# Table of contents

1 Foreword ................................................................................................................................. 5  
  1.1 Notes on the documentation.............................................................................................. 5  
  1.2 Safety instructions ............................................................................................................. 6  

2 Overview .................................................................................................................................... 7  
  2.1 Scenarios............................................................................................................................ 7  
  2.2 Version overview ................................................................................................................ 10  
  2.3 Application examples.......................................................................................................... 13  
    2.3.1 Post-processing in the Cloud....................................................................................... 13  

3 Installation .................................................................................................................................. 20  
  3.1 System requirements.......................................................................................................... 20  
  3.2 Installation (TC3) .............................................................................................................. 22  
  3.3 Installation (TC2) .............................................................................................................. 25  
  3.4 Installation Windows CE (TC3) ......................................................................................... 28  
  3.5 Installation Windows CE (TC2) ......................................................................................... 30  
  3.6 Licensing (TC3) ................................................................................................................ 35  
  3.7 Licensing (TC2) ................................................................................................................ 37  

4 Technical introduction .............................................................................................................. 38  
  4.1 Server .............................................................................................................................. 38  
    4.1.1 Overview ..................................................................................................................... 38  
    4.1.2 Quick start................................................................................................................... 38  
    4.1.3 Configurator ................................................................................................................ 40  
    4.1.4 Data Access ................................................................................................................ 65  
    4.1.5 Historical Access ........................................................................................................ 90  
    4.1.6 Alarms and Conditions............................................................................................... 94  
    4.1.7 Method Call ................................................................................................................ 100  
    4.1.8 File transfer ................................................................................................................ 103  
    4.1.9 Global Discovery Server ............................................................................................ 105  
    4.1.10 Security ..................................................................................................................... 109  
    4.1.11 Miscellaneous .......................................................................................................... 112  
  4.2 Client I/O .......................................................................................................................... 116  
    4.2.1 Overview ..................................................................................................................... 116  
    4.2.2 Quick start................................................................................................................... 117  
    4.2.3 Supported data types.................................................................................................. 120  
    4.2.4 Adding nodes of a Server ......................................................................................... 121  
    4.2.5 Node attributes .......................................................................................................... 122  
    4.2.6 Method call ................................................................................................................ 123  
    4.2.7 StructuredTypes ......................................................................................................... 126  
    4.2.8 Data recording ............................................................................................................ 128  
    4.2.9 Writing variables........................................................................................................ 130  
    4.2.10 Security ..................................................................................................................... 131  
  4.3 Client PLCopen ..................................................................................................................... 134  
    4.3.1 Overview ..................................................................................................................... 134  
    4.3.2 Supported data types.................................................................................................. 134
1 Foreword

1.1 Notes on the documentation

This description is only intended for the use of trained specialists in control and automation engineering who are familiar with applicable national standards.

It is essential that the documentation and the following notes and explanations are followed when installing and commissioning the components.

It is the duty of the technical personnel to use the documentation published at the respective time of each installation and commissioning.

The responsible staff must ensure that the application or use of the products described satisfy all the requirements for safety, including all the relevant laws, regulations, guidelines and standards.

Disclaimer

The documentation has been prepared with care. The products described are, however, constantly under development.

We reserve the right to revise and change the documentation at any time and without prior announcement.

No claims for the modification of products that have already been supplied may be made on the basis of the data, diagrams and descriptions in this documentation.

Trademarks

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered trademarks of and licensed by Beckhoff Automation GmbH.

Other designations used in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owners.

Patent Pending

The EtherCAT Technology is covered, including but not limited to the following patent applications and patents:


with corresponding applications or registrations in various other countries.

EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.

Copyright

© Beckhoff Automation GmbH & Co. KG, Germany.

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization are prohibited.

Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.
1.2 Safety instructions

Safety regulations

Please note the following safety instructions and explanations!
Product-specific safety instructions can be found on following pages or in the areas mounting, wiring, commissioning etc.

Exclusion of liability

All the components are supplied in particular hardware and software configurations appropriate for the application. Modifications to hardware or software configurations other than those described in the documentation are not permitted, and nullify the liability of Beckhoff Automation GmbH & Co. KG.

Personnel qualification

This description is only intended for trained specialists in control, automation and drive engineering who are familiar with the applicable national standards.

Description of symbols

In this documentation the following symbols are used with an accompanying safety instruction or note. The safety instructions must be read carefully and followed without fail!

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠️ DANGER</td>
<td>Serious risk of injury! Failure to follow the safety instructions associated with this symbol directly endangers the life and health of persons.</td>
</tr>
<tr>
<td>⚠️ WARNING</td>
<td>Risk of injury! Failure to follow the safety instructions associated with this symbol endangers the life and health of persons.</td>
</tr>
<tr>
<td>⚠️ CAUTION</td>
<td>Personal injuries! Failure to follow the safety instructions associated with this symbol can lead to injuries to persons.</td>
</tr>
<tr>
<td>📝 NOTE</td>
<td>Damage to the environment or devices Failure to follow the instructions associated with this symbol can lead to damage to the environment or equipment.</td>
</tr>
</tbody>
</table>

Tip or pointer

This symbol indicates information that contributes to better understanding.
2 Overview

OPC Unified Architecture (OPC UA) is the next generation of the familiar OPC standard. This is a globally standardized communication protocol via which machine data can be exchanged irrespective of the manufacturer and platform. OPC UA already integrates common security standards directly in the protocol. Another major advantage of OPC UA over the conventional OPC standard is its independence from the COM/DCOM system.

Detailed information on OPC UA can be found on the webpages of the OPC Foundation.

Components

The following software components have been integrated for Win32/64 and Windows CE-based systems:

<table>
<thead>
<tr>
<th>Software component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPC UA Server [38]</td>
<td>Provides an OPC UA Server interface so that UA clients can access the TwinCAT runtime.</td>
</tr>
<tr>
<td>OPC UA Client [134]</td>
<td>Provides OPC UA Client functionality to enable communication with other OPC UA Servers based on PLCopen-standardized function blocks and an easy-to-configure I/O device.</td>
</tr>
</tbody>
</table>

The following software components have been integrated for Win32/64-based systems:

<table>
<thead>
<tr>
<th>Software component (Windows only)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPC UA Configurator</td>
<td>Graphical user interface for configuring the TwinCAT OPC UA Server</td>
</tr>
<tr>
<td>OPC UA Sample Client [165]</td>
<td>Graphical sample implementation of an OPC UA Client in order to carry out a first connection test with the TwinCAT OPC UA Server.</td>
</tr>
<tr>
<td>OPC UA Gateway [152]</td>
<td>Wrapper technology that provides both an OPC COM DA Server interface and OPC UA Server aggregation capabilities.</td>
</tr>
</tbody>
</table>

2.1 Scenarios

In the following, some scenarios will be illustrated in accordance with which the components can be implemented and used, depending on the application case and infrastructure:

- OPC UA Server: Integrated in Industrial PC or Embedded PC [8]
- OPC UA Server: Runs on a central computer with connection to remote TwinCAT runtime(s). [9]
Overview


**OPC UA Server: Integrated in Industrial PC or Embedded PC**

**Recommended scenario**

This scenario describes how the TwinCAT OPC UA Server should be used under normal circumstances.

One of the biggest advantages of the TwinCAT OPC UA Server is that it can be integrated into even the smallest embedded platform, e.g. the CX8000 series. Thanks to this integration, general handling is very simple and convenient. OPC UA Clients, e.g. HMI or MES/ERP systems, can connect to the OPC UA Server and read or write symbol information from the TwinCAT runtime.

The following software components and configurations run on the central server:

- Third party OPC UA Client, which may be an HMI, MES or ERP system, for example.

The following software components and configurations run on the Industrial PC or Embedded PC:

- The OPC UA Server automatically establishes a connection with the first local TwinCAT PLC runtime.
- TwinCAT runtime

This scenario has the following advantages:

- Network usage is optimized because it is based on OPC UA communication technologies, such as OPC UA registrations.
- Memory usage is decentralized. Each device is only responsible for its own memory requirements.
- OPC UA features security mechanisms that are directly integrated in the protocol. This is very useful if one of the Industrial PCs or Embedded PCs is connected via the internet, for example.
**OPC UA Server: Runs on a central computer with connection to remote TwinCAT runtime(s)**

This scenario describes the conventional implementation of OPC Servers. Servers using the old OPC A technology were often implemented on a central server instead of the Industrial PC on which TwinCAT runtime was executed, in order to avoid DCOM configurations. (Remember: in contrast to OPC UA, OPC DA is based on COM/DCOM technologies)

The following software components and configurations run on the central server:

- TwinCAT 3 ADS (or TwinCAT 2 CP) for the required ADS connectivity
- OPC UA Server with data access devices configured for remote TwinCAT runtimes
- ADS routes to remote TwinCAT runtimes
- Symbol files from any remote TwinCAT runtime
- OPC UA Client, which can be an HMI, MES or ERP system, for example.

The following software components and configurations run on the Industrial PC or Embedded PC:

- TwinCAT runtime
- ADS route to the central server

The more remote TwinCAT runtimes are connected to the central OPC UA Server, the higher the network usage will be.

