/ww/en/view/109737901

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications − e.g. Catalogs − the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

Warranty and Liability 2

1 Introduction 4

1.1 Overview 4
1.2 Mode of operation 5
1.3 Components used 7

2 Engineering 8

2.1 Planning the OPC UA server of the S7-1500 8
2.1.1 Enabling OPC UA Server 8
2.1.2 Enabling global security settings 10
2.1.3 Configuring OPC UA security policies (server endpoints) 11
2.1.4 Security via certificate management (optional) 12
2.1.5 Enabling tags for the OPC UA communication 14
2.2 Programming the OPC UA client example 15
2.2.1 OPC UA Client S7-1500 15
2.2.2 UAClientHelperAPI 18
2.2.3 Sequence diagrams of the client example 19
2.3 Operation 24
2.3.1 Description of the user interface 24
2.3.2 Commissioning OPC UA server of the S7-1500 27
2.3.3 Commissioning OPC UA Client S7-1500 28
2.3.4 Creating, exporting and loading client certificate into the S7-1500 (optional) 28
2.3.5 Establishing connection to the OPC UA server 32
2.3.6 Browsing address space of the OPC UA server 34
2.3.7 Read/write tags 34
2.3.8 Subscriptions 36

3 Valuable Information 37

3.1 Basics 37
3.1.1 General OPC UA information 37
3.1.2 OPC UA address space 38
3.1.3 OPC UA Security 41
3.1.4 OPC UA server of the S7-1500 43
3.2 TIA Portal project details 44
3.2.1 S7-1500 and OPC UA configuration 44
3.2.2 S7 program 44

4 Appendix 45

4.1 Siemens services 45
4.2 Links and Literature 46
4.3 Change documentation 46

1 Introduction

1.1 Overview

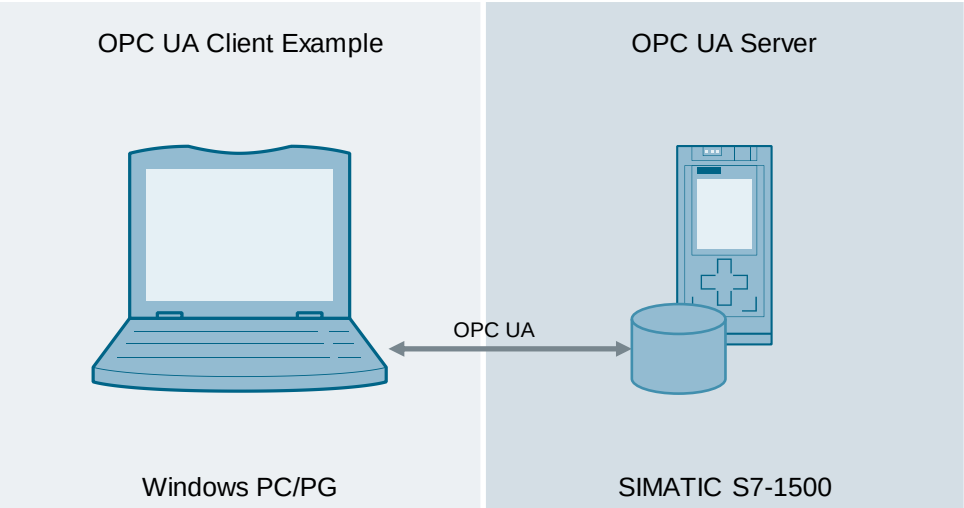
OPC UA (Open Platform Communications Unified Architecture) is an M2M communication protocol adopted in 2009 that was specified by the OPC foundation. The OPC specification has been developed to create an interoperable, secure and reliable communication protocol. Based on these properties OPC UA increasingly prevails as standard in the industrial environment.

With the current firmware of SIMATIC S7-1500 an integrated OPC UA Server has been added to the control system. This enables an additional option of direct process data exchange of the SIMATIC S7-1500 with a wide variety of other systems that support OPC UA.

Content of this application example

In order to exchange data with the server of the SIMATIC S7-1500 via OPC UA, this application example will show you how you can create a simple client in .Net. Furthermore, the configuration of the OPC UA server of the SIMATIC S7-1500 is explained step by step.

Figure 1-1



Advantages of the application example

This application example offers you the following advantages:

- Expandable TIA project with preconfigured OPC UA server for a SIMATIC S7-1500.
- A simple and expandable OPC UA client, created in .NET.
- A commented C# class that summarizes the OPC UA client basic functions and guarantees an easy implementation.

Assumed knowledge

The following basic knowledge is required by the user:

- Basics of programming in C#/.NET
- Basics of configuring in the TIA Portal
- Basics of OPC
- Basics in software security and certificate handling

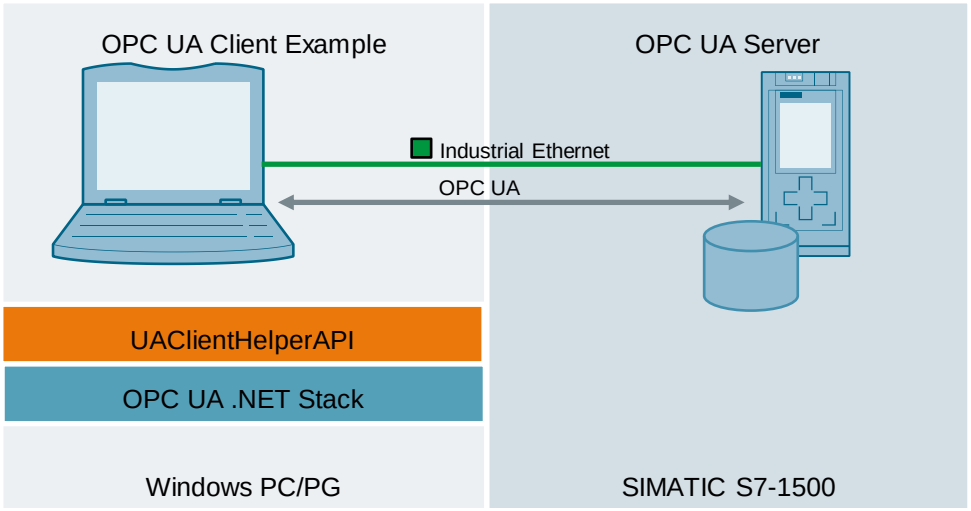
1.2 Mode of operation

Below, you will find an explanation of what components, functions and mode of operations are used in the application example.

General function description

The following figure shows the most important components of this application example:

Figure 1-2



A simple OPC UA .NET client for Windows PCs/PGs communicates with the OPC UA server of a SIMATIC S7-1500.

The client supports the following OPC UA service sets:

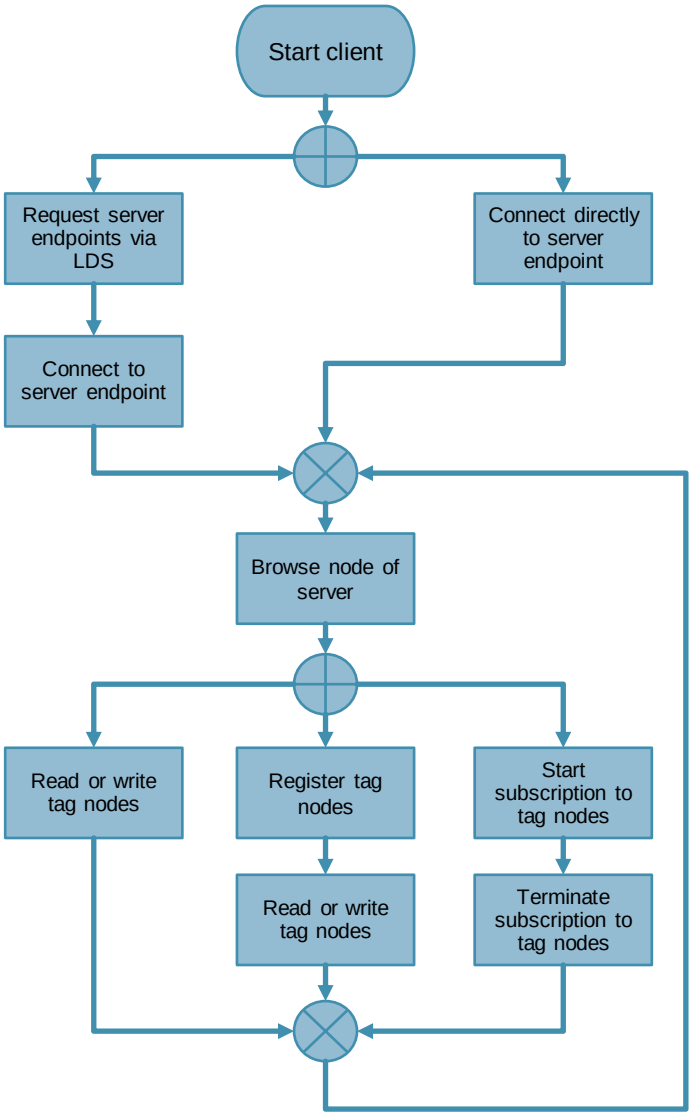
- Searching and finding server: Discovery Service Set (FindServers, GetEndpoints)
- Creating and ending sessions: Sessions Service Set (CreateSession, CloseSession)
- Navigating in the address space: View Service Set (Browse, RegisterNodes, UnregisterNodes)
- Reading and writing tags and attributes: Attribute Service Set (Read, Write)
- Subscribing tags: Subscription Service Set (CreateSubscription, DeleteSubscribtion); MonitoredItem Service Set (CreateMonitoredItem, DeleteMonitoredItem)

The SIMATIC S7-1500 OPC UA server is planned and configured via the TIA Portal. The OPC UA Client is created in C# / .NET and internally uses the freely accessible OPC UA .NET stack of the OPC Foundation. For easier individual implementations of a .NET client the “UAClientHelperAPI” C# class is included in delivery. This class summarizes the basic functions of the .NET stack of the OPC foundation and considerably facilitates the use of the basic functions for you. Client and server are connected via Ethernet and communicate through OPC UA via TCP/IP.

Functional sequence

Once the OPC UA server has been planned configured (with client certificate) and loaded into the CPU, the following functional sequence is the result for the client of this example:

Figure 1-3



Note In order to request server endpoints via a LDS (Local Discovery Server) or GDS (Global Discovery Server) a LDS has to be installed on the PC/PG or a GDS has to be available in the network.

1.3 Components used

This application example was created with the following components:

Table 1-1

Component	Number	Article number	Note
S7-1500 CPU 1516F-3 PN/DP	1	6ES7 516-3AN01-0AB0	Firmware 2.0 or higher
TIA Portal	1	6ES7822-1..04-..	V14 or higher
Visual Studio 2013	1	-	Community version also possible.
OPC UA .Net Stack	1	-	V1.2.336.0 Download: Links & Literature in item \2\.

2 Engineering

2.1 Planning the OPC UA server of the S7-1500

The following step-by-step instructions show you how to plan and configure the SIMATIC S7-1500 OPC UA server via the TIA Portal.

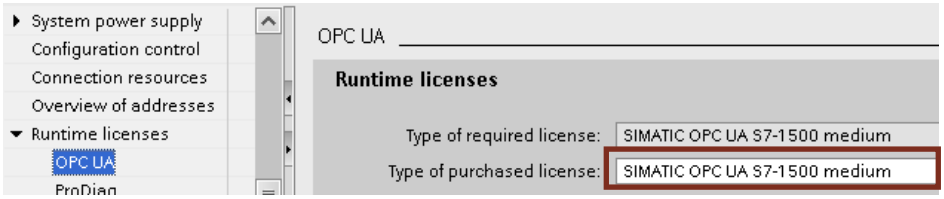
Prerequisites

- Create a TIA Portal V14 project.
- Configure a SIMATIC S7-1500 with firmware 2.0 or higher.

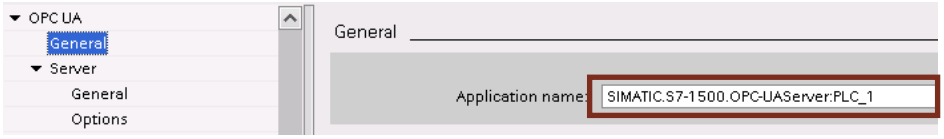
2.1.1 Enabling OPC UA Server

The OPC UA server of the S7-1500 is disabled by default. The instructions below show you the required steps to enable the server:

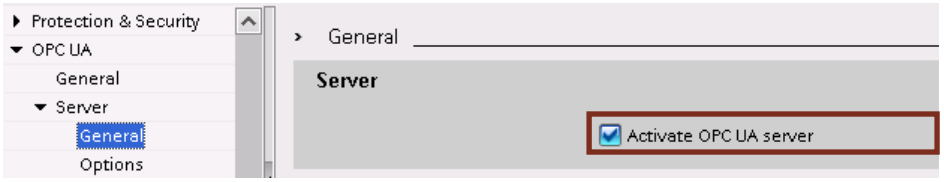
1. Navigate to the “Properties” of the configured S7-1500 CPU in the TIA Portal.
2. Navigate to “Runtime licenses” > “OPC UA” in the inspector window and select the required license there.