The OPC UA Server uses advanced ADS recording techniques to query the symbol values of the TwinCAT runtime. The more symbols there are, the more cyclical queries are in progress. As a result, optimized OPC UA communication only takes place locally on the central server (between OPC UA Client and OPC UA Server).

This scenario has the following disadvantages compared to scenario 1:

- Network usage can be very high depending on the number of devices and symbols present.
- The memory requirement on the central server is very high because the OPC UA Server has to import symbol information from every TwinCAT runtime.
- No security between the central server and TwinCAT runtime based on data encryption - ADS was designed for high performance.
- The need to exchange symbol files between TwinCAT runtime and central server after each PLC program modification.

**OPC UA Server: Access to BC Controller**

Although small BC controllers are not able to run their own OPC UA Server, they may nevertheless have access to the PLC runtime executed on a remote BC Controller, such as a BC9191, and publish their symbol values via OPC UA. In this scenario the OPC UA Server must run together with a TwinCAT 3 ADS (or TwinCAT 2 CP) on another computer, and the scenario must be configured in the same way as scenario 2.
2.2 Version overview

The TwinCAT OPC UA supplement/function product is supplied in various setup versions, which reflect different development states. For new projects it is recommended to change to the latest setup version in order to be able to use all new product functions. Older setup versions are still available to download for existing projects.

Two versions are currently available:

- Setup Version 3.x.x: Long-standing existing version, which already offers a variety of functions. This version is still maintained with regard to optimizations.
- Setup Version 4.x.x: New version. Future developments and new product functionalities will only be implemented in this version.

The following table provides an overview of the different versions with regard to their product functionalities.
<table>
<thead>
<tr>
<th>Functionality</th>
<th>3.x.x</th>
<th>4.x.x</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server - Data Access (DA)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection of one / several PLC</td>
<td>yes</td>
<td>yes</td>
<td>Enables read/write access to the TwinCAT 2/3 PLC</td>
</tr>
<tr>
<td>Connection of a TcCOM module</td>
<td>yes</td>
<td>yes</td>
<td>Enables read/write access to TwinCAT 3 TcCOM modules</td>
</tr>
<tr>
<td>Connection of an I/O Task</td>
<td>yes</td>
<td>yes</td>
<td>Enables read/write access to the TwinCAT 2/3 I/O task</td>
</tr>
<tr>
<td>Connection of BC controllers</td>
<td>yes</td>
<td>yes</td>
<td>Enables read/write access to Beckhoff BC controllers</td>
</tr>
<tr>
<td>Connection of existing projects (&quot;brownfield&quot;)</td>
<td>yes</td>
<td>yes</td>
<td>Enables connection of existing controllers, e.g. via a gateway PC</td>
</tr>
<tr>
<td><strong>Server - Historical Access (HA)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using HA for PLC</td>
<td>yes</td>
<td>yes</td>
<td>Enables activation of variables from the TwinCAT 2/3 PLC for historical access</td>
</tr>
<tr>
<td>Using HA for TcCOM modules</td>
<td>yes (only TC3 C++)</td>
<td>yes</td>
<td>Enables activation of variables from a TwinCAT 3 TcCOM module for historical access</td>
</tr>
<tr>
<td>Using HA for I/O tasks</td>
<td>no</td>
<td>yes</td>
<td>Enables activation of variables from a TwinCAT 2/3 I/O task for historical access</td>
</tr>
<tr>
<td>Using HA for BC controllers</td>
<td>no</td>
<td>yes</td>
<td>Enables activation of variables from a Beckhoff BC controller for historical access</td>
</tr>
<tr>
<td>Using HA for existing projects (&quot;brownfield&quot;)</td>
<td>no</td>
<td>yes</td>
<td>Enables activation of variables for historical access without having to adapt the runtime project</td>
</tr>
<tr>
<td>Multiple instantiation of data memories</td>
<td>no</td>
<td>yes</td>
<td>Enables use of multiple instances per storage type.</td>
</tr>
<tr>
<td><strong>Server - Alarms &amp; Conditions (AC)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using AC for PLC</td>
<td>yes</td>
<td>yes</td>
<td>Enables activation of variables from the TwinCAT 2/3 PLC for alarms and conditions</td>
</tr>
<tr>
<td>Using AC for TcCOM modules</td>
<td>no</td>
<td>yes</td>
<td>Enables activation of variables from a TwinCAT 3 TcCOM module for alarms and conditions</td>
</tr>
<tr>
<td>Using AC for I/O tasks</td>
<td>no</td>
<td>yes</td>
<td>Enables activation of variables from a TwinCAT 2/3 I/O task for alarms and conditions</td>
</tr>
<tr>
<td>Using AC for BC controllers</td>
<td>no</td>
<td>yes</td>
<td>Enables activation of variables from a Beckhoff BC controller for alarms and conditions</td>
</tr>
<tr>
<td>Using AC for existing projects (&quot;brownfield&quot;)</td>
<td>no</td>
<td>yes</td>
<td>Enables activation of variables for alarms and conditions without having to adapt the runtime project</td>
</tr>
<tr>
<td><strong>Server - Method Calls</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Method calls for PLC</td>
<td>yes</td>
<td>yes</td>
<td>OPC UA Server enables TwinCAT 3 PLC methods to be activated and displayed as OPC UA methods</td>
</tr>
<tr>
<td>Method calls for TcCOM modules</td>
<td>yes (only TC3 C++)</td>
<td>yes</td>
<td>OPC UA Server enables TwinCAT 3 C++ methods to be activated and displayed as OPC UA methods</td>
</tr>
<tr>
<td><strong>Server - Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X509 certificates, self-signed</td>
<td>yes</td>
<td>yes</td>
<td>Generation of self-signed certificates</td>
</tr>
<tr>
<td>X509 certificates, custom</td>
<td>yes</td>
<td>yes</td>
<td>Enables the use of custom certificate authorizations</td>
</tr>
<tr>
<td>User authentication</td>
<td>yes</td>
<td>yes</td>
<td>OPC UA Server enables authentication of local or domain users</td>
</tr>
</tbody>
</table>
### Overview

#### Functionality

<table>
<thead>
<tr>
<th>Functionality</th>
<th>3.x.x</th>
<th>4.x.x</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access level at namespace level</td>
<td>no</td>
<td>yes</td>
<td>OPC UA Server allows definition of different access levels at namespace level</td>
</tr>
<tr>
<td>Access level at node level</td>
<td>no</td>
<td>yes</td>
<td>OPC UA Server allows definition of different access levels at node level</td>
</tr>
</tbody>
</table>

#### Server – Configuration

<table>
<thead>
<tr>
<th>Functionality</th>
<th>3.x.x</th>
<th>4.x.x</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual Studio</td>
<td>no</td>
<td>yes</td>
<td>Configurator integrated in Visual Studio (&quot;TwinCAT XAE&quot;) for parameterizing the individual functionalities.</td>
</tr>
<tr>
<td>Remote access</td>
<td>no</td>
<td>yes</td>
<td>Configurator allows remote configuration of TwinCAT OPC UA Servers independent of the operating system used on the target device.</td>
</tr>
<tr>
<td>Configuration namespace for connecting custom tools</td>
<td>no</td>
<td>yes</td>
<td>A dedicated namespace in the server enables connection of custom tools (based on OPC UA) for managing certificates or configuration files, or for restarting the server. Can be combined with security mechanisms, see above.</td>
</tr>
</tbody>
</table>

#### Client - PLC

<table>
<thead>
<tr>
<th>Functionality</th>
<th>3.x.x</th>
<th>4.x.x</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect/Read/Write/Disconnect</td>
<td>yes</td>
<td>yes</td>
<td>PLC function blocks based on PLCopen specification with Connect/Read/Write/Disconnect function.</td>
</tr>
<tr>
<td>Method calls with simple data types</td>
<td>yes</td>
<td>yes</td>
<td>PLC function blocks based on PLCopen specification with option to call OPC UA methods from a server, which use simple data types as input/output parameters.</td>
</tr>
<tr>
<td>Method calls with complex data types</td>
<td>no</td>
<td>no</td>
<td>PLC function blocks based on PLCopen specification with option to call OPC UA methods from a server, which use complex data types as input/output parameters.</td>
</tr>
<tr>
<td>Simple data types</td>
<td>yes</td>
<td>yes</td>
<td>Read/Write operations on simple data types, e.g. Int16, Int32, Float, Double, String, ...</td>
</tr>
<tr>
<td>Arrays with simple data types</td>
<td>yes</td>
<td>yes</td>
<td>Read/Write operations on arrays with simple data types, e.g. Int16, Int32, Float, Double, String, ...</td>
</tr>
<tr>
<td>Complex data types</td>
<td>no</td>
<td>no</td>
<td>Read/Write operations on complex data types, e.g. structures, ByteString, NodeId, LocalizedText, ...</td>
</tr>
<tr>
<td>Arrays with complex data types</td>
<td>no</td>
<td>no</td>
<td>Read/Write operations on arrays with complex data types, e.g. structures, ByteString, NodeId, LocalizedText, ...</td>
</tr>
<tr>
<td>X509 certificates, self-signed</td>
<td>yes</td>
<td>yes</td>
<td>Generation of self-signed certificates</td>
</tr>
<tr>
<td>X509 certificates, custom</td>
<td>yes</td>
<td>yes</td>
<td>Enables the use of custom certificate authorizations</td>
</tr>
<tr>
<td>User authentication</td>
<td>yes</td>
<td>yes</td>
<td>OPC UA Server enables authentication of local or domain users</td>
</tr>
</tbody>
</table>

#### Client - I/O

<table>
<thead>
<tr>
<th>Functionality</th>
<th>3.x.x</th>
<th>4.x.x</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect/Read/Write/Disconnect</td>
<td>no</td>
<td>yes</td>
<td>Easy to configure I/O device with Connect/Read/Write/Disconnect function.</td>
</tr>
<tr>
<td>Method calls with simple data types</td>
<td>no</td>
<td>yes</td>
<td>Easy to configure I/O device with option to call OPC UA methods from a server using simple data types as input/output parameters.</td>
</tr>
<tr>
<td>Method calls with complex data types</td>
<td>no</td>
<td>yes</td>
<td>Easy to configure I/O device with option to call OPC UA methods from a server using complex data types as input/output parameters.</td>
</tr>
<tr>
<td>Functionality</td>
<td>3.x.x</td>
<td>4.x.x</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------</td>
<td>-------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Simple data types</td>
<td>no</td>
<td>yes</td>
<td>Read/Write operations on simple data types, e.g. Int16, Int32, Float, Double, String, ...</td>
</tr>
<tr>
<td>Arrays with simple data types</td>
<td>no</td>
<td>yes</td>
<td>Read/Write operations on arrays with simple data types, e.g. Int16, Int32, Float, Double, String, ...</td>
</tr>
<tr>
<td>Complex data types</td>
<td>no</td>
<td>yes</td>
<td>Read/Write operations on complex data types, e.g. structures, ByteString, NodeId, LocalizedText, ...</td>
</tr>
<tr>
<td>Arrays with complex data types</td>
<td>no</td>
<td>yes</td>
<td>Read/Write operations on arrays with complex data types, e.g. structures, ByteString, NodeId, LocalizedText, ...</td>
</tr>
<tr>
<td>X509 certificates, self-signed</td>
<td>yes</td>
<td>yes</td>
<td>Generation of self-signed certificates</td>
</tr>
<tr>
<td>X509 certificates, custom</td>
<td>yes</td>
<td>yes</td>
<td>Enables the use of custom certificate authorizations</td>
</tr>
<tr>
<td>User authentication</td>
<td>yes</td>
<td>yes</td>
<td>OPC UA Server enables authentication of local or domain users</td>
</tr>
</tbody>
</table>

**Gateway**

<table>
<thead>
<tr>
<th>Functionality</th>
<th>3.x.x</th>
<th>4.x.x</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server aggregation</td>
<td>yes</td>
<td>yes</td>
<td>Aggregation of several TwinCAT OPC UA servers. Access to the aggregated servers is provided via an OPC UA server integrated in the gateway.</td>
</tr>
<tr>
<td>OPC COM DA server</td>
<td>yes</td>
<td>yes</td>
<td>Aggregation of several TwinCAT OPC UA servers. Access to the aggregated servers is provided via an OPC COM DA server integrated in the gateway.</td>
</tr>
<tr>
<td>X509 certificates, self-signed</td>
<td>yes</td>
<td>yes</td>
<td>Generation of self-signed certificates</td>
</tr>
<tr>
<td>X509 certificates, custom</td>
<td>yes</td>
<td>yes</td>
<td>Enables the use of custom certificate authorizations</td>
</tr>
<tr>
<td>User authentication</td>
<td>yes</td>
<td>yes</td>
<td>The OPC UA server integrated in the gateway enables authentication of local or domain users. Furthermore, user authentication can also be used when establishing a connection to the aggregated TwinCAT OPC UA servers.</td>
</tr>
</tbody>
</table>

### 2.3 Application examples

#### 2.3.1 Post-processing in the Cloud

The overall concept of providing a generic, standardized and callable interface in the cloud that accepts incoming data for further analysis is based on an endpoint in the cloud, either a Windows-based virtual machine or a real hardware running a Windows operating system, in addition to the decentralized clients that call this service. In this documentation, this device is generally referred to as OPC UA Server (in the cloud).
Data logger

The documentation shows how computing resources in the Cloud can be accessed and how local TwinCAT PLC devices can be connected in order to use these resources. As an initial example, this application case can be applied to a typical data storage scenario in which decentralized TwinCAT PLC devices send data to the cloud, in which the incoming data is stored in an SQL database via the TwinCAT Database Server. Although the general scenario also involves sending data back and forth (i.e. sending parameters to the cloud, performing calculations in the cloud, and then returning the computed results), this specific scenario does not require the return of results from the cloud.
System requirements: OPC UA Server (the cloud)

The cloud must be able to host one of the following operating system variants. Note that using virtualization technology requires a more costly solution for 64-bit operating systems.

Device is a virtual machine

- 32-bit Windows operating system
- 64-bit Windows operating system with CPU core isolation (two cores required as a minimum)

Device is a dedicated hardware

- 32-bit Windows operating system
- 64-bit Windows operating system

In addition, the following software components must be installed on the device:

- TwinCAT 3 XAR (Runtime only) or XAE (Runtime and Engineering)
- TwinCAT 3 Function TF6100 OPC UA

Note that when installing a complete TwinCAT 3 XAE, additional configuration settings such as handling licenses or the option of debugging the device directly in the cloud may be useful. The following software components must be installed to store data in a central database received from a client:

- TwinCAT 3 Function TF6420 Database

System requirements: Decentralized OPC UA Client

The decentralized OPC UA Client is based on a TwinCAT 3 PLC runtime and can therefore be hosted on any hardware configuration that supports the operation of a TwinCAT 3 PLC. In addition, TwinCAT 3 Function TF6100 OPC UA must be installed on the client device in order to be able to use the TwinCAT OPC UA Client to execute UA methods on the server in the cloud.

Technical description

The implementation of an OPC UA Server in the cloud is very application-specific. Beckhoff provides a general architecture description, which is independent of the individual application. As an application example, this article frequently refers a data aggregation scenario in which process data is transferred from decentralized clients via OPC UA to a central server, where the data is collected in a central database. The
advantage of OPC UA in this case is not only the standardized interface (and therefore to use this concept for any type of OPC UA Client), but also the ability to secure the communication channel by using the integrated security mechanism of OPC UA.

The TwinCAT OPC UA Server is used to disclose the methods defined in IEC61131-3 PLC to the OPC UA namespace. These methods can be called by any TwinCAT OPC UA Client (based on the PLCopen function blocks) or by third party OPC UA Clients.

**Decentralized OPC UA Client**

The main purpose of the OPC UA Client is to call methods on the remote server. The client is most probably a TwinCAT-3-embedded device that fulfils the decentralized part of the application. For the data aggregation example, this would mean querying process data and sending it to the server by calling a method.

**Interface description (to the cloud)**

As an interface to a centralized cloud system, there are only two methods provided by the server:

- int Send(data): This method forwards the data using an OPC UA method call and returns a JobID.
- int QueryState(jobID): Using the previously retrieved JobID, the client can cyclically query the current status of the job. This could be omitted if the server in the cloud can handle all situations, or if the client cannot help out in case of problems.

Communication between clients and the cloud can be secured by OPC UA's built-in security concepts, e.g. by using client and server certificates to encrypt data communication.

**The cloud**

The OPC UA Server in the cloud is based on TwinCAT 3 PLC methods that are disclosed to the OPC UA namespace. The PLC project contains the following three components:

- MethodCall provider: This component provides the above-mentioned send method, which collects data, creates a JobID and places the data in the queue as different jobs. There may also be a QueryState method to allow OPC UA Clients to query the current job status.
- Queue: The queue stores a list of jobs to be executed. Each job in the queue contains the following information: {ID, Status, Data}. New elements (jobs) are added by the MethodCall provider and can be deleted by it. The entire queue can be based on a hash table within the PLC program.
- Aggregator: The application that processes the jobs. It cyclically looks in the queue to see whether there are any jobs to be processed. If this is the case, it takes over the job (sets the status to "processed") and starts processing the job, e.g. connecting to a database via the function blocks of the TwinCAT Database Server. Note that there can be more than one aggregator to enable parallel processing of the queue.
Sample

The following sample illustrates the scenario by executing simple jobs: Jobs can be presented to the server by an OPC UA Client. In this sample, the job data consists of a definable time interval that is recorded by the aggregator to complete the job. The sample consists of the following PLC components on the OPC UA Server:

- **ST_JobEntry**: Represents a job in the queue. In terms of the data, the job only consists of a name and a duration. A duration defines the length of time a job takes.
- **E_JobState**: Represents the status of a job. The sample implementation defines the following values: QUEUED, PROCESSING, READY, FAILED and INVALID.
- **LongTerm**: Represents the MethodCall server (consisting of the methods Calc_Request and Calc_Response) and the aggregator that processes the job (which is implemented in the function block).
- **FB_SpecialHashTableCtrl**: Represents the queue in the form of a hash table, as reflected by PLC examples from the Beckhoff Information System. Here, different methods for handling the queue are provided (Add, Count, GetFirst, GetNext, Lookup, Remove, Reset).