3. Navigate to “OPC UA” > “General” in the inspector window and assign a suitable name for your OPC UA server in the “Application name” field. With this name the S7-1500 UA server identifies itself to the UA clients.

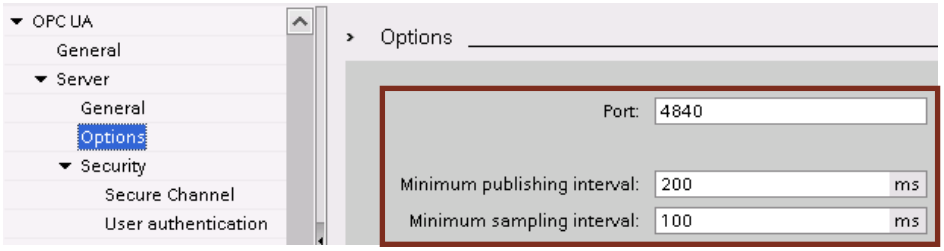


4. Navigate to “OPC UA” > “Server” > “General” in the inspector window and enable the “Activate OPC UA server” check box there.



Note This setting is sufficient to enable the OPC UA server of the CPU and to guarantee basic operation. Please note that the server in its standard configuration allows the connection of any client.

5. Navigate to “OPC UA” > “Server” > “Options” in the inspector window and assign your desired port address for the OPC UA server of the CPU. Furthermore, assign a “Minimum publishing interval” and a “Minimum sampling interval” for the OPC UA server.



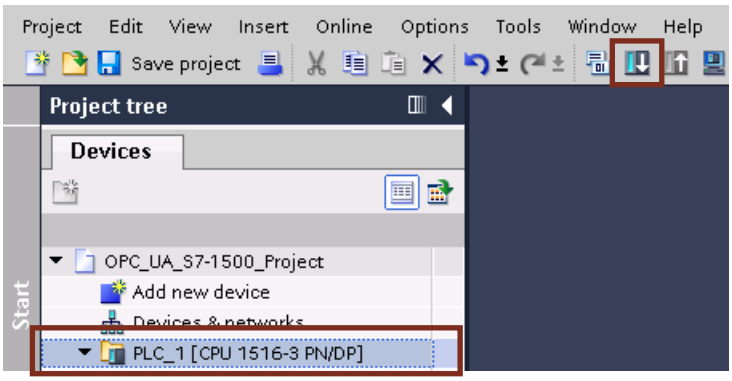
Note

“Minimum publishing interval”:
This value determines at what minimal intervals the OPC UA server is allowed to send data to a client via OPC UA subscriptions.

“Minimum sampling interval”:
This value determines at what minimal intervals the OPC UA server is allowed to request data changes of the CPU data management.

These values have an influence on the communication and CPU load and should therefore be considered. The minimal value depends on the CPU type.

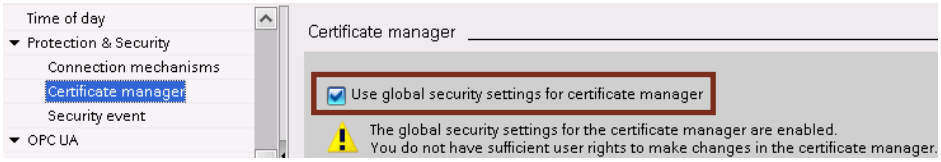
6. Select the CPU in your project navigation and load the project into the controller.



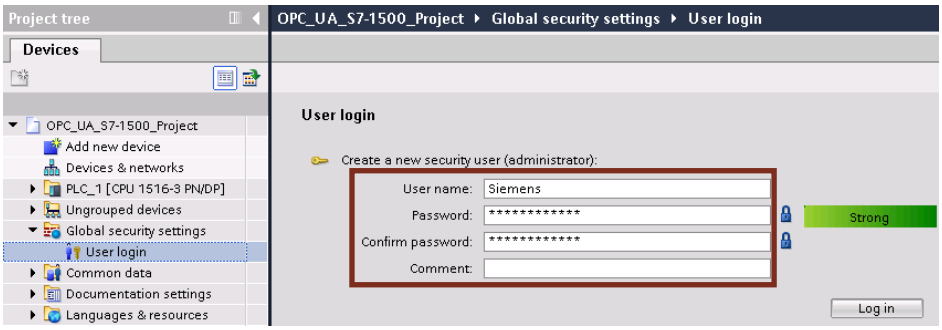
2.1.2 Enabling global security settings

In order to manage the software certificates for the OPC UA server, the global security settings of the TIA project have to be enabled. The instructions below show you the required steps:

1. Navigate to the “Properties” of the configured S7-1500 CPU in the TIA Portal.
2. Navigate to “Protection & Security” > “Certificate manager” and enable the “Use global security settings for certificate manager” check box.



3. Navigate to “Global security settings” > “User login” in the project navigation and assign a user name and a password, in order to be able to make security settings in your project. Confirm with “Log in”.

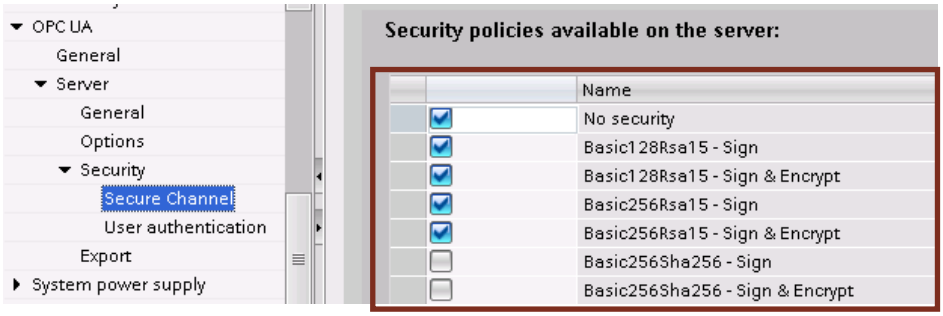


4. Via the assigned user name and the password you can log onto the TIA project to access the certificate manager and other security functions.

2.1.3 Configuring OPC UA security policies (server endpoints)

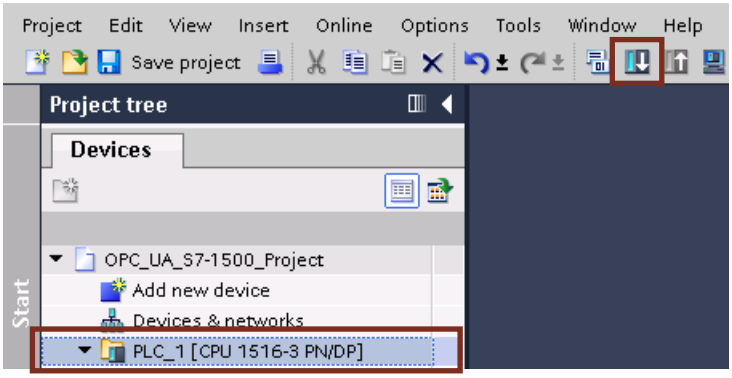
You can configure the way of the encryption and authentication between OPC UA client and server via the security policies of the OPC UA server. The following instruction shows you the required steps to enable the existing security policies:

1. Navigate to the “Properties” of the configured S7-1500 CPU in the TIA Portal.
2. Navigate to “OPC UA” > “Server” > “Security” > “Secure Channel” in the inspector window and select your desired security policies in “Security policies available on the server”. The server creates a separate endpoint for each selected policy to which a client can connect.



Note For an OPC UA Client to be able to connect to the endpoints of the OPC UA server it has to support the selected policies.

3. Select the CPU in your project navigation and load the project into the controller.



2.1.4 Security via certificate management (optional)

The following prerequisites have to be fulfilled for these settings:

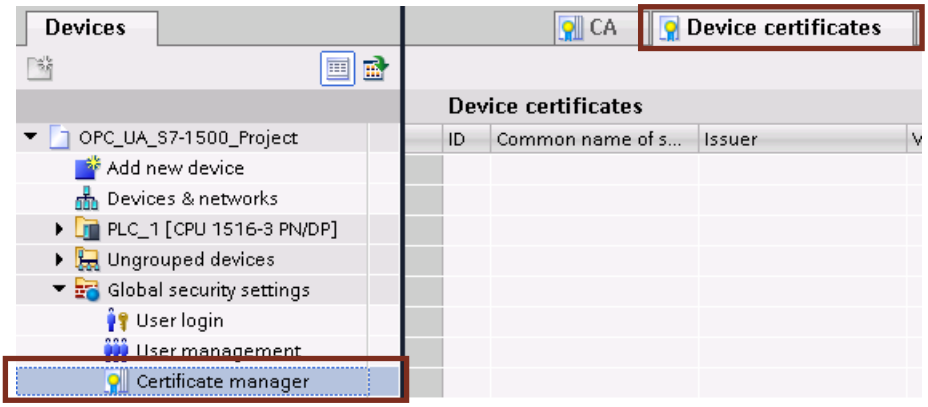
- Global security settings are enabled
- You are logged in to the global security settings
- Client certificates are available.

The following instruction shows you what you have to configure, in order to only allow OPC UA clients with defined software certificates to connect to the OPC UA server:

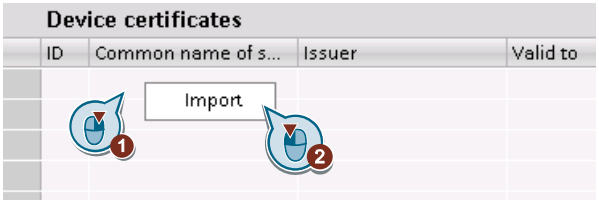
1. Navigate to the “Properties” of the configured S7-1500 CPU in the TIA Portal.
2. Navigate to the “OPC UA” > “Server” > “Security” > “Secure Channel” inspector window and disable the “Automatically accept all client certificates during runtime” check box in “Trusted clients”.

Note However, when you enable the security policy “none”, any client can still connect via the appropriate endpoint even without accepted certificate.

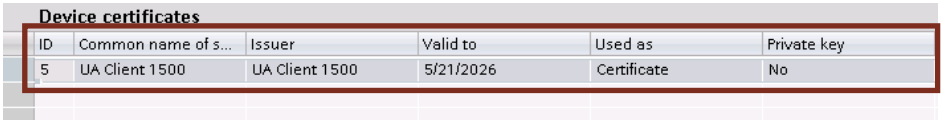
3. Navigate to “Global security settings” in the project navigation and open the “Certificate Manager”.
4. Go to the “Device certificates” tab.



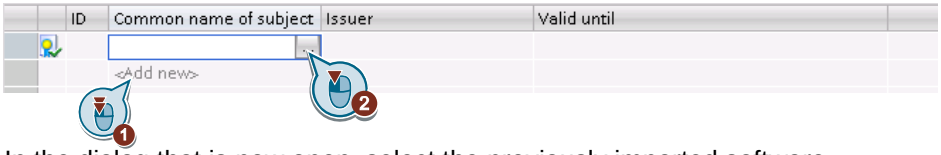
5. Right-click in the work area and then left-click “Import”.



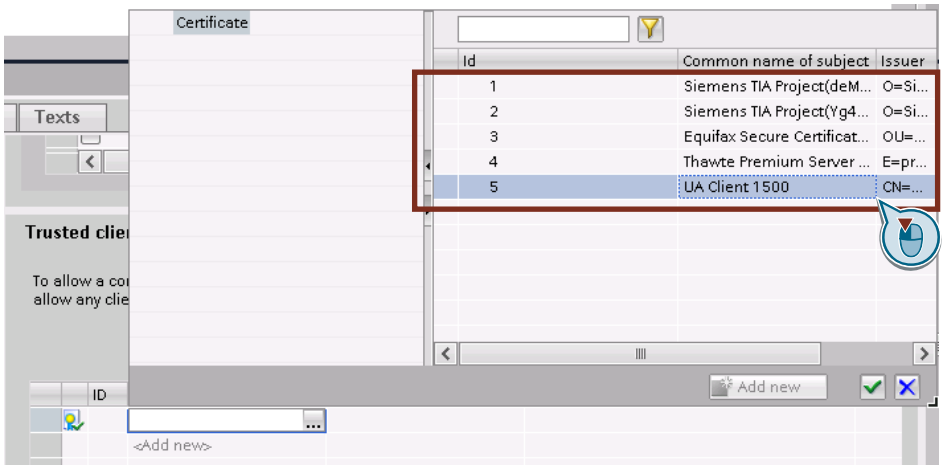
6. Select the software certificate of your OPC UA client via the opened file browser and confirm with “Open”. The imported certificates can then be viewed in the work area.