Using the example

UA Expert could be used as a sample client to call the methods provided by the OPC UA Server in the cloud. By calling the Calc_Request method, the client receives a JobID (or 0 for displaying an error):
The client can query the JobState by calling the method Calc_Response with the JobID. In addition, the previously set duration and the job name are returned for subsequent reference.

Installation

The following chapter describes the installation and configuration of each software component required on the server in the cloud.

Runtime only

If the server does not host the engineering environment of TwinCAT 3, the TwinCAT 3 XAR installation must be used. Note that in this case the entire handling for proper function involves several steps, and future maintenance may be more difficult because the XAR installation lacks the programming and debugging environment. In this scenario, the user must ensure that maintenance of the ADS routes between the actual engineering computer (on which the PLC program for the server is developed) and the device that hosts the server in the cloud must allow not only downloading and debugging of the PLC program, but also activation of licenses for the TwinCAT 3 runtime. Note that you must open the firewall ports to enable ADS traffic. See
the ADS documentation for more information. The TC3 License Request Generator tool was developed for easier handling of TwinCAT 3 runtime licenses. It can be downloaded via the Beckhoff FTP server and enables the creation of License Request Files and the import of License Response Files:


Runtime and Engineering

This is the recommended setup scenario. The server in the cloud hosts a TwinCAT 3 runtime and the corresponding engineering components to enable debugging and easier handling of the runtime system. In this case it is necessary to install TwinCAT 3 XAE on the system.

Additional software

After successful installation of TwinCAT XAE or XAR, the following software components must be installed and configured on the device:

TF6100 OPC UA

The TF6100 function installs an OPC UA Server (and Client) on the device. The server is required to provide the OPC UA Clients with the PLC methods. When the PLC program is downloaded into the runtime, the OPC UA Server automatically imports the first PLC runtime into its namespace. All variables and methods of the PLC marked as available via OPC UA are imported into the OPC UA namespace and become available to clients. Refer to the TF6100 documentation for more information.

TF6420 Database

If the server is to store the data received from the clients in a database, the TF6420 function must be used. It provides generic function blocks for TwinCAT 3 PLCs for accessing the database, e.g. to insert values into a database table. Install the TF6420 setup and consult the TF6420 documentation for more information on using the corresponding function blocks.

Licensing

All TwinCAT 3 software products require a license to be available on the server. The license can be either a 7-day trial or an unlimited license. Licenses can be activated using the TwinCAT 3 XAE License Manager. If a TwinCAT 3 XAR installation is used on the server, use the TC3 License Generator.
## 3 Installation

### 3.1 System requirements

**OPC UA Server**

<table>
<thead>
<tr>
<th>Technical data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows 7, 10</td>
</tr>
<tr>
<td></td>
<td>Windows CE 6/7</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded Standard 2009</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded 7</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Target platforms</td>
<td>PC architecture (x86, x64, ARM)</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>4.5.2 (only required for configurator)</td>
</tr>
<tr>
<td>TwinCAT Version</td>
<td>TwinCAT 2, TwinCAT 3</td>
</tr>
<tr>
<td>TwinCAT installation level</td>
<td>TwinCAT 2 CP, PLC, NC-PTP</td>
</tr>
<tr>
<td></td>
<td>TwinCAT 3 XAE, XAR, ADS</td>
</tr>
<tr>
<td>Required TwinCAT license</td>
<td>TS6100 TwinCAT OPC UA (for TwinCAT 2)</td>
</tr>
<tr>
<td></td>
<td>TF6100 TC3 OPC UA (for TwinCAT 3)</td>
</tr>
</tbody>
</table>

**OPC UA Client**

<table>
<thead>
<tr>
<th>Technical data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows 7, 10</td>
</tr>
<tr>
<td></td>
<td>Windows CE 6/7</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded Standard 2009</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded 7</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Target platforms</td>
<td>PC architecture (x86, x64, ARM)</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>---</td>
</tr>
<tr>
<td>TwinCAT version</td>
<td>TwinCAT 2, TwinCAT 3</td>
</tr>
<tr>
<td>Minimum TwinCAT installation level</td>
<td>TwinCAT 2 PLC, NC-PTP</td>
</tr>
<tr>
<td></td>
<td>TwinCAT 3 XAE, XAR</td>
</tr>
<tr>
<td>Required TwinCAT license</td>
<td>TS6100 TwinCAT OPC UA (for TwinCAT 2)</td>
</tr>
<tr>
<td></td>
<td>TF6100 TC3 OPC UA (for TwinCAT 3)</td>
</tr>
</tbody>
</table>
### OPC UA I/O Client

<table>
<thead>
<tr>
<th>Technical data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows 7, 10</td>
</tr>
<tr>
<td></td>
<td>Windows CE 7</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded 7</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Target platforms</td>
<td>PC architecture (x86, x64, ARM)</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>---</td>
</tr>
<tr>
<td>TwinCAT version</td>
<td>TwinCAT 3.1 Build 4022.4</td>
</tr>
<tr>
<td>Minimum TwinCAT installation level</td>
<td>TwinCAT 3 XAE, XAR</td>
</tr>
<tr>
<td>Required TwinCAT license</td>
<td>TF6100 TC3 OPC UA</td>
</tr>
</tbody>
</table>

### OPC UA Gateway

<table>
<thead>
<tr>
<th>Technical data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows 7, 10</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded Standard 2009</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded 7</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Target platforms</td>
<td>PC architecture (x86, x64, ARM)</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>---</td>
</tr>
<tr>
<td>TwinCAT version</td>
<td>---</td>
</tr>
<tr>
<td>Minimum TwinCAT installation level</td>
<td>---</td>
</tr>
<tr>
<td>Required TwinCAT license</td>
<td>---</td>
</tr>
</tbody>
</table>

### OPC UA Configurator

<table>
<thead>
<tr>
<th>OPC UA Configurator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows 7, 10</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded Standard 2009</td>
</tr>
<tr>
<td></td>
<td>Windows Embedded 7</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Target platforms</td>
<td>PC architecture (x86, x64, ARM)</td>
</tr>
<tr>
<td>Visual Studio 2017 dependency</td>
<td>Installing .NET Targeting Package 4 using the Visual Studio Installer</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>4.5.2</td>
</tr>
<tr>
<td>TwinCAT version</td>
<td>TwinCAT 2 (standalone tool, up to setup version 3)</td>
</tr>
<tr>
<td></td>
<td>TwinCAT 3 (Visual Studio integrated, from setup version 4)</td>
</tr>
<tr>
<td>Minimum TwinCAT installation level</td>
<td>TwinCAT 2 CP, PLC, NC-PTP (standalone tool, up to setup version 3)</td>
</tr>
<tr>
<td></td>
<td>TwinCAT 3 XAE, XAR, ADS (standalone tool, up to setup version 3)</td>
</tr>
<tr>
<td></td>
<td>TwinCAT 3 XAE (Visual Studio integrated, from setup version 4)</td>
</tr>
<tr>
<td>Required TwinCAT license</td>
<td>---</td>
</tr>
</tbody>
</table>
3.2 Installation (TC3)

The following section describes how to install the TwinCAT 3 function TF6100 OPC UA for Windows-based operating systems.

- The TwinCAT 3 function setup file was downloaded from the Beckhoff website.

1. Run the setup file as administrator. To do this, select the command Run As Admin in the context menu of the file.
   - The installation dialog opens.
2. Accept the end user licensing agreement and click Next.

---

<table>
<thead>
<tr>
<th>OPC UA Sample Client</th>
<th>Description</th>
</tr>
</thead>
</table>
| Operating system     | Windows 7, 10  
                      | Windows Embedded 7   
                      | Windows Server 2008 R2  
                      | Windows Server 2012    
                      | Windows Server 2016    |
| Target platforms     | PC architecture (x86, x64, ARM) |
| .NET Framework       | 4.6 |
| TwinCAT version      | --- |
| Minimum TwinCAT installation level | --- |
| Required TwinCAT license | --- |
3. Enter your user data.

4. If you want to install the full version of the TwinCAT 3 function, select **Complete** as installation type. If you want to install the TwinCAT 3 function components separately, select **Custom**.
5. Select **Next**, then **Install** to start the installation.

![Installation dialog box](image)

→ A dialog box informs you that the TwinCAT system must be stopped to proceed with the installation.

6. Confirm the dialog with **Yes**.

![Confirmation dialog box](image)
7. Select Finish to exit the setup.

The TwinCAT 3 function has been successfully installed and can be licensed (see Licensing (TC3) [35]).

3.3 Installation (TC2)

The following section describes how to install the TwinCAT 2 Supplement TwinCAT OPC UA for Windows-based operating systems.

- Download and install the setup file [25]
- After the installation [28]

Download and install the setup file

Like many other TwinCAT add-on products, OPC UA is available as a 30-day demo version or full version for download from the Beckhoff website www.beckhoff.com.

- The setup file for the TwinCAT 2 Supplement has been downloaded from the Beckhoff homepage.

1. Run the downloaded setup file TcOpcUaSvr.exe as an administrator. To do this, select the command Run As Admin in the context menu of the file.
   - The installation dialog opens.

2. Select an installation language.
3. Click **Next** and accept the license agreement.
4. Enter your information. All fields are mandatory. If you want to install a 30-day demo, please enter "DEMO" as license key.
5. Click Install to start the installation.

6. Restart the computer to complete the installation.

After the installation

The TwinCAT add-on OPC UA is automatically configured during installation, and no further settings are required for using this product. Further steps may include:

• Establish an initial connection to the installed UA server and test its configuration with the OPC UA Sample Client. (See Sample Client [165])
• Personalize the UA server setup using the OPC UA Configurator. (See Configurator [40])
• Also, make sure your firewall opens TCP port 4840 because the OPC UC Server requires this port.

3.4 Installation Windows CE (TC3)

The following section describes how to install the TwinCAT 3 function TF6100 OPC UA on a Beckhoff Embedded PC with Windows CE.

• Download and install the setup file [29]
• Transfer the CAB file to the Windows CE device [29]
• Run the CAB file on the Windows CE device [29]

If an older version of TF6100 is already installed on the Windows CE device, it can be updated:

• Software upgrade [30]
Download and install the setup file

The executable file for Windows CE is part of the TF6100 OPC UA setup. This is made available on the Beckhoff website www.beckhoff.com and automatically contains all versions for Windows XP, Windows 7 and Windows CE (x86 and ARM).

Download the setup and install the function as described in the section Installation.

After the installation, the installation folder contains three directories (one directory per hardware platform)

- **CE-ARM**: ARM-based Embedded PCs running Windows CE, e.g. CX8090, CX9020
- **CE-X86**: X86-based Embedded PCs running Windows CE, e.g. CX50xx, CX20x0
- **Win32**: Embedded PCs running Windows XP, Windows 7 or Windows Embedded Standard

The CE-ARM and CE-X86 directories contain the CAB files of the TwinCAT 3 function for Windows CE in relation to the respective hardware platform of the Windows CE device.

Sample: "TF6310" installation folder

Transferring the CAB file to the Windows CE device

Transfer the corresponding executable file to the Windows CE device.

There are various options for transferring the executable file:

- via network shares
- via the integrated FTP server
- via ActiveSync
- via CF/SD cards

Further information can be found in the Beckhoff Information System in the "Operating Systems" documentation (Embedded PC > Operating Systems > CE).

Run the CAB file on the Windows CE device

After transferring the CAB file to the Windows CE device, double-click the file there. Confirm the installation dialog with OK. Then restart the Windows CE device.

After restarting the device, the files (Client and Server) are automatically loaded in the background and are available.

The software is installed in the following directory on the Windows CE device:

\Hard Disk\TwinCAT\Functions\TF6310-TCP-IP
Software upgrade

If an older TF6100 version is already installed on the Windows CE device, carry out the following steps on the Windows CE device to upgrade to a new version:

1. Open the CE Explorer by clicking **Start > Run** and entering "Explorer".
2. Navigate to `\Hard Disk\TwinCAT\Functions\TF6100-OPC-UA\Server` or (in a second step) `\Hard Disk\TwinCAT\Functions\TF6100-OPC-UA\Client`.
3. Rename the file `TcOpcUaServer.exe` or `TcOpcUaClient.exe`.
4. Restart the Windows CE device.
5. Transfer the new CAB file to the Windows CE device.
6. Run the CAB file on the Windows CE device and install the new version.
7. Delete the old (re-named) files.
8. Restart the Windows CE device.

⇒ The new version is active after the restart.

3.5 Installation Windows CE (TC2)

The following section describes how to install the TwinCAT 2 Supplement on a Beckhoff Embedded PC with Windows CE, e.g. CX1000, CX1020, CX9000, CX9001, CX9010, CX8090, CP62xx or CP69xx.

- Download and install the setup file [30]
- Transfer the setup file to a Windows CE device [33]
- Run the setup file on the Windows CE device [34]

**Installation on small embedded platforms (CX9001, CX9010)**

Very small embedded devices may require some additional manual steps to install the CAB file. These steps may include, for example, the deleting of unnecessary files from the memories of the devices so that there is sufficient space to install all the files of the application.

Download and install the setup file

Just like many other TwinCAT supplementary products, OPC UA for CE is available as a download on the Beckhoff homepage. To obtain the installation files for Windows CE, you must first install the downloaded setup file on a host computer. This can be any Windows CE-based system.

1. Double-click the downloaded file `TcOpcUaSvrCE.exe`.
2. Select an installation language.
3. Click **Next** and accept the license agreement.
4. Enter your information. All fields are mandatory. Note that OPC UA for CE is not currently available as a demo version. Therefore, you will need a valid license key to continue with the installation.

![Customer Information](image)
5. Select **Full** as the installation type and click on **Continue**

6. Click **Install** to start the installation.

   ⇒ After installation you will find the setup files for Windows CE in the directory `\TwinCAT\CE`. This directory contains setup files for the following CE platforms:
   - TwinCAT OPC UA Client CE\I586: OPC UA Client (PLC library) for x86-based CPUs (such as CX10xx, CP62xx, C69xx, ...)
   - TwinCAT OPC UA Client CE\ARMV4I: OPC UA Client (PLC library) for ARM-based CPUs (such as CX9001, CX9010, CP6608, ...)
   - TwinCAT OPC UA Server CE\I586: OPC UA Server for x86-based CPUs (such as CX10xx, CP62xx, C69xx, ...)
   - TwinCAT OPC UA Server CE\ARMV4I: OPC UA Server for ARM-based CPUs (such as CX9001, CX9010, CP6608, ...)

**Transfer the setup file to the Windows CE device**

Transfer the corresponding executable file to the Windows CE device. There are various options for transferring the setup file:

- from a shared folder
- via the integrated FTP server
- via ActiveSync
- via a CF card

Further information can be found in the Beckhoff Information System in the "Operating systems" documentation (Embedded PC > Operating systems > **CE**)
Run the setup file on the Windows CE device

Execute the transferred setup file TcOpcUsrCe.xxxx.CAB on the CE device:

1. Navigate to the directory to which you have transferred the setup file.

2. Double-click the CAB file. If a message dialog box appears that says this program is not compatible with the current operating system, make sure you are using the correct CAB file (ARM, I586) for your IPC/Embedded PC.

3. If you are sure that the CAB file matches the Embedded PC/IPC, confirm this message dialog with Yes.

4. Select \Hard Disk\System\ as destination directory

5. Click OK to start the installation.
After installation, the setup file is automatically deleted.

Once you have installed the OPC UA Server, this component will be available after restarting your Windows CE device.

3.6 Licensing (TC3)

The TwinCAT 3 Function can be activated as a full version or as a 7-day test version. Both license types can be activated via the TwinCAT 3 development environment (XAE).

The licensing of a TwinCAT 3 Function is described below. The description is divided into the following sections:

- Licensing a 7-day test version
- Licensing a full version

Further information on TwinCAT 3 licensing can be found in the “Licensing” documentation in the Beckhoff Information System (TwinCAT 3 > Licensing).

Licensing the 7-day test version of a TwinCAT 3 Function

Note: A 7-day test version cannot be enabled for a TwinCAT 3 license dongle.

1. Start the TwinCAT 3 development environment (XAE).
2. Open an existing TwinCAT 3 project or create a new project.
3. If you want to activate the license for a remote device, set the desired target system. To do this, select the target system from the Choose Target System drop-down list in the toolbar.
   - The licensing settings always refer to the selected target system. When the project is activated on the target system, the corresponding TwinCAT 3 licenses are automatically copied to this system.
4. In the Solution Explorer, double-click License in the SYSTEM subtree.

   The TwinCAT 3 license manager opens.
5. Open the **Manage Licenses** tab. In the **Add License** column, check the check box for the license you want to add to your project (e.g. "TF6420: TC3 Database Server").

6. Open the **Order Information (Runtime)** tab.
   - In the tabular overview of licenses, the previously selected license is displayed with the status “missing”.

7. Click **7-Day Trial License...** to activate the 7-day trial license.
   - A dialog box opens, prompting you to enter the security code displayed in the dialog.

8. Enter the code exactly as it appears, confirm it and acknowledge the subsequent dialog indicating successful activation.
   - In the tabular overview of licenses, the license status now indicates the expiry date of the license.

9. Restart the TwinCAT system.
The 7-day trial version is enabled.

**Licensing the full version of a TwinCAT 3 Function**

A description of the procedure to license a full version can be found in the Beckhoff Information System in the documentation "TwinCAT 3 Licensing".

### 3.7 Licensing (TC2)

The licensing of the TwinCAT OPC UA for TwinCAT 2 takes place during the installation [25] by entering a license key.
4 Technical introduction

4.1 Server

4.1.1 Overview

The TwinCAT OPC UA Server provides a standardized communication interface for accessing symbol values from the TwinCAT runtime. This facilitates integration of third-party software for reading or writing variable values.