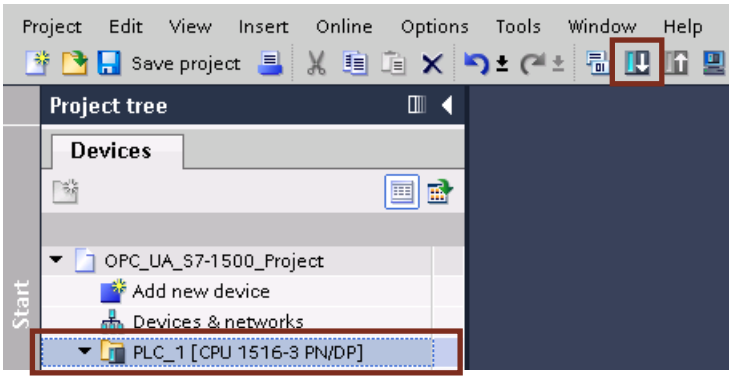
7. Navigate to the “OPC UA” > “Server” > “Security” > “Secure Channel” inspector window and go to the “Trusted clients” area.
8. Double-click “<Add new>” in the list and then click the “…” icon.



9. In the dialog that is now open, select the previously imported software certificate of the certificate manager that your OPC UA server is to trust and confirm it with the green tick.



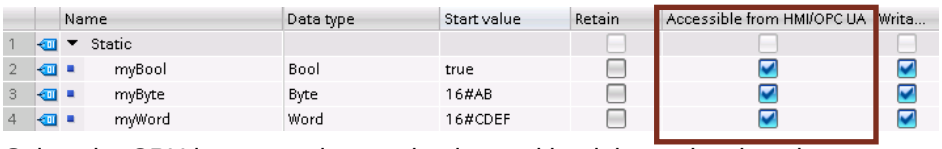
10. Select the CPU in your project navigation and load the project into the controller.



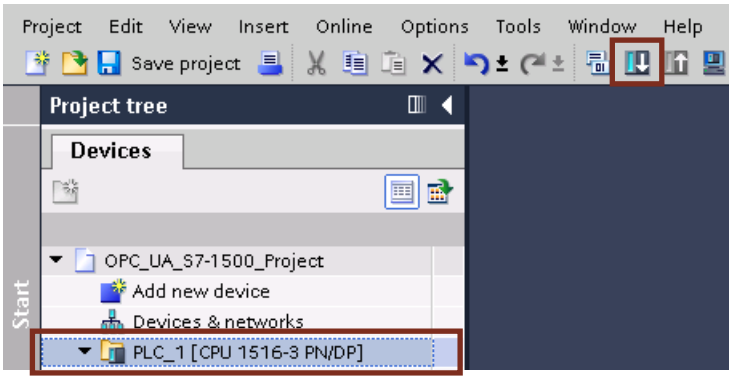
2.1.5 Enabling tags for the OPC UA communication

For each tag (apart from temporary ones) in the S7 user program you can specify individually whether they are to be enabled for the OPC UA communication. The following instruction explains you what you have to do.

1. Navigate in your TIA project to the tags you want to have in a FB, DB or the PLC tags.
2. Enable the “Accessible from HMI/OPC UA” check box in the tag declarations.



3. Select the CPU in your project navigation and load the project into the controller.



4. The tags modified by you are now writable or readable via OPC UA clients.

2.2 Programming the OPC UA client example

The following descriptions explain the functions and principles of the OPC UA client example program.

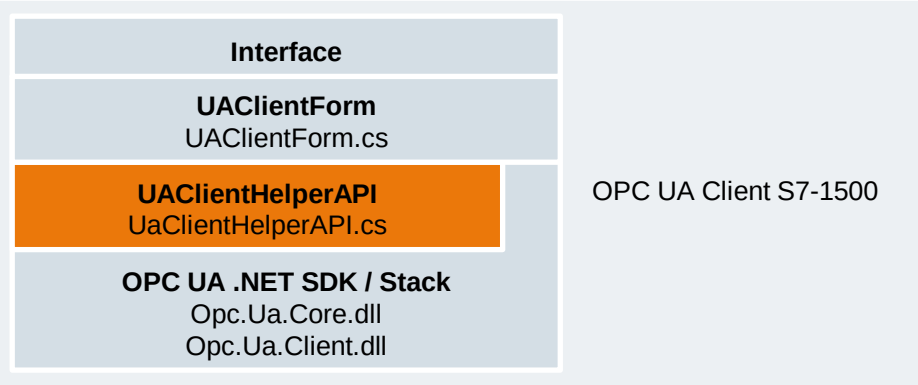
2.2.1 OPC UA Client S7-1500

The OPC UA client example program “OPC UA Client S7-1500” has been created in .NET and requires .NET Framework 4.5.1.

Structural configuration

The following figure shows the structure of the OPC UA client example of this application example:

Figure 2-1



The “UAClientForm” class is derived from the Windows.Forms system class and includes the form constructor as well as the EventHandlers of the program interface. The methods of the “UAClientHelperAPI” class are accessed in the EventHandlers.

The “UAClientHelperAPI” class is a user-specific class that summarizes the most important calls of the OPC UA .NET stack. Additionally, private methods are included, in order to create and fill required objects for the OPC UA .NET stack. This class can be expanded and reused as desired and can be used by developers, in order to create simple separate OPC UA clients.

The “OPC UA .NET Stack” of the OPC Foundation includes the actual classes/objects that execute and manage the OPC UA communication. The stack consists of a multitude of libraries (DLLs). This application example is only realized via the methods and objects of Core.dll and Client.dll. Both files are included in this application example. The download of the complete .NET Stack as well as its documentation can be found in the links and literature in item \2\.

Using UAClientHelperAPI in the example

In the following table the functions are listed in which the public methods of the UAClientHelperAPI are used:

Table 2-1

UAClientHelperAPI	Used within UAClientForm.cs in the method…
FindServers	EndpointButton_Click
GetEndpoints	EndpointButton_Click
Connect	ConnectServerButton_Click EpConnectButton_Click
Disconnect	ConnectServerButton_Click EpConnectButton_Click ClientForm_FormClosing
BrowseRoot	BrowsePage_Enter
BrowseNode	NodeTreeView_BeforeExpand
Subscribe	SubscribeButton_Click
AddMonitoredItem	SubscribeButton_Click
RemoveMonitoredItem	SubscribeButton_Click
RemoveSubscription	UnsubscribeButton_Click
ReadNode	NodeTreeView_BeforeSelect
WriteValues	WriteValButton_Click RgWriteValButton_Click
ReadValues	ReadValButton_Click RgReadButton_Click
RegisterNodeIds	RegisterButton_Click
UnregisterNodeIds	UnregisterButton_Click

The following table lists the EventHandlers in which the public events of the UAClientHelperAPI are to be processed:

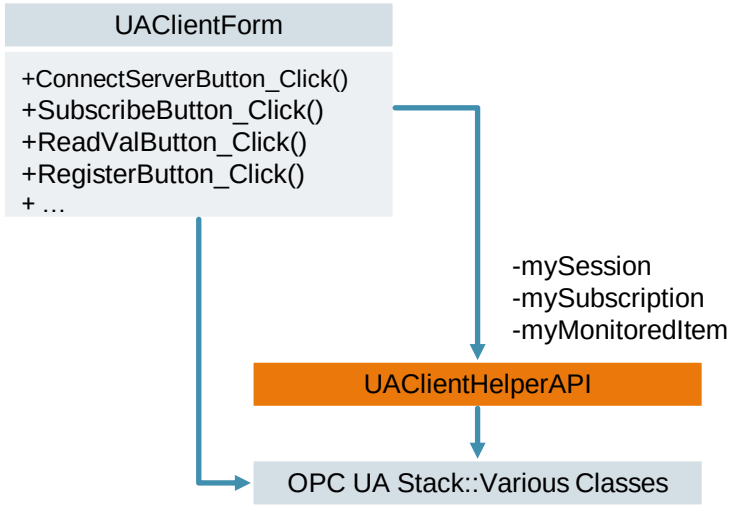
Table 2-2

UAClientHelperAPI	Used within UAClientForm.cs in event handler…
ItemChangeNotification	Notification_MonitoredItem
KeppAliveNotification	Notification_KeppAlive

Class diagram

The following class diagram shows you the classes of the OPC UA client example. The functions of the program interface are implemented by the classes used.

Figure 2-2



2.2.2 UAClientHelperAPI

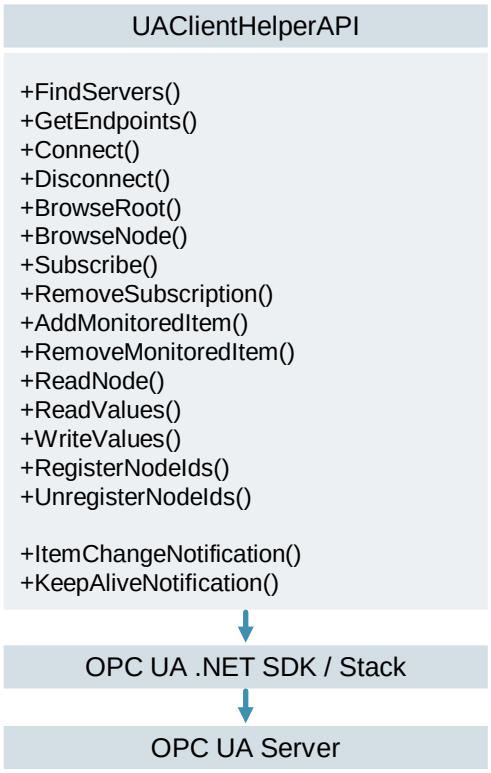
The following explanations describe the reusable “UAClientHelperAPI” class that illustrates the main functionalities of the OPC UA client example.

Class diagram

The following class diagram shows you the “UAClientHelperAPI” class. The most important access methods to an OPC UA server are encapsulated in this class and are summarized in a simple way.

The UAClientHelperAPI accesses the .NET-Assemblys Opc.UA.Client.dll and Opc.UA.Core.dll of the OPC Foundation.

Figure 2-3



Method description

The following table explains the functions of the public methods within the “UAClientHelperAPI” class, via which the OPC UA client functionalities are realized:

Table 2-3

Method	Explanation
FindServers	Searches for OPC UA servers in the network. Requirement: A LDS (Local Discovery Server) or GDS (Global Discovery Server) has to be available.
GetEndpoints	Determines the available endpoints on a server via which a connection can be established.
Connect	Establishes a connection to a server and creates a secure channel and a session to the server.

Method	Explanation
Disconnect	Ends an existing session and disconnects the connection to the server.
BrowseRoot	Returns a collection of nodes that can be found in the root directory of the server.
BrowseNode	Returns a collection of nodes that can be found in a specific node.
Subscribe	Creates a subscription on the server.
RemoveSubscription	Deletes a specific subscription from the server.
AddMonitoredItem	Adds a MonitoredItem for monitoring an existing subscription.
RemoveMonitoredItem	Deletes an existing MonitoredItem of a subscription.
ReadNode	Reads the metadata of a specific node.
ReadValues	Reads the values of a tag node.
WriteValues	Writes values in tag nodes.
RegisterNodeIds	Registers node IDs at the server for an optimized access to the nodes.
UnregisterNodeIds	Deletes the registration of already registered node IDs.
ItemChangeNotification	Event that is fired when the value of a MonitoredItem is changed.
KeepAliveNotification	Event that is fired when the value of a KeepAliveNotification arrives.

Note Within a class the “Validator_CertificateValidation” EventHandler is implemented that handles a certificate event.
As soon as a server certificate is transferred to the client, this process is reported via the event. The server certificate is accepted in the EventHandler.
This means that the client accepts any server certificate.

2.2.3 Sequence diagrams of the client example

The following sequence diagrams show the program sequences of the OPC UA example client for various functions of the example.

Establishing and ending connection to the OPC UA server

The following sequence diagram shows the procedures, in order to establish and disconnect the connection to the OPC UA server. By clicking the “Get Endpoints” button, the user receives available endpoints and can select an endpoint from it. The connection establishment is then performed via the “Connect to Server” button.
The methods that are executed when clicking the button are shown in the following diagram:

Figure 2-4

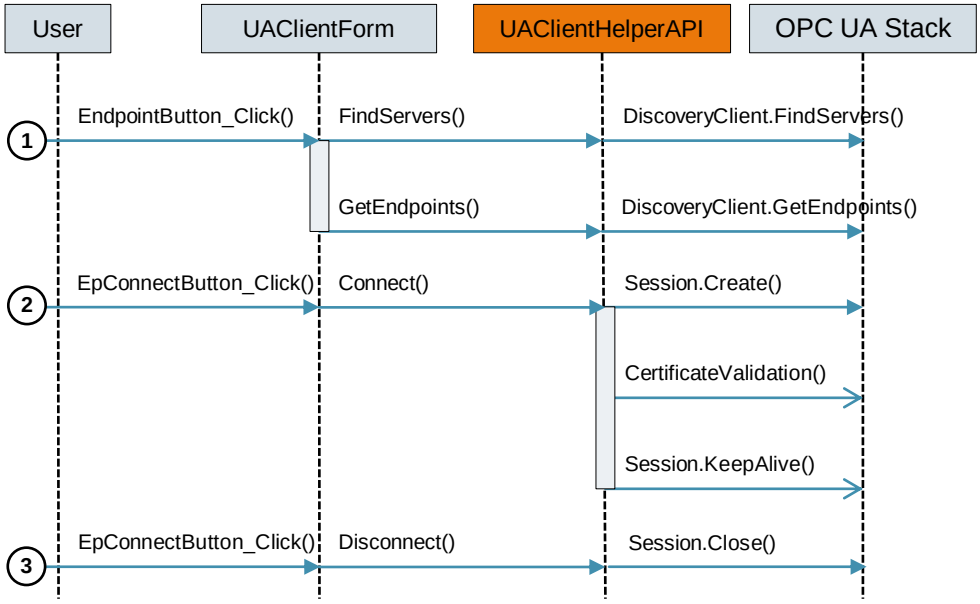


Table 2-4

No.	Description
1.	Via the “Get Endpoints” button, the EndpointButton_Click() method of the interface is called which in turn calls the FindServers() and GetEndpoints() methods of the UAClientHelperAPI. As a result, the user receives all available endpoints in the network (if a LDS or GDS is available) or of a server.
2.	Once the user has selected an endpoint from the list and has clicked the “Connect to server” button, the EpConnectButton_Click() UI method is called. This calls the Connect() method of the UAClientHelperAPI. A session object and another object for the Session.Create() method is created and filled. Once the Session.Create() is executed, it is responded to an arriving CertificateValidation event via which the server certificate can be validated.
3.	When the button is clicked again the EpConnectButton_Click() method is executed again. If a connection already exists, the Disconnect() method of the UAClientHelperAPI is executed. This ends the existing session via the OPC UA stack session.Close() method.

Browsing on the OPC UA server

The following sequence diagram shows the procedures, in order to browse nodes in the OPC UA address space of the server.

Figure 2-5

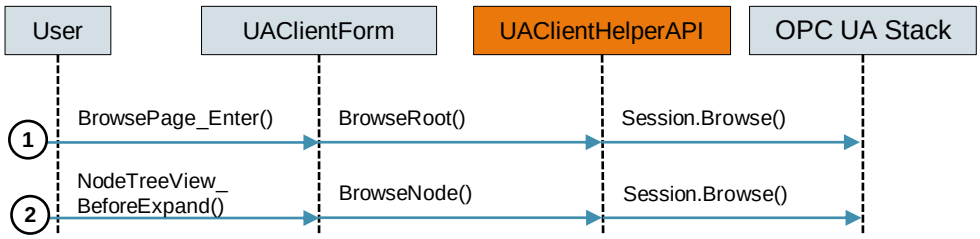


Table 2-5

No.	Description
1.	As soon as the user in the client example goes to the “Browse Nodes” tab, the BrowsePage_Enter() UI method is called. This calls the BrowseRoot() method of the UAClientHelperAPI. In this, the Session.Browse() method of the OPC UA stack is called with the suitable transfer parameters, in order to browse the root node of the server.
2.	When a node of the tree view of the address space is be expanded, the NodeTreeView_BeforeExpand() UI method is called. This calls the BrowseNode() method of the UAClientHelperAPI. In this, the Session.Browse() method of the OPC UA stack is called with the suitable transfer parameters, in order to browse any node of the server.

Reading and writing tags

The following sequence diagram shows the procedures, in order to read or write tags:

Figure 2-6

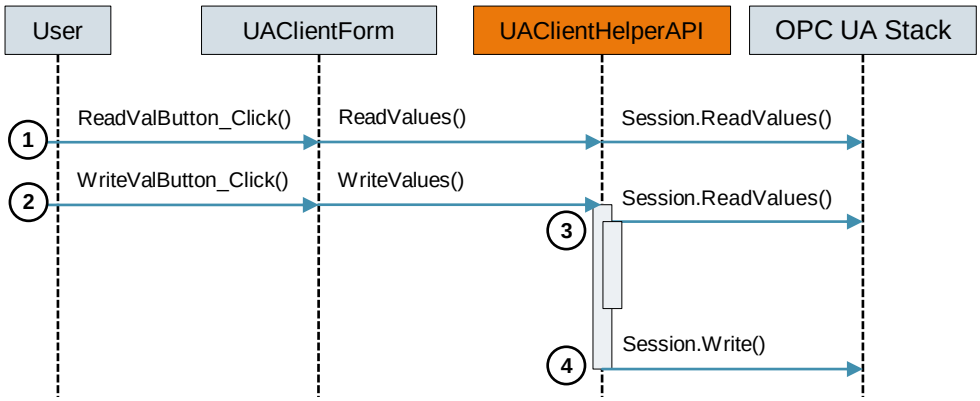


Table 2-6

No.	Description
1.	When you click the “Read” button, the ReadValButton_Click() UI method is called. It transfers the ReadValues() method a list of node ID strings to the UAClientHelperAPI. From the transmitted string list a node ID list is created and transferred to the Session.ReadValues() OPC UA stack method. This method reads all values of the node IDs of the list and returns them.
2.	When you click the “Write” button, the WriteValButton_Click() UI method is called. This transfers the WriteValues() method a list of node ID strings to the UAClientHelperAPI.
3.	Node IDs are created from the transmitted strings. These are read via the Session.ReadValues() method, in order to determine their data types.
4.	The Session.Write() method writes the values to the server via the determined data types and node IDs.

Registering node IDs

The following sequence diagram shows the procedures, in order to register node IDs on the OPC UA server. Optimized read and write operations can be executed via these registered IDs.

Figure 2-7

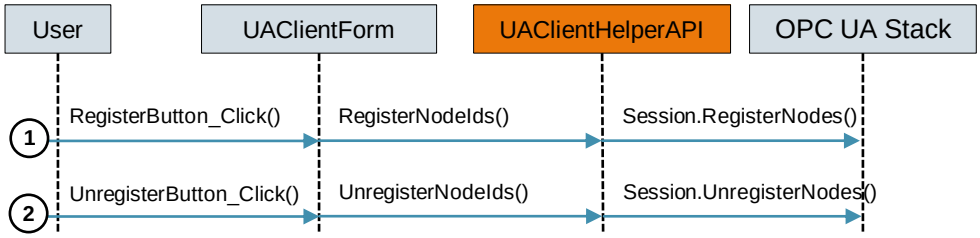


Table 2-7

No.	Description
1.	When you click the “Register” button, the RegisterButton_Click() UI method is called. This transfers the RegisterNodeIds() method a list of node ID strings to the UAClientHelperAPI. From the transmitted string list, a node ID list is created and transferred to the Session.RegisterNodes() OPC UA stack method. This method registers all node IDs of the list.
2.	When you click the “Unregister” button, the UnregisterButton_Click() UI method is called. This transfers the UnregisterNodeIds() method a list of node ID strings to the UAClientHelperAPI. From the transmitted string list, a node ID list is created and transferred to the Session.UnregisterNodes() OPC UA stack method. This method cancels the registration of all transferred node IDs.

Subscribing/ending subscriptions

The following sequence diagram shows the procedures, in order to subscribe or end subscriptions to certain tags:

Figure 2-8

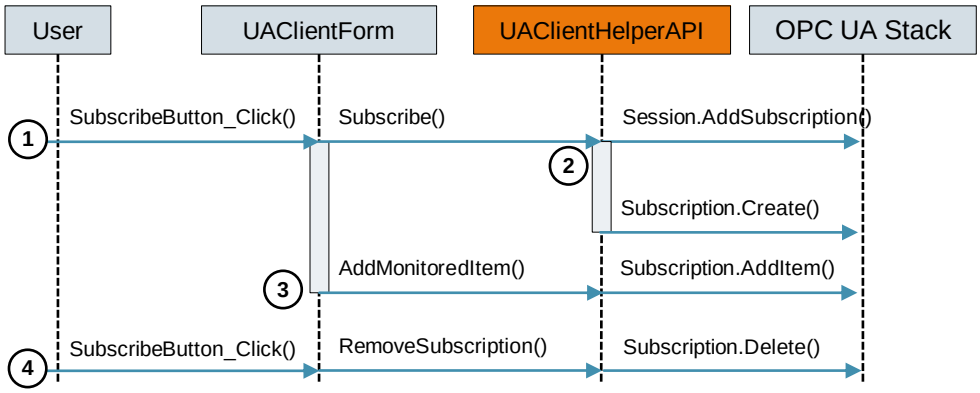


Table 2-8

No.	Description
1.	When you click the “Subscribe” button, the SubscribeButton_Click() UI method is called. This calls the Subscribe() method of the UAClientHelperAPI.
2.	Within the Subscribe() method, a subscription is created, transferred to the session (Session.AddSubscription) and enabled (Subscription.Create()).
3.	Within the SubscribeButton_Click() UI method a monitored item is created once a subscription has been created and transferred to the AddMonitoredItem() method of the UAClientHelperAPI. This adds the transferred MonitoredItem via the Subscription.AddItem() method to the subscription.
4.	When you click the “Subscribe” button again, the UnregisterButton_Click() UI method is called. This calls the RemoveSubscription() method of the UAClientHelperAPI. Within this method, the Subscription.Delete() UA stack method is called that ends the subscription on the server.

2.3 Operation

The following step-by-step instructions show you how you can commission the application example and how you can operate it.

2.3.1 Description of the user interface

The user interface of the “OPC UA Client S7-1500” example client is divided in four tabs:

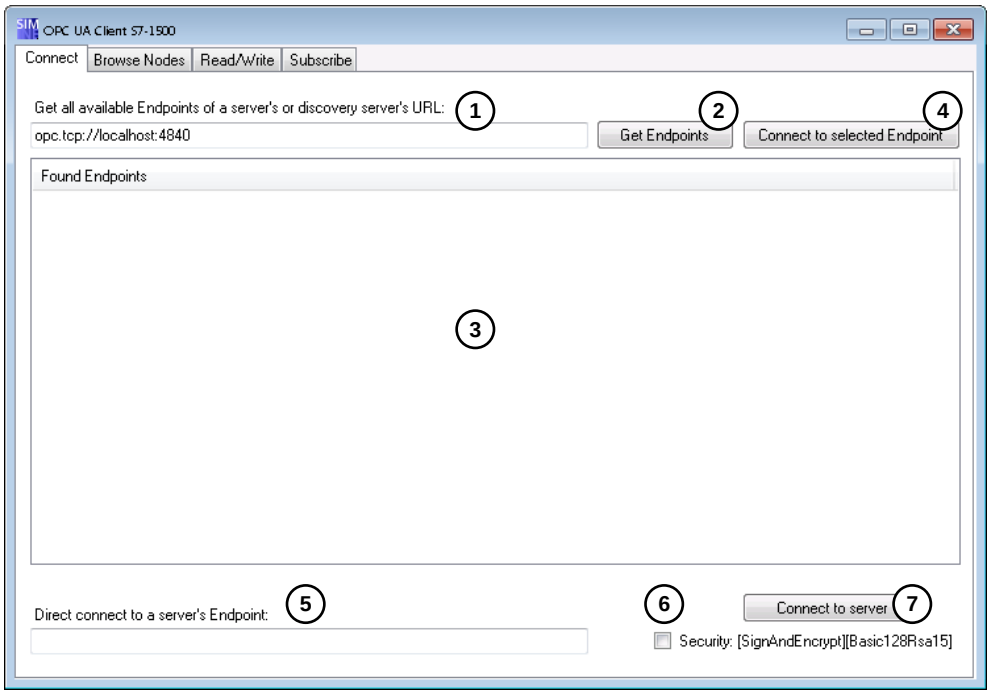
- “Connect”
- “Browse Nodes”
- “Read/Write”
- “Subscribe”

The descriptions below explain the individual tabs in more detail:

“Connect”

The following figure shows the interface of the “Connect” tab.