This part of the documentation describes the various configuration options available for the TwinCAT OPC UA Server.

We recommend following our QuickStart guide.

4.1.2 Quick start

After successful installation and licensing, execute the following steps to make PLC variables available via the TwinCAT OPC UA Server.

- Step 1: Configure PLC variables for the OPC UA access
- Step 2: Configure the download of the symbol file
- Step 3: Activate the license for the server
- Step 4: Activate the project
- Step 5: Establish a connection to the OPC UA Server

Requirements

This quick-start procedure assumes that the TwinCAT OPC UA Server is in the delivery state. The server is automatically configured to access the first (local) PLC runtime.

Step 1: Configure PLC variables for the OPC UA access

Open an existing PLC project and insert the following comment before the selected variables. Alternatively you can create a new PLC project.

TwinCAT 3 (TMC import):

```plaintext
{attribute 'OPC.UA.DA' := '1'}
```

bVariable : BOOL;

TwinCAT 2 (TPY import):

```plaintext
bVariable : BOOL; (* OPC:1:some description *)
```

Step 2: Configure the download of the symbol file

By default, the TwinCAT OPC UA Server establishes a connection with the first PLC runtime on the local system and uses the corresponding symbol file to build the namespace.

To make the symbol file available, activate the download of the symbol file in the settings of the PLC project.
Step 3: Activate the license for the server

Check whether a license exists. In TwinCAT 3 you can enter a TF6100 license in the TwinCAT license management (see Licensing (TC3) [35]). A 7-day trial license is sufficient for a basic introduction.

Step 4: Activate the project

Activate the TwinCAT project and restart TwinCAT. Then log into the PLC runtime and start the PLC program.

**NOTE**

Note for the CE platform

Please note that the TwinCAT OPC UA Server under Windows CE is not restarted with a TwinCAT restart as well. Here you have to either restart the CE device or call the Restart() method from the configuration namespace [112] to restart the server so that it reads the TMC file and provides the PLC variables.

Step 5: Establish a connection to the OPC UA Server

To establish a connection from an OPC UA Client, the client must establish a connection with the URL of the OPC UA Server, e.g. opc.tcp://CX-12345:4840 or opc.tcp://192.168.1.1:4840.

**Default port and end points**

Please also note our information on the Default port and end points [114] used by the server.

To connect to the TwinCAT OPC UA Server you can use the OPC UA Sample Client provided, which can be called up via the Windows start menu.

For more advanced testing we recommend using the free UA Expert software from Unified Automation.

After successful connection to the server you will find the released PLC variables under the object PLC1.
4.1.3 Configurator

The TF6100 setup (version 4.x.x and higher) contains the latest version of the OPC UA Server Configurator. This was integrated in Microsoft Visual Studio as a separate project type to provide an integrated and consistent engineering concept. You can configure all the different facets of the OPC UA Server and in doing so also use source control mechanisms such as Team Foundation Server or Subversion Integrations.

Toolbar

The toolbar of the OPC UA Configurator can be used to establish a connection with a local or remote TwinCAT OPC UA Server. All configuration settings can then be implemented for the selected server.

If the toolbar is not displayed, you can add it to the user interface via the menu View > Toolbars.
Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

4.1.3.1 Creating a new project

The project package of the OPC UA Configurator integrates itself in the so-called connectivity package. You can select this when creating a new Visual Studio project.

Project template "TwinCAT Connectivity Project":

![TwinCAT Connectivity Project](image1)

Project template "TwinCAT OPC-UA Server Project":

![TwinCAT OPC-UA Server Project](image2)

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>
4.1.3.2 Select target device

The OPC UA Configurator enables the complete parameterization of the Server via OPC UA. In much the same way as in the TwinCAT XAE system, you can select a target OPC UA Server via the toolbar.

All settings in the configuration are then implemented for this OPC UA Server. The basis for this is the so-called configuration namespace of the server (see Namespace for configuration of the server).

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

4.1.3.3 Adding ADS devices

The OPC UA Server can "talk" to one or more ADS devices. To establish a connection, a route to the respective ADS device is required. In the OPC UA Configurator, ADS devices are created, configured and thus announced to the OPC UA Server in the Data Access facet.

New ADS devices are added to the configuration via the context menu command Add new Device Type.
When the command is executed, a dialog box opens in which connection parameters can be configured for this device, e.g. AMS Net ID, ADS port or the symbol file.

You can subsequently modify the connection parameters if necessary via the Properties window in Visual Studio.
Selecting the symbol file

Symbol files that are present on the selected target device can be imported directly. These symbol files can be stored either in the TwinCAT boot directory or in the symbol directory of the OPC UA Server. You can select the files via the corresponding dialog during the symbol file configuration.

The TwinCAT OPC UA File Explorer can be connected to either the local TwinCAT directory or the remote boot directory. The latter is read in via the server's configuration namespace (see Namespace for configuration of the server [112]).
4.1.3.4 Downloading and uploading configurations

Via the configurator you can initiate the download/upload of complete server configurations as well as loading every single facet (data access, historical access, etc.) individually to the target device and opening it there. The functions necessary for this are integrated both in the toolbar and in the context menu of the respective facet.

Opening a configuration from the target device

You can open the configuration of the selected target device via the corresponding button in the toolbar.

See also: Select target device [42]

Activating the configuration on a target device

You can download the currently opened configuration to the selected target device using the corresponding button in the toolbar.

See also: Select target device [42]
Opening a partial configuration

You can open the partial configuration of the selected target device using the command **Read Configuration from Target** in the context menu of a certain facet of the configuration.

---

See also: Select target device [42]

---

Downloading a partial configuration

You can download the partial configuration to the selected target device using the command **Write Configuration to Target** in the context menu of a certain facet of the configuration.
4.1.3.5 Importing and exporting configuration files

The context menu commands enable the import/export of configuration files of the OPC UA Server.

Importing a partial configuration

You can import the partial configuration (e.g. historical access) from an XML configuration file using the command **Import UA Configuration** in the context menu of a certain facet of the configuration.

Exporting a partial configuration

You can export the partial configuration (e.g. historical access) to an XML configuration file using the command **Export UA Configuration** in the context menu of a certain facet of the configuration.
4.1.3.6 Configuring historical access

To configure Historical Access, you must first set up the History Adapters. These are the different locations for storing historical data, such as RAM, file, SQL Server.

History adapters are added to the configuration using the context menu command **Add new History Adapter**.

Depending on the adapter type you have to specify further parameters, e.g. the desired file storage path or the access data for the SQL Server.
After you have created a history adapter you can add the desired variables to the adapter. These variables must already exist on the selected OPC UA Server when the engineering is implemented. You can use the integrated OPC UA Target Browser to select the variables and then add the variables from the target browser to the history adapter by drag & drop.

Additional parameters can be specified in the properties window of the newly added variable, e.g. the desired SamplingRate or the size of the ring buffer to be used in the History Adapter.

See also: Select target device [42]

4.1.3.7 Configuring Alarms and Conditions

In order to configure Alarms and Conditions (A&C) you must first set up the Condition Controllers. These are container units that group together alarms.
Condition Controllers are added to the configuration using the context menu command **Add New Condition Controller**.

After you have created a Condition Controller, you can add the desired variables to the controller and monitor them in the sense of alarms and conditions. A condition is created for each variable, which specifies the parameters for monitoring. These variables must already exist on the selected OPC UA Server when the engineering is implemented. You can use the integrated **OPC UA Target Browser** to select the variables and then add the variables from the target browser to the Condition Controller by drag & drop.

In the dialog window which then opens you can define the condition type and further parameters for the monitoring, e.g. SamplingRate and Severity.
Depending on the selected condition type you can specify additional parameters in the properties window of the condition. The threshold values for the respective condition type are displayed as individual entries in the tree view of the configuration. Here too, you can configure the corresponding parameters in the properties window.

Subsequently you have to define the alarm texts that are to be sent to the OPC UA Client when a condition is triggered. The section Configuring alarm texts (p. 53) describes how alarm texts are created. You can drag and drop the alarm texts onto the respective threshold value of a condition.
**Alarm type OffNormal**

An OffNormal alarm type is used to define which state of a Boolean variable is evaluated as normal. An alarm is triggered if the variable value deviates from this. The PLC must be used for working with value ranges (e.g., integer or double variables). Depending on the value, a corresponding TRUE or FALSE state is then passed to the OPC UA server.

<table>
<thead>
<tr>
<th>State</th>
<th>Value range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>TRUE or FALSE, depending on the user's decision.</td>
</tr>
<tr>
<td>OffNormal</td>
<td>TRUE or FALSE, depending on the configuration of the normal state. Cannot be configured by the user.</td>
</tr>
</tbody>
</table>

The first step is to configure the normal state as described above. The user then defines an alarm text for the respective state (OffNormal and Normal) via Resources. This can be done either by drag & drop or by selecting from the **Resource ID** dropdown list.

**Alarm type Limit**

With an alarm type Limit you define different threshold values upon whose reaching an alarm is to be sent. The following table describes the different threshold values using an example configuration.