Figure 2-9



The following table describes the functions of the interface of the previous figure:

Table 2-9

No.	Description
1.	Text field to enter an OPC UA (Discovery) server URL.
2.	Button to search OPC UA endpoints with the URL from the text field (1).
3.	List of the OPC UA endpoints found.

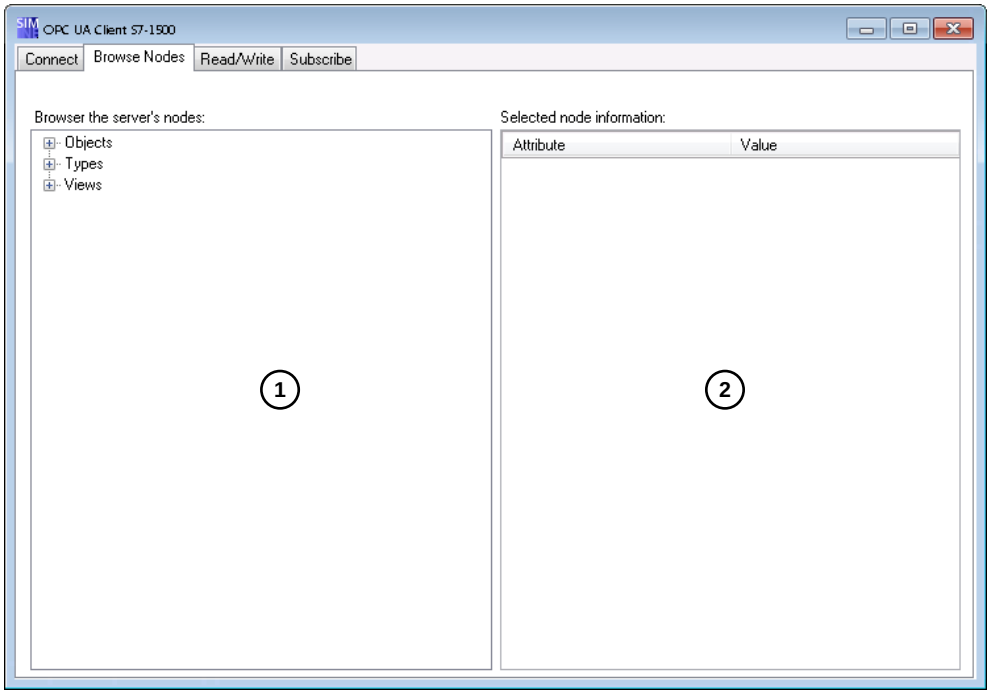
No.	Description
4.	Button to establish a connection to a selected endpoint of the list (3).
5.	Text field to enter an OPC UA server URL.
6.	Check box to select the preferred connection and transmission type to server URL from text field (5): • Enabled: Signs and encrypts via a software certificate and the “Basic128Rsa15” encryption algorithm. • Disabled: No signing or encryption.
7.	Button to establish a connection to server URL from text field (5).

Note In order to access the “Browse Nodes”, “Read/Write” and “Subscribe” tabs, you have to be connected with an OPC UA server.

“Browse Nodes”

The following figure shows the interface of the “Browse Nodes” tab.

Figure 2-10



The following table describes the functions of the interface of the previous figure:

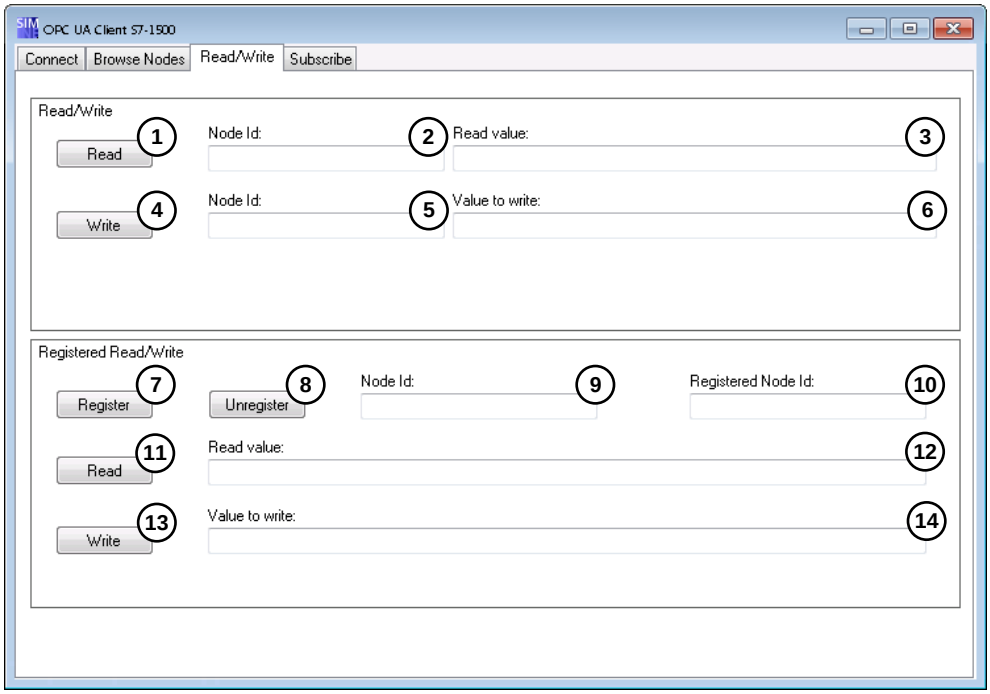
Table 2-10

No.	Description
1.	Tree view of the available nodes on the OPC UA server.
2.	Data view of the attributes of a selected node from the tree view (1).

“Read/Write”

The following figure shows the interface of the “Read/Write” tab.

Figure 2-11



The following table describes the functions of the interface of the previous figure:

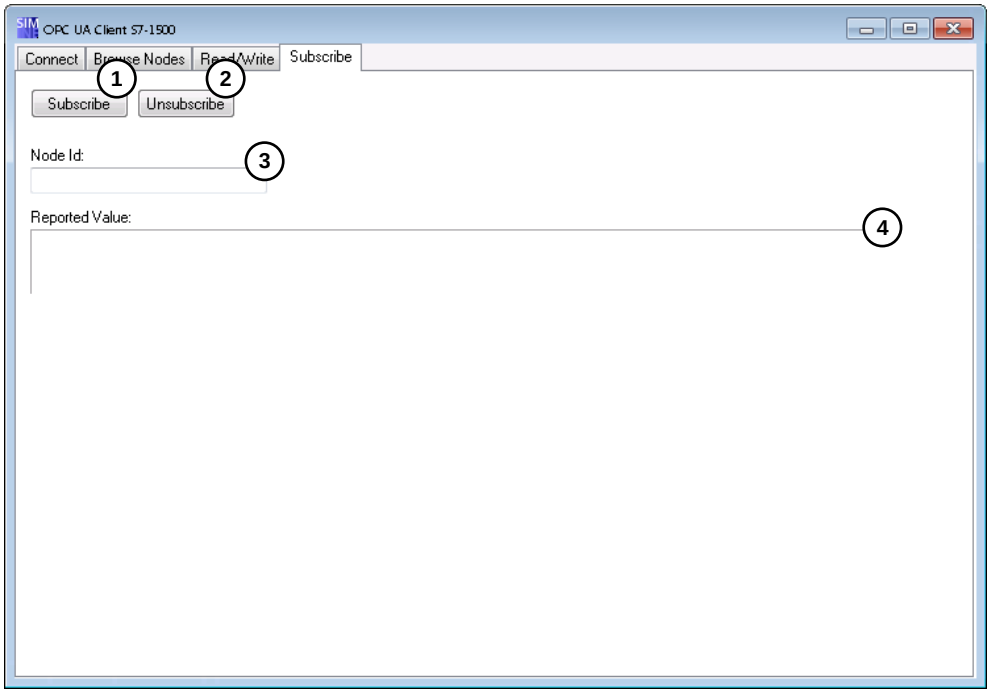
Table 2-11

No.	Description
1.	Button to read an entered node ID from text field (2).
2.	Text field to enter a node ID to be read.
3.	Text field to output the value of the read node ID from text field (2).
4.	Button to write an entered node ID from text field (5).
5.	Text field for entering a node ID to be written.
6.	Text field to enter the value of the node ID to be written from text field (5).
7.	Button to register an entered node ID from text field (9).
8.	Button to cancel the registration of an entered node ID from text field (9).
9.	Text field to enter a node ID to be registered.
10.	Text field to output a registered node ID.
11.	Button to read a registered node ID from text field.
12.	Text field to output the value of the read registered node ID from text field.
13.	Button to write a registered node ID.
14.	Text field to enter the value of the node ID to be written.

“Subscribe”

The following figure shows the interface of the “Subscribe” tab.

Figure 2-12



The following table describes the functions of the interface of the previous figure:

Table 2-12

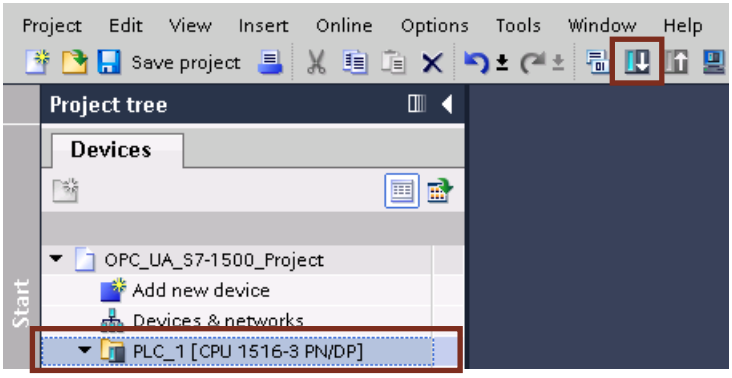
No.	Description
1.	Button to start a subscription on an OPC UA server and to create a MonitoredItem via the node ID from text field (2).
2.	Button to end a subscription and to delete the MonitoredItem.
3.	Text field to enter a node ID that is added as MonitoredItem of the subscription.
4.	Text field to output the value of the MonitoredItem of the subscription with time stamp and status.

2.3.2 Commissioning OPC UA server of the S7-1500

Carry out the configurations steps in chapter 2.1 “Configuring the OPC UA server of the S7-1500” or download the pre-prepared TIA Portal project into your controller. Proceed as follows:

1. Download the “109737901_OPC_UA_Client_S7-1500_CODE_V10.zip” project onto your hard drive. The download can be found on the HTML page of this entry (https://support.industry.siemens.com/cs/ww/en/view/109737901).
2. Unzip the project.

3. Navigate to “OPC_UA_Server_1500” in the unzipped folder. The TIA Portal project is located in this folder.
4. Open the project by double-clicking the “UA Server 1500.ap14” file.
5. Select the CPU in the project navigation and load the project into the controller.



2.3.3 Commissioning OPC UA Client S7-1500

The example client is provided via a Visual Studio project.

1. Download the “109737901_OPC_UA_Client_S7-1500_CODE_V10.zip” project onto your hard drive. The download can be found on the HTML page of this entry (https://support.industry.siemens.com/cs/ww/en/view/109737901).
2. Unzip the project.
3. Navigate to “OPC_UA_Client_1500” > “UA_Client_1500” > “Application” in the unzipped folder. The compiled executable .EXE file of the OPC UA example client is located in this file.
4. Start the program by double-clicking the “UA Client 1500.exe” file.
5. Confirm the message of the user account control with “Yes”.

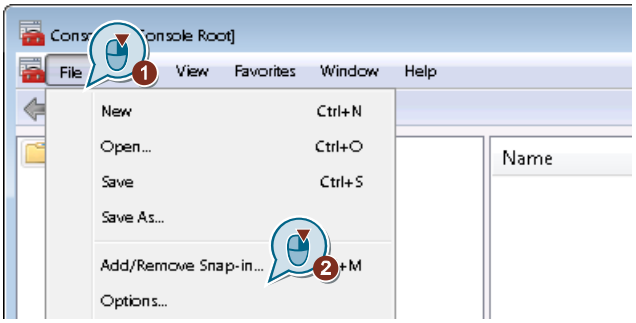
Note The example client requires the rights of the user account control, in order to get access to the Windows Certificate Store. The certificates created by the example client are stored or searched in this store.