<table>
<thead>
<tr>
<th>State</th>
<th>Example threshold values</th>
<th>Associated value range (INT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HighHigh</td>
<td>5000</td>
<td>5000-32767</td>
</tr>
<tr>
<td>High</td>
<td>2000</td>
<td>2000-4999</td>
</tr>
<tr>
<td>Normal</td>
<td>-</td>
<td>1000-1999</td>
</tr>
<tr>
<td>Low</td>
<td>1000</td>
<td>500-999</td>
</tr>
<tr>
<td>LowLow</td>
<td>500</td>
<td>-32768-499</td>
</tr>
</tbody>
</table>

In the first step, the various threshold values are configured as described above. The user then defines an alarm text for the respective state (HighHigh, High, Normal, Low, LowLow) via Resources. This can be done either by drag & drop or by selecting from the **Resource ID** dropdown list.

**Requirements**

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

See also: Select target device [42]
4.1.3.8 Configuring alarm texts

The OPC UA Configurator enables the (multilingual) management of alarm texts that are used, for example, with Alarms and Conditions [49]. The configuration of the alarm texts takes place in the Resources facet. Each alarm text is identified by a unique ID. Multiple language texts can then be assigned to this ID.

You can create so-called “resource items” using the context menu command **Add new Resource Item**.

![Solution Explorer](image)

You add new language items to a resource item using the command **Add new Language Item** in the resource item’s context menu.
You can further parameterize a language item, e.g. the language text and the assigned language, in the properties window. When you define the language the associated LocaleID is automatically set. The LocaleID is requested by the OPC UA Client to indicate in which language it expects alarm texts.

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

4.1.3.9 Configuring endpoints

The endpoints of the OPC UA Server indicate which security mechanisms are to be used during the connection establishment of a client. These range from "unencrypted" to "encrypted and signed", based on different key strengths.
The endpoints can be activated and deactivated using the configurator. It may be useful to deactivate the unencrypted endpoint so that all clients can only connect themselves with valid certificates that are classified as trustworthy.

The endpoints are configured directly at the level of the OPC UA Server project. By double-clicking on the project you can make the corresponding settings on the UA Endpoints tab. The settings become effective after an activation of the configuration and a subsequent restart of the server (see Downloading and uploading configurations [45] and Restarting the server [64]).

![UA Endpoints tab](image)

**Requirements**

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

### 4.1.3.10 Configuring certificate trust settings

The Configurator facilitates management of the client certificates on the server. In the project settings you can classify the certificates as trustworthy or refuse them on the UA Endpoints tab in the Client certificates area.

After an OPC UA Client has attempted to connect to a secure server endpoint for the first time, the client certificate is deposited on the server and declared "rejected". The server administrator can subsequently enable the certificate. A subsequent connection attempt of the client with a secured endpoint will then be successful.
### 4.1.3.11 Configuring security settings

The OPC UA Server enables the configuration of permissions at namespace and node level. This allows you to fine-granulate the access to ADS devices (for example, to different PLC runtimes) as well as variables. These security settings are available for all ADS devices that can be displayed in the server namespace.

**Configuration**

The permissions are configured on the basis of an XML-based configuration file (*TcUaSecurityConfig.xml*), which is located in the same directory as the server. The configuration file consists of the three areas "Users", "Groups" and "AccessInfos".

- **Administrator**
  - Access Rights
    - PLC1 – Full access
    - PLC2 – Full access
    - PLC3 – Full access

- **HMI_User**
  - Access Rights
    - PLC1 – No access
    - PLC2 – No access
    - PLC3 – rw Access to MAIN
**Users**

In the "Users" area you can configure user accounts that are to be accepted by the OPC UA Server as logins. There are three different authentication methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS (recommended authentication method)</td>
<td>The mechanisms of the operating system are used to validate user name and</td>
</tr>
<tr>
<td></td>
<td>password. The user account is subject completely to the control of the</td>
</tr>
<tr>
<td></td>
<td>operating system and/or domain.</td>
</tr>
<tr>
<td>Server (not recommended)</td>
<td>User name and password are known only to the OPC UA Server. Both pieces</td>
</tr>
<tr>
<td></td>
<td>of information are stored in plain text in the XML file.</td>
</tr>
<tr>
<td>None</td>
<td>Only the user name of the server is evaluated, the password is ignored.</td>
</tr>
</tbody>
</table>

Users can be configured with a tag `<DefaultAccess>` that specifies the standard access of the user to a certain namespace.

Users can be members of one or more groups. You can specify this using the `MemberOf` attribute. In case of memberships of several groups, separate the groups by a semicolon.

**Groups**

In order to enable a simpler configuration with several user accounts, you can combine the users into groups.

Groups can also be configured with a tag `<DefaultAccess>`.

You can nest groups using the `MemberOf` attribute. In case of memberships of several groups, separate the groups by a semicolon.
AccessInfos

If a fine-granular setting of permissions at the node level is to be implemented, then <AccessInfos> can be configured additionally, which specify the access permissions on nodes. Access rights can be passed on to subelements. Although AccessInfos allow the most fine-grained configuration of permissions, such a configuration can quickly become confusing. Therefore, check whether configuring access rights at the namespace level (see above) is not sufficient.

The AccessInfo for a node contains the following settings:

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS</td>
<td>configures the NamespaceName in which the node is localized</td>
</tr>
<tr>
<td>Id</td>
<td>configures the identifier of the node, including the IdentifierType (e.g. s = String)</td>
</tr>
<tr>
<td>Depth</td>
<td>inheritance level of permissions (-1 for infinite)</td>
</tr>
<tr>
<td>User/Group</td>
<td>user or group that is to be given access to this node, including the AccessLevels</td>
</tr>
</tbody>
</table>

AccessInfos can be configured by dragging & dropping variables from the Target Browser. The configurable permissions are cumulative.

Example configuration

Let’s take the following simple control program. The variables are already published in the OPC UA namespace of the server. The OPC UA Server is initially in the delivery state.
Access restrictions

Access to the server is to be restricted for clients as follows:

- Anonymous access is to be deactivated.
- There is to be a user - "Administrator" - who has full access to the complete server.
- There is to be a user - "User1" - who only has read access to MAIN.Instance1. The user should not come from the operating system here, but should only be used internally in the server.
- There is to be a user - "User2" - who only has read access to MAIN.Instance2. The user should not come from the operating system here, but should only be used internally in the server.
- General access permissions are to be configured for all users via a group called "Users".

Settings

The configuration of the OPC UA Server is set as follows:
Settings for the user "Administrator":

```
<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Server</td>
</tr>
<tr>
<td>IsRoot</td>
<td>True</td>
</tr>
<tr>
<td>MemberOf</td>
<td>Users</td>
</tr>
<tr>
<td>Password</td>
<td>●</td>
</tr>
<tr>
<td>User</td>
<td>Administrator</td>
</tr>
</tbody>
</table>
```

Settings for the user "User1":

```
<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Server</td>
</tr>
<tr>
<td>IsRoot</td>
<td>False</td>
</tr>
<tr>
<td>MemberOf</td>
<td>Users</td>
</tr>
<tr>
<td>Password</td>
<td>●</td>
</tr>
<tr>
<td>User</td>
<td>User1</td>
</tr>
</tbody>
</table>
```

Settings for the user "User2":

```
<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>IsRoot</td>
<td></td>
</tr>
<tr>
<td>MemberOf</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>●</td>
</tr>
<tr>
<td>User</td>
<td></td>
</tr>
</tbody>
</table>
```
Settings for AccessInfos "MAIN.Instance1":

Settings for AccessInfos "MAIN.Instance2":
Settings for the group "Users":

The user group is equipped both with basic access to required server and type system namespaces and with read and browse permissions to the PLC1 namespace.

Result

Following activation of the configuration, the namespace of the server for "User1" looks like the following after establishment of a connection:
The user has only read rights to the node "Instance1", which is clear from the attribute UserAccessLevel:

<table>
<thead>
<tr>
<th>DataType</th>
<th>ST_Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>NamespaceIndex</td>
<td>4</td>
</tr>
<tr>
<td>IdentifierType</td>
<td>String</td>
</tr>
<tr>
<td>Identifier</td>
<td>&lt;StructuredDataType&gt;:ST_Test</td>
</tr>
<tr>
<td>ValueRank</td>
<td>-1</td>
</tr>
<tr>
<td>ArrayDimensions</td>
<td>BadAttributeIdInvalid (0x80350000)</td>
</tr>
<tr>
<td>AccessLevel</td>
<td>CurrentRead, CurrentWrite</td>
</tr>
<tr>
<td>UserAccessLevel</td>
<td>CurrentRead</td>
</tr>
</tbody>
</table>

The user "Administrator", conversely, has full access rights to all elements of the namespace:
4.1.3.12 Restarting the server

The OPC UA Configurator enables the triggering of a restart of the OPC UA Server. This can be done locally or remotely and refers to the selected target device.

Loss of connection

A restart of the OPC UA Server always leads to a loss of the connection of all connected clients.

The restart is triggered via the toolbar.

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

See also: Select target device [42]

4.1.3.13 Troubleshooting and logging

For an advanced diagnosis you can activate the logging function of the OPC UA Server.