2.3.4 Creating, exporting and loading client certificate into the S7-1500 (optional)

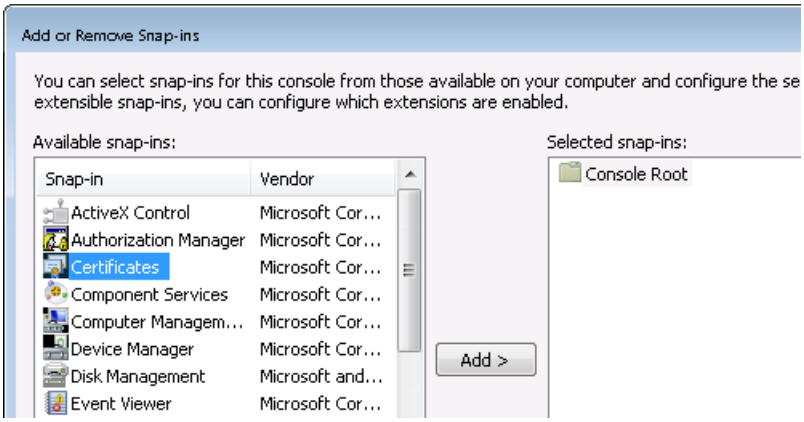
If you want to increase the security of your application via the certificate management, please follow the following steps:

1. Start the OPC UA Client S7-1500.
2. During the first program start, a software certificate of the client program is created and stored in the Windows Certificate Store. This certificate has to be known by the OPC UA server if you want to communicate signed and encrypted with a server.

3. Click on “Start” > “Run” in Windows and enter “mmc". Confirm with the “Enter” button.
4. In the now opened certificate store click “File” > “Add/Remove Snap-in…”.

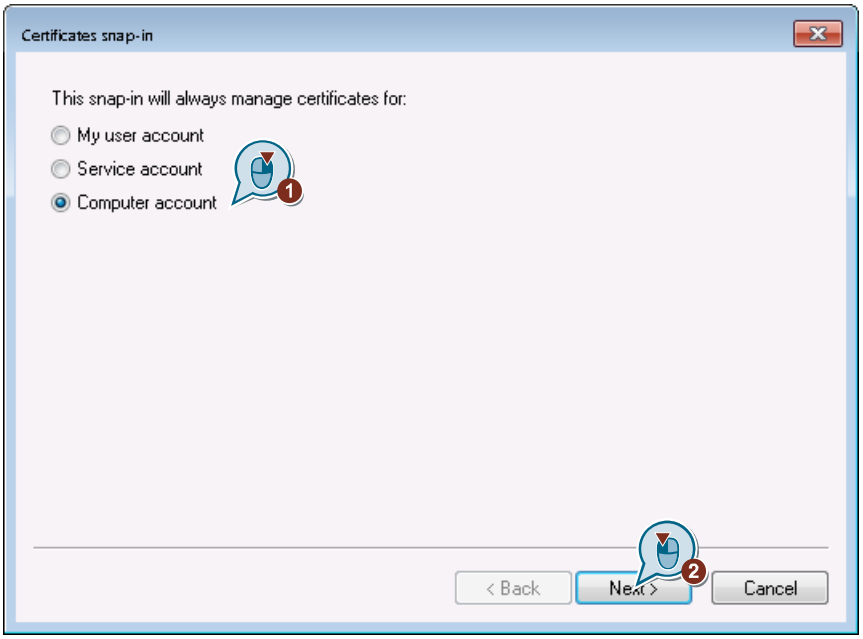


5. Search for “Certificates” in the dialog that appears, select it and click “Add >”.



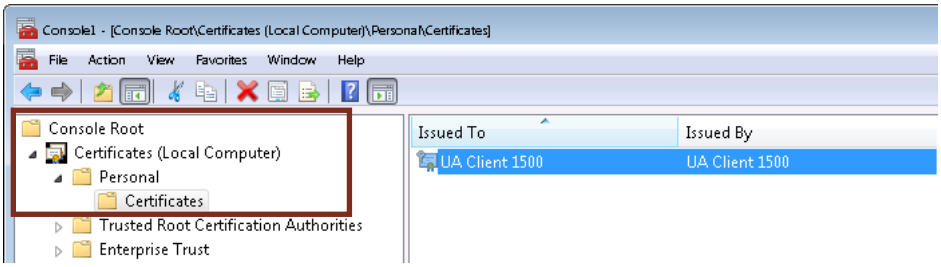
6. Select the “Computer account” check box and confirm with “Next >”.

Figure 2-13

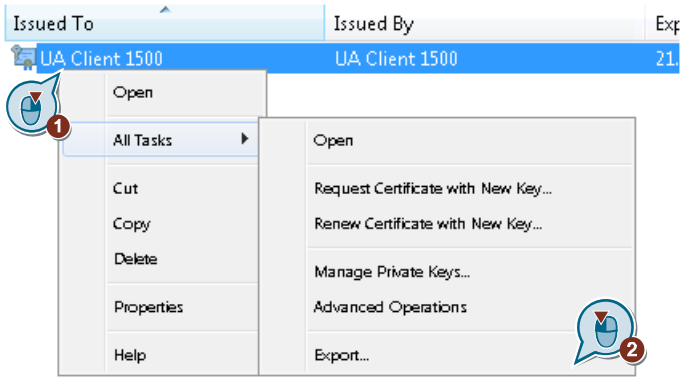


7. Click “Finish” in the next dialog.

8. Then click “OK” to confirm.
9. Navigate from the “Console Root” to “Certificates” (Local Computer) > “Personal” > “Certificates”.

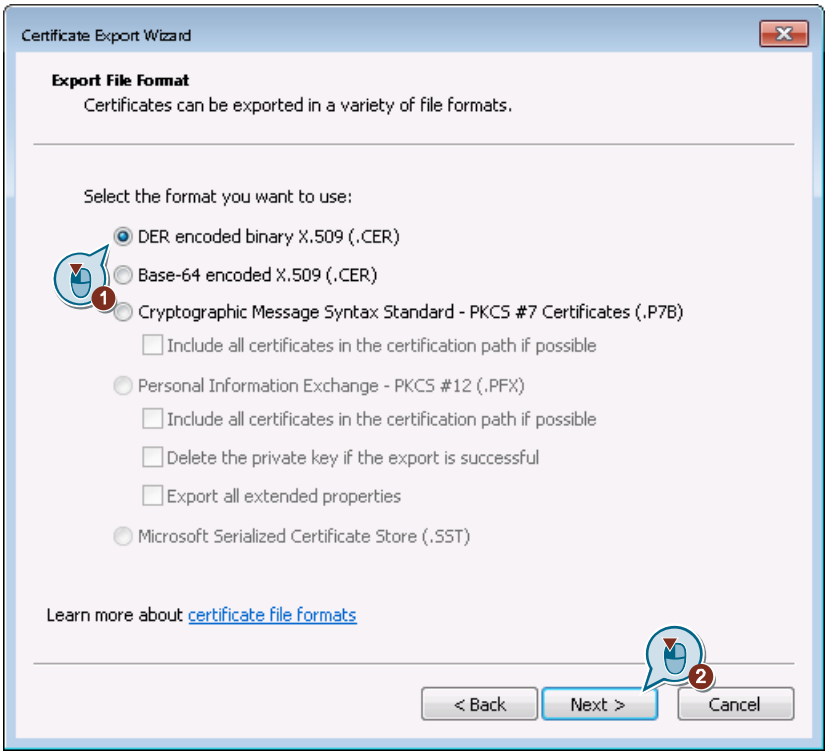


10. Right-click the “UA Client 1500” certificate that has been created by the example client and navigate to “All Tasks” in the context menu. Then click on “Export…”.

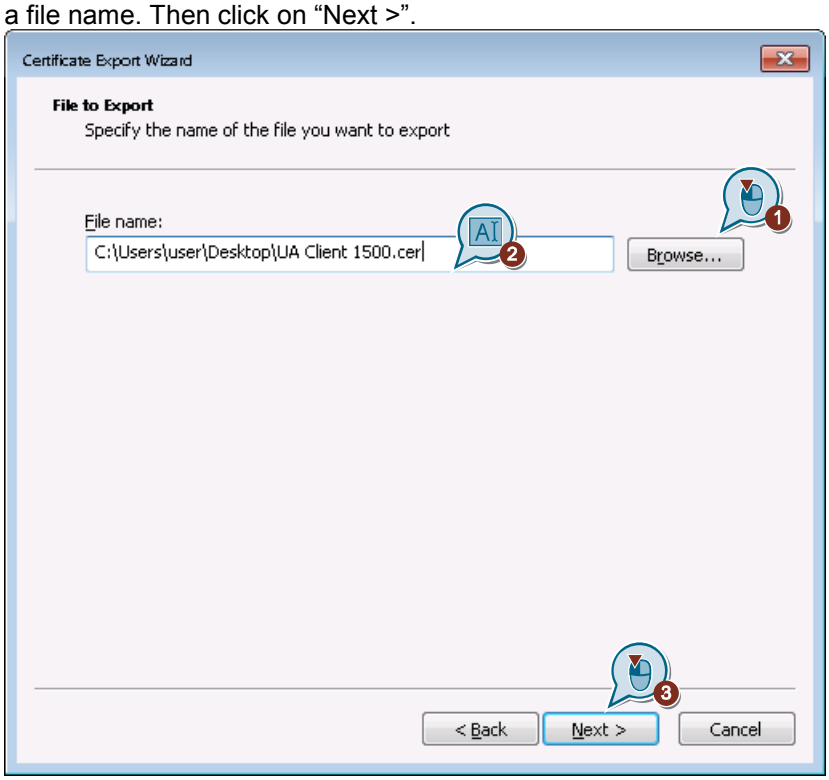


11. In the dialog that appears then, click “Next”.
12. Select the “No, do not export private key” check box and click on “Next >”.

13. Select the “DER encoded binary X.509 (.CER)” check box and then click “Next >”.



14. Select a suitable storage location for the certificate via “Browse…” and assign a file name. Then click on “Next >”.



15. Click “Finish” in the dialog that follows.

16. The certificate is now stored in the selected storage location and can be imported into the TIA Portal or into other OPC UA servers from there.
17. (Optional) Follow the configuration instructions in chapter 2.1.4 “Security via certificate management (optional)”.

2.3.5 Establishing connection to the OPC UA server

You have two options to connect with an OPC UA server:

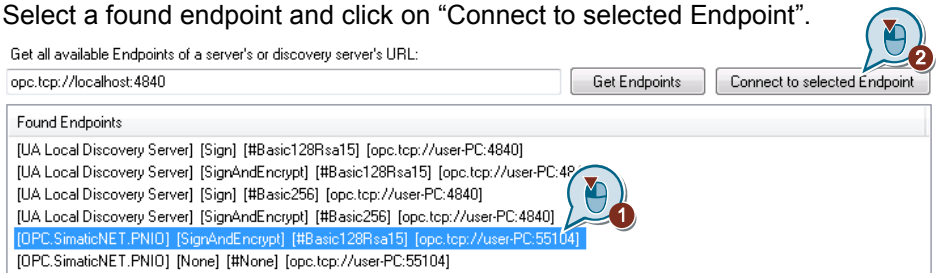
- Establishing connection via an endpoint browser
- Direct connection establishment via an OPC UA server URL.

The example client accepts all certificates of the OPC UA servers automatically.

Establishing connection via an endpoint browser

1. Enter the URL of an OPC UA server, LDS or GDS into the text field. Click the “Get Endpoints” button.

2. Select a found endpoint and click on “Connect to selected Endpoint”.



Note The OPC UA server of the S7-1500 does not have a discovery endpoint and this is why it cannot be found via LDS or GDS.

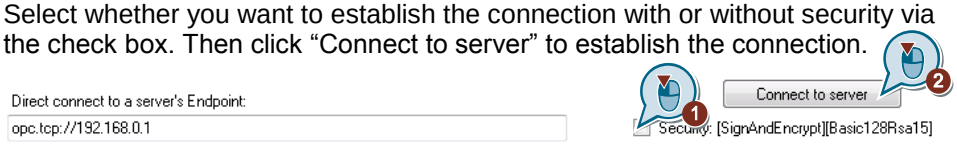
Note If you want to connect to “Sign” or “SignAndEncrypt” endpoints, the client certificate of the example client has to be known to the server and be accepted.

3. When you are successfully connected with a server, the text on the buttons change to “Disconnect from Server”.
4. You can disconnect the session and connection to the OPC UA server again via the “Disconnect from Server” button.

Direct connection establishment via an OPC UA server URL

1. Enter an OPC UA server URL (for example, that of the server of the S7-1500) into the text field.

2. Select whether you want to establish the connection with or without security via the check box. Then click “Connect to server” to establish the connection.



   When the check box is set, an encrypted (Basic128Rsa15) and signed connection to the server is established. When the check box is not set, an endpoint of the server is connected without these properties.

Note

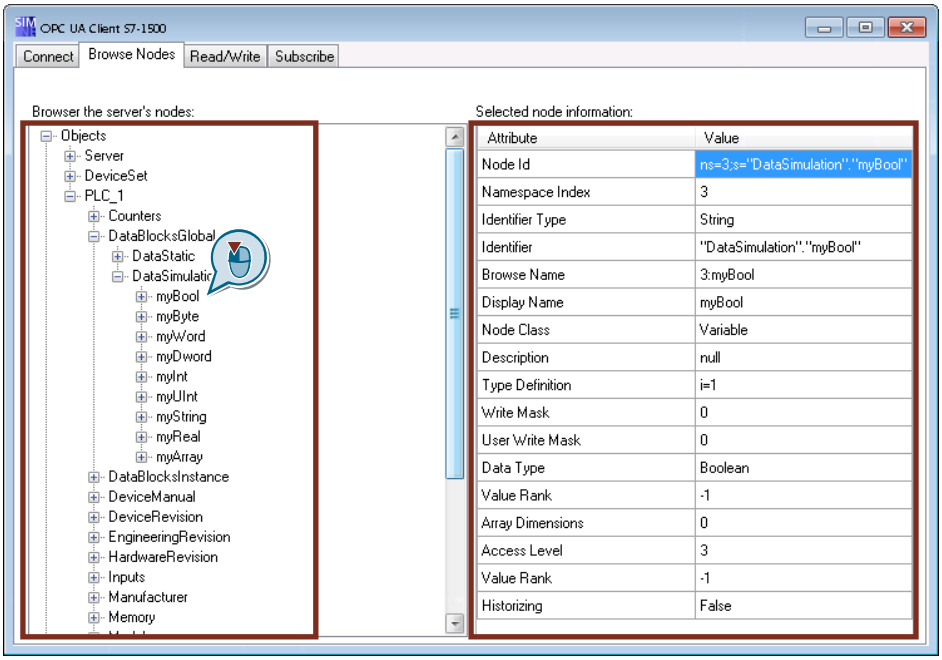
The endpoints [Sign&Encrypt; Basic128Rsa15] and/or [none;none] have to be enabled via the configuration in the OPC UA server of the S7-1500. Please note chapter 2.1.3 “Configuring OPC UA security policies (server endpoints)”.

3. When you are successfully connected with a server, the text on the buttons change to “Disconnect from Server”.
4. You can disconnect the session and connection to the OPC UA server again via the “Disconnect from Server” button.

2.3.6 Browsing address space of the OPC UA server

You can navigate via the “Browse Nodes” tab within the address space of the OPC UA server.

1. Connect with an OPC UA server.
2. Go to the “Browse Nodes” tab.
3. In the tree you can browse through the individual nodes in the address space of the OPC UA server. When you are clicking on a node in the tree you will receive specific information on the selected node on the right side in the data view.



Note The information of the data view displayed, depends on the node class of the selected node (object, tag und data type).

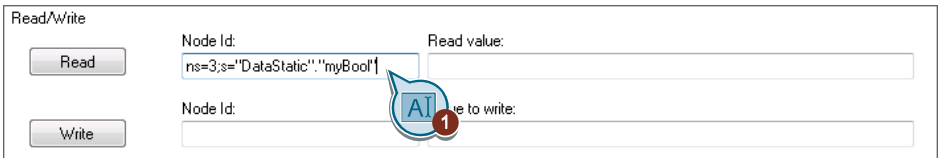
2.3.7 Read/write tags

Data access to tags of an OPC UA server is realized and shown to you in the “Read/Write” tab.

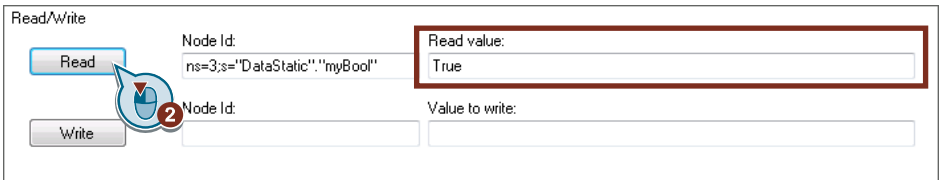
1. Connect with an OPC UA server.
2. Go to the “Browse Nodes” tab and navigate to a tag node that you want to read or write.
3. Click on the node of the tag and copy the value of the “Node Id” field from the data view with the <CTRL+C> button combination.
4. Go to the “Read/Write” tab.

Reading tag nodes

1. Add the previously copied node ID with the CTRL-V key combination into the upper field “Node Id:” of the “Read/Write” field.

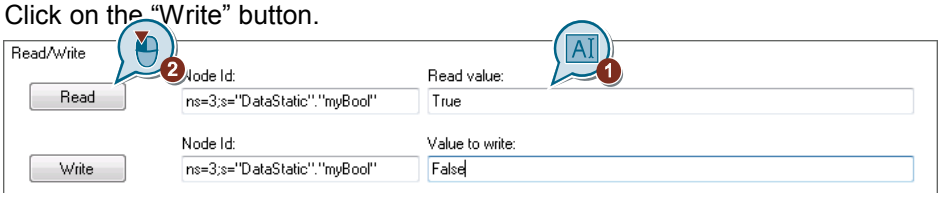


2. Click on the “Read” button. The read value is output in the “Read value:” text field.



Reading tag nodes

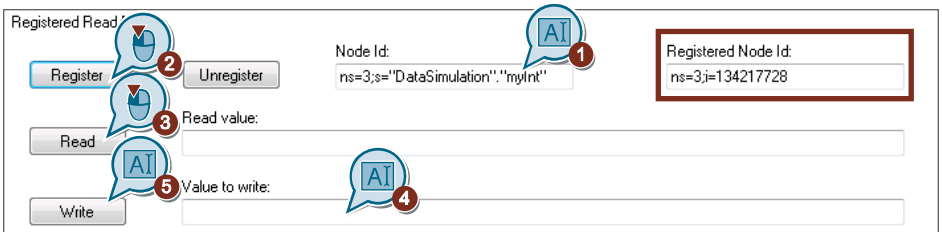
1. Add the previously copied node ID with the CTRL-V key combination into the bottom field “Node Id:” of the “Read/Write” area. Enter the value to be written into the “Values to write:” field (in this example the Boolean value “False”). Click on the “Write” button.



2. The write operation was successful when there is no error message.
3. You can read the tag again to check it.

Registered read/write

1. Add the previously copied node ID with the CTRL-V key combination into the “Node Id:” field of the “Registered Read/Write” area and click the “Register” area. The registered or optimized node ID is displayed in the “Registered Node Id:” field.



Note The registered node ID does not necessarily differ from the original.

2. Click on the “Read” button, in order to read the registered node ID. The read value is shown in the “Read value:” field.
3. Enter a value in the “Values to write:” field.
4. Click on the “Write” button, in order to write the previously entered value to a registered node.
5. The write operation has been carried out successfully when no error message is output.
6. You can read the tag again to check it.

7. Click on the “Unregister” button, in order to release a registered node ID.

2.3.8 Subscriptions

You get value changes or updates of tags via a subscription, without ordering cyclic reading.

1. Connect with an OPC UA server.
2. Go to the “Browse Nodes” tab and navigate to a tag node that you want to read or write.
3. Click on the node of the tag and copy the value of the “Node Id” field from the data view with the <CTRL+C> button combination.
4. Go to the “Subscribe” tab.
5. Add the previously copied node ID with the CTRL-V key combination into the “Node Id:” field. Click the "Subscribe" button.

6. In the “Reported Value:” text field, value, status, source and server time stamp of the MonitoredItems are displayed.

Note In this example the publishing interval of the subscription is set to 1000ms and the sampling interval of the MonitoredItems is set to 1ms.

7. Click the “Unsubscribe" button to end the subscription.

3 Valuable Information

3.1 Basics

3.1.1 General OPC UA information

Overview

In recent years, the OPC Foundation (an interest grouping of well-known manufacturers for the definition of standard interfaces) has defined a large number of software interfaces to standardize the information flow from the process level to the management level. According to the different requirements within an industrial application, different OPC specifications have been developed in the past: Data Access (DA), Alarm & Events (A&E), Historical Data Access (HDA) and Data eXchange (DX). Access to process data is described in the DA specification, A&E describes an interface for event-based information, including acknowledgement, HDA describes functions for archived data and DX defines a lateral server to server communication.

Based on the experience with these classic OPC interfaces, the OPC Foundation defined a new platform, called OPC Unified Architecture (UA). The aim of this standard is the generic description and uniform access to all information which is to be exchanged between systems or applications. This includes the functionality of all previous OPC interfaces. Furthermore, this has generated the option of natively integrating the interface into the appropriate system, irrespective of which operating system the system is operated on and irrespective of the programming language in which the system was created.

Further information is available on the homepage or the OPC Foundation (\5\).

What is OPC?

In the past, OPC was a collection of software interfaces for data exchange between PC applications and process devices. These software interfaces have been defined according to the rules of Microsoft COM (Component Object Model) and can therefore be easily integrated into Microsoft operating systems. COM or DCOM (Distributed COM) provides the functionality of inter process communication and organizes the information exchange between applications, even across network boundaries (DCOM). Using mechanisms of the Microsoft operating system, an OPC client (COM client) can use it to exchange information with an OPC server (COM server).

The OPC server provides process information of a device at its interface. The OPC client connects itself with the OPC server and can access the offered data.

The use of COM or DCOM causes OPC servers and clients to run only on a Windows PC or in the local network and that the communication to the respective automation system has to be realized mainly via proprietary protocols. Additional tunneling tools often have to be used for the network communication between client and server in order to get through firewalls or to avoid the complicated DCOM configuration. The interface can furthermore only be accessed natively with C++ applications; .NET or JAVA applications can only gain access via a wrapper layer. These restrictions lead to additional communication and software layers which increase the configuration workload and the complexity.

Due to the widespread use of OPC, the standard is increasingly used for the general connection of automation systems and no longer only for the original application as the driver interface in HMI and SCADA systems to access process information.

To solve the mentioned restrictions in real-life situations and to fulfill the additional requirements, the OPC Foundation has defined a new platform in the last 7 years, called OPC Unified Architecture, which offers a uniform basis for the exchange of information between components and systems. OPC UA is available as an IEC 62541 standard and therefore also forms the basis for other international standards.

OPC UA offers the following features:

- Summary of all previous OPC features and information such as DA, A&E and HDA in a generic interface.
- Use of open and platform-independent protocols for inter-process or network communication.
- Internet access and communication by means of firewalls.
- Integrated access control and security mechanisms on protocol and application level.
- Extensive representation options for object-oriented models; objects can have tags and methods and can fire events.
- Expandable type system for objects and complex data types.
- Transport mechanisms and modeling rules form the basis for other standards.
- Scalability of small embedded systems up to business applications and from simple DA address spaces up to complex, object-oriented models.

3.1.2 OPC UA address space

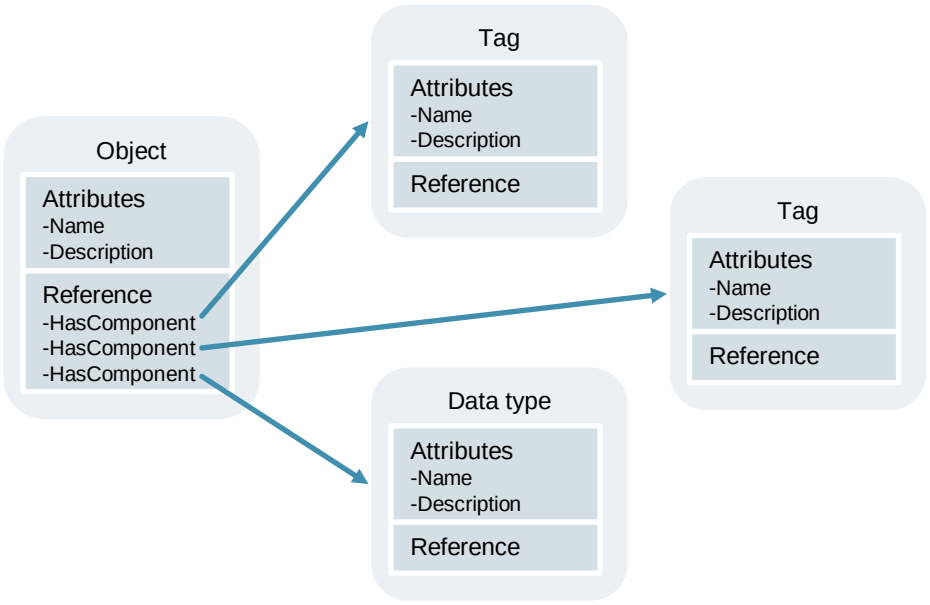
The following descriptions explain the address space of an OPC UA server.

Nodes in the address space

A node in the OPC UA address space is of a certain type, such as, for example, object, tag or method and is described by a list of attributes. All nodes have joint attributes such as name or description and specific attributes such as, for example, the value of a tag. The list of attributes cannot be extended. Additional information on the node can be added as property. Properties are a special type of tag. The nodes are interconnected with references. The references are typified. There are two main groups: Hierarchical references, such as, for example, HasComponent for the components of an object or non-hierarchical references such as, for example, HasTypeDefinition for a connection of an object instance to an object type.

The following figure shows an example for nodes and the connecting references:

Figure 3-1



Available types of nodes in the address space

The following table shows the node types defined in the standard.

Table 3-1

Node type	Description
Object	An object is used as typified container or folder for tags, methods and events.
Tag	Tags represent the data of objects or the properties of a node as attributes.
Method	Methods are components of objects and can have a list of input or output parameters. The parameters are described via defined attributes.
View	Views represent a part of the address space. The node is used as access point and as filter when browsing.
Object type	Object types supply information on the structure or the components of an object.
Tag type:	Tag types typically describe which attributes or data types can be found in an instance of a tag.
Reference type	Reference types define the possible types of references between nodes.
Data type	Data types describe the content of the value in a tag.

Name spaces and node IDs

Each node in the OPC UA address space is uniquely identified by a node ID. This node ID is made up of a namespace to distinguish codes from different subsystems and a code which can either be a numerical value, a string or a GUID.

Strings are typically used for the ID. This is analog to OPC Data Access, where the item ID as identifier is also a string. Numerical values are used for statistical namespaces such as, for example, type system. OPC UA defines a namespace with associated namespace index for the nodes defined by the OPC Foundation. The OPC UA servers additionally define one or several namespaces with index.

The namespaces defined by the servers are variable and can change. This is why it is recommended to request the current namespace for the client when establishing the session.

The figure below explains the structure of a node ID:

Figure 3-2

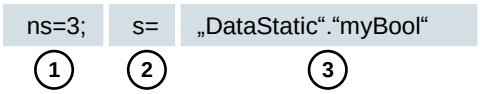


Table 3-2

No.	Description
1.	Namespace index
2.	Node ID type (s=String; i=Numeric: g=GUID)
3.	ID

Attributes of the nodes

The table below explains the most important node attributes:

Table 3-3

Attribute	Node type	Description
Node ID	All	The unique node ID with namespace index
Namespace index	All	The namespace index that is assigned to the node.
Identifier Type	All	The node ID type
Identifier	All	The unique node ID within the namespace index
Browse Name	All	The browse name
Display Name	All	The display name
Node Class	All	The node class (object, tag, data type)
Description	All	Short description of the node
Type Definition	All	Reference for data type description of the tag
Write Mask	All	Write rights to node attributes (0=no, 1=yes) without consideration of user groups
User Write Mask	All	Write rights to node attributes (0=no, 1=yes) without consideration of the current user
Data Type	Tag	Data type of the tag
Value Rank	Tag	Value type of the tag (none, scalar, vector, array)
Array Dimensions	Tag	Number of array dimensions
Access Level	Tag	Access authorization (read, write, read/write) to the node
Minimum Sampling Interval	Tag	The smallest possible sampling interval of the tag on the server side
Historizing	Tag	Course of time of the tag available on server (yes, no)

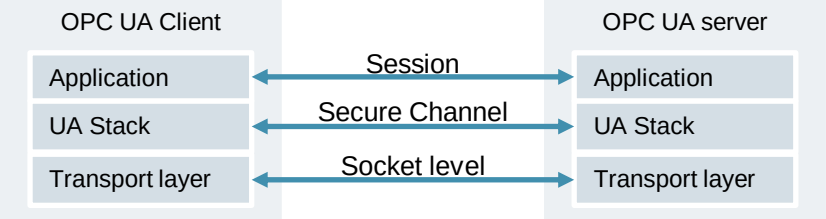
3.1.3 OPC UA Security

The following explanations outline the security concept of OPC UA.

Security layers

The following figure gives an overview of the security layers of OPC UA

Figure 3-3



The user authentication is carried out via the **Session**. This is done, for example, through a user name and a password or via certificates.

Via a **Secure Channel** the applications are mutually authenticated and a message-based security of the communication is performed. Each message is signed and encrypted to ensure the integrity and secrecy of the messages. Basis of these mechanisms are certificates (X509) which uniquely identify the applications based on a Public Key Infrastructure (PKI) system.

On the **socket level**, a connection-oriented security of the socket connection via Secure Socket Layer (SSL) or via Virtual Private Network (VPN) can be used in addition or as an alternative to the secure channel.

Configuration options for the security

The following table describes the different configuration options for the security mechanisms.

Table 3-4

Option	Description
Security Policy	**None** – In the secure channel no security is used. **Basic128Rsa15** – Set of encryption algorithms. **Basic256** – Set of expandable encryption algorithms.
Message Security Mode	**None** – The messages are not secured. **Sign** – The messages are signed. **Sign&Encrypt** – The messages are signed and encrypted.
User Authentication	**Anonymous** – User authentication is not necessary. **User Password** – The user authentication is performed using user names and password. **Certificate** – The user authentication is performed using a certificate.

Certificate exchange between client and server

When all applications involved, implement the guidelines of the OPC UA regarding the security configuration, only one manual step (4) is necessary at the server for the exchange of certificates, since the certificates are automatically exchanged between the applications and the certificates only have to be accepted by an administrator.

The following figure illustrates the certificate exchange between client and server:

Figure 3-4

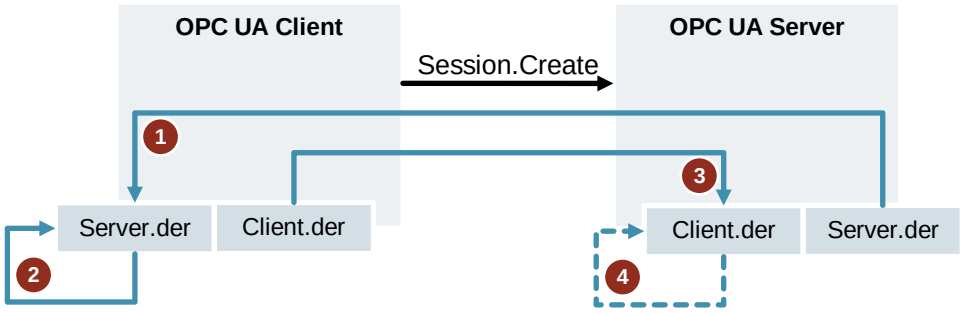


Table 3-5

No.	Description
1.	When establishing a connection to the server (Session.Create) the client receives the server certificate via the server endpoint.
2.	The client program can then decide how it deals with the certificate: Reject or accept.
3.	In the same process the client sends its certificate to the server. The server rejects the certificate at first and then stores it in a reject folder.
4.	As a result, the client certificate has to be accepted manually by an administrator on the server. In most cases, this is done by an administrator copying the client certificate from a reject folder into a trusted folder.

Note For the OPC UA Server of the S7-1500 the client certificate has to be loaded via the TIA Portal onto the controller, in order to accept it.

3.1.4 OPC UA server of the S7-1500

This chapter gives you an overview of some key data of the OPC UA server of the S7-1500. Additionally, notes and tips in handling the server are also given.

Note Further information on the OPC UA server of the S7-1500 can be found in the “Function Manual: S/-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Communication” (\4\).

Supported OPC UA services of the S7-1500 data access

The OPC UA server of the S7-1500 currently supports the following services for data access:

- Read
- Write
- Registered read/write
- Subscriptions

Performance when accessing many tags of the server

When you want to read or write many tags from a S7-1500, you can increase the performance considerably by structuring the tags on the S7-1500. To do this, use arrays and structures, in order to declare read/write tags.

Viewed individually, arrays are the most performant. They are faster by factor 2 to 3 than structures and they are faster by factor 10 to 100 than individual accesses (by a number of approximately 1000 tags).

Use the “Registered read/write” for recurring accesses, in order to increase the performance.

License concept

Table 3-6

CPU type	ET 200SP CPU up to S7-1513(F)	1515 / 1516(F)	1517 / 1518(F)
Required license	Small	Medium	Large

3.2 TIA Portal project details

The explanation below describes the TIA Portal project included in this application example.

3.2.1 S7-1500 and OPC UA configuration

The following configuration steps from chapter 2.1 “Configuring the OPC UA Servers of the S7-1500” have already been carried out for you in the TIA Portal project of this entry.

- The OPC UA server is enabled.
- The global security settings are enabled.
- The server endpoints are set up.
- The tags for the OPC UA communication are enabled.

Only the settings in chapter 2.1.4 “Security via certificate management” are optional and can still be carried out by you, in order to additionally increase the security in the project.

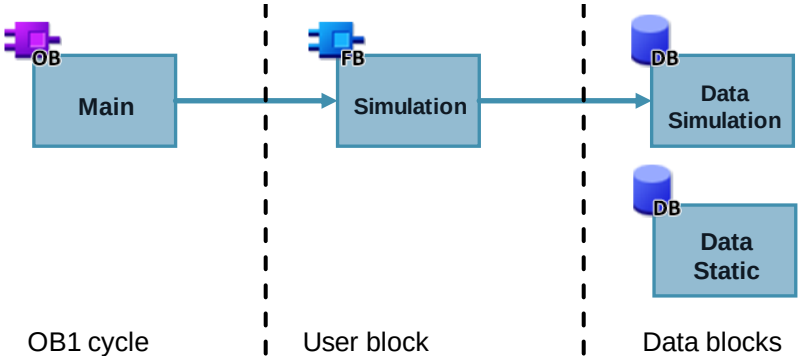
3.2.2 S7 program

The S7 program of the TIA project consists of the OB1, a user block and two data blocks.

Call hierarchy

The following figure shows the call hierarchy of the S7 user program.

Figure 3-5



Explanation of the blocks

In the cyclic user program only the “Simulation” function block is called. This FB creates pseudo-randomly generated values and fills the tags in the “DataSimulation” data block with it. The “DataStatic” data block includes predefined tags with statistic values.

In this application example, both data blocks include the exemplary process tags to which the OPC UA clients may access externally.

4 Appendix

4.1 Siemens services

Industry Online Support

Do you have any questions or need support?

Siemens Industry Online Support offers access to our entire service and support know-how as well as to our services.

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

Product information, manuals, downloads, FAQs and application examples – all information is accessible with just a few mouse clicks at https://support.industry.siemens.com.

Technical Support

Siemens Industry's Technical Support offers quick and competent support regarding all technical queries with numerous tailor-made offers – from basic support to individual support contracts.

Please address your requests to the Technical Support via the web form: http://www.siemens.en/industry/supportrequest.

Service offer

Our service offer comprises, among other things, the following services:

- Product Training
- Plant Data Services
- Spare Parts Services
- Repair Services
- On Site and Maintenance Services
- Retrofit & Modernization Services
- Service Programs and Agreements

Detailed information on our service offer is available in the Service Catalog: https://support.industry.siemens.com/cs/sc

Industry Online Support app

Thanks to the "Siemens Industry Online Support" app, you will get optimum support even when you are on the move. The app is available for Apple iOS, Android and Windows Phone.
https://support.industry.siemens.com/cs/sc/2067

4.2 Links and Literature

Table 4-1

No.	Topic
\1\	This entry in the Siemens Industry Online Support https://support.industry.siemens.com/cs/ww/en/view/109737901
\2\	Download of the OPC UA .NET stacks incl. the Sample Applications of the OPC Foundation https://opcfoundation.org/developer-tools/developer-kits-unified-architecture/net-stack-and-sample-applications/
\3\	Download of the Sample Applications of the OPC Foundation https://opcfoundation.org/developer-tools/developer-kits-unified-architecture/sample-applications/
\4\	Function Manual: S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Communication https://support.industry.siemens.com/cs/ww/en/view/59192925
\5\	Homepage of the OPC Foundation https://opcfoundation.org/

4.3 Change documentation

Table 4-2

Version	Date	Modifications
V1.0	10/2016	First version