Writing the log file

Activating the logging function on the server causes a log file to be written on the file system. Make sure that there is sufficient memory space available and set the logging parameters accordingly (number of log files, size per log file).
Performance and timing behavior

Activation of the logging function will change the timing behavior of the OPC UA Server. As a result there may be losses of speed, depending on the platform and project.

The logging function is activated using the **Activate** button on the **Online Panel** tab in the project configurator. You can activate the function locally or remotely depending on the selected target device. The logging function remains active until it is deactivated again via the configurator or until the OPC UA Server is restarted.

Activate App Trace

In most cases it is sufficient to create a so-called "AppTrace". The following applies: The higher the "trace level", the more detailed (and more) data is written.

Activate Stack Trace

In a few cases it is also necessary to create a so-called "StackTrace". The same applies here: The higher the "trace level", the more detailed (and more) data is written.

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

See also: [Selecting a target device](#)

4.1.4 Data Access

4.1.4.1 PLC

This section describes how to configure the namespace of the OPC UA Server such that it contains variables from a TwinCAT PLC runtime. The TwinCAT OPC UA Server can represent several namespaces, i.e., several PLC runtimes. In order for a PLC variable to be accessible via the respective namespace, it must be explicitly enabled for this purpose in the PLC program.

Quick start

Note that the OPC UA Server always connects by default to the first local PLC runtime system, therefore a configuration is not necessary in most cases (see also Quick start). A separate configuration is only necessary in a few cases, e.g., if additional runtimes are to be displayed in the server.
This documentation article contains the following topics:

- **General Information [¶.66]**
- Step 1: **Selecting PLC variables to be publicly accessible via OPC UA [¶.67]**
- Step 2: **Downloading the symbol description and activating it in the PLC project [¶.69]**
- [Optional] Step 3: **Configuring the data access device in the OPC UA Server [¶.70]**
- [Optional] Step 4: **Explicit hiding of variables [¶.70]**

**General Information**

Several parameters are available for configuring the server and accessing PLC variables, which can be set via the TwinCAT OPC UA Configurator.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS Port</td>
<td>Defines the ADS port under which the PLC runtime can be reached. The ADS port can be read in the properties of the PLC project.</td>
<td>800 (BC Controller) 801 (TwinCAT 2) 811 (TwinCAT 2) … 851 (TwinCAT 3 - standard) 852 (TwinCAT 3) …</td>
</tr>
<tr>
<td>AutoCfg</td>
<td>Defines the runtime type, e.g., PLC, C++, I/O. Some AutoCfg options are available as filtered or unfiltered variants. Filtered means the user can determine which symbols are to be published via OPC UA (see below). When using an unfiltered option, each symbol is made available via OPC UA.</td>
<td>7 TwinCAT 2 (TPY) 8 TwinCAT 2 (TPY) filtered 4040 TwinCAT 3 (TMC) 4041 TwinCAT 3 (TMC) filtered</td>
</tr>
<tr>
<td>AutoCfgSymFile</td>
<td>Symbol file of the respective PLC runtime. By default, the automatically generated symbol file of the first PLC runtime of the local system is imported.</td>
<td>Path to the symbol file. Points by default to the symbol file (TMC) of the first local PLC runtime.</td>
</tr>
<tr>
<td>IoMode</td>
<td>Defines the method for accessing symbols. This is particularly important for accessing BC devices.</td>
<td>1 (access via handle - default) 3 (Access to BC Controller)</td>
</tr>
<tr>
<td>Array expansion</td>
<td>By default, subelements of an array are not mapped as separate nodes in the UA namespace. Instead, only the array is mapped as a single element. UA Clients can nevertheless access subelements via their IndexRange. (Some older OPC UA Clients do not yet support this option). The flag was introduced so that access is nevertheless possible for these clients. It ensures that every array position is displayed as a separate node in the UA namespace. This leads to higher memory requirement of the OPC UA Server.</td>
<td>0 (disabled - default) 1 (enabled)</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disables the PLC runtime in the UA namespace, so that the corresponding node is not displayed. It is advisable to enable this parameter if certain PLC runtimes are not yet available at the time of project planning, for example because the corresponding devices are not yet connected to the network.</td>
<td>0 (disabled - default) 1 (enabled)</td>
</tr>
</tbody>
</table>
The following section uses a sample to illustrate how the variables can be imported from a PLC program into the server. It is assumed that the PLC runtime and the TwinCAT OPC UA Server in its standard configuration (delivery state after installation) are on the same computer.

**Step 1: Configuring PLC variables**

The TwinCAT OPC UA Server automatically establishes a connection to the first PLC runtime on the local system. The PLC symbols marked in the PLC program for OPC UA are taken into account when the server is started. A comment at the appropriate position (instance, structure, variable) in the PLC program code is used for identification (see the following samples).

**Sample 1**

In this sample, the PLC variables bMemFlag1, bMemFlag2, bMemAlarm2 and iReadOnly are enabled via OPC UA. The PLC variable bMemAlarm1 should not be accessible via the OPC UA Server.

**TwinCAT 3 (TMC import):**

```
{attribute 'OPC.UA.DA' := '1'}
bMemFlag1 : BOOL;
{attribute 'OPC.UA.DA' := '1'}
bMemFlag2 : BOOL;
bMemAlarm1 : BOOL;
{attribute 'OPC.UA.DA' := '1'}
bMemAlarm2 : BOOL;
{attribute 'OPC.UA.DA.Access' := '1'}
iReadOnly : INT;
```

**TwinCAT 2 (TPY import):**

```
bMemFlag1 : BOOL; (*~ (OPC:1:some description) *)
bMemFlag2 : BOOL; (*~ (OPC:1:some description) *)
bMemAlarm1 : BOOL;
bMemAlarm2 : BOOL; (*~ (OPC:1:some description) *)
iReadOnly : INT; (*~ (OPC:1:some description)
   (OPC_PROP[0005]:1:read-only flag) *)
```

Due of the additional comment `OPC.UA.DA.Access` the access level for the variable iReadOnly is set to "ReadOnly". The various options can be found in the complete list of PLC comments (see List of attributes and comments).

**TPY import for TwinCAT 3**

The TPY import can also be used in TwinCAT 3 PLC projects for migration purposes, e.g. if you convert a TwinCAT 2 project into a TwinCAT 3 project and do not want to make any changes to the PLC comments. Please note, however, that some advanced functions are only available for the newer import mechanism (TMC).

You may assign a description to a variable in the server, which is stored in the corresponding OPC UA attribute ("Description"). This function is only available for TwinCat 3.

**TwinCAT 3 (TMC import):**

```
{attribute 'OPC.UA.DA' := '1'}
bMemFlag1 : BOOL; (* Description for variable bMemFlag1 *)
```

The comment automatically becomes the description attribute of the node in the UA namespace.
Sample 2:

In this sample, the two instances fbTest1 and fbTest2 of the function block FB_BLOCK1 should be available via OPC UA. When an entire instance is released, all its symbols are also available via OPC UA. The PLC program looks like the following:

**TwinCAT 3 (with TMC import):**

```
PROGRAM MAIN
VAR
  {attribute 'OPC.UA.DA' := '1'}
  fbTest1 : FB_BLOCK1;
  fbTest2 : FB_BLOCK1;
END_VAR

FUNCTION_BLOCK FB_BLOCK1
VAR_INPUT
  {attribute 'OPC.UA.DA' := '1'}
  ni1 : INT;
  ni2 : INT;
END_VAR

VAR_OUTPUT
  {attribute 'OPC.UA.DA' := '1'}
  no1 : INT;
  no2 : INT;
END_VAR

VAR
  {attribute 'OPC.UA.DA' := '1'}
  nx1 : INT;
  nx2 : INT;
END_VAR
```

**TwinCAT 2 (with TPY import):**

```
PROGRAM MAIN
VAR
  fbTest1 : FB_BLOCK1; (*~ (OPC:1:some description) *)
  fbTest2 : FB_BLOCK1;
END_VAR

FUNCTION_BLOCK FB_BLOCK1
VAR_INPUT
  ni1 : INT; (*~ (OPC:1:some description) *)
  ni2 : INT;
END_VAR

VAR_OUTPUT
  no1 : INT; (*~ (OPC:1:some description) *)
  no2 : INT;
END_VAR

VAR
  nx1 : INT; (*~ (OPC:1:some description) *)
  nx2 : INT;
END_VAR
```
The instance fbTest1 is enabled for OPC UA, whereby all contained symbols are automatically enabled for OPC UA, i.e. fbTest.ni1, fbTest.ni2, etc. The instance fbTest2 is not marked for OPC UA, but the three variables contained in it - ni1, no1 and nx1 - were marked in the function block. They are therefore available in all instances via OPC UA.

**Step 2: Activating the download of the symbol file**

The symbol file contains information about all variables available in a PLC project. The TwinCAT OPC UA Server needs this information to configure its namespace. By default, the current symbol information is automatically generated and stored in a symbol file. This is located in the project folder of the corresponding TwinCAT project. To ensure that the symbol file is transferred to the target runtime, enable the download of the symbol file in the settings of the PLC project.

**TwinCAT 3:**

![TwinCAT 3 project settings](https://example.com/twincat3.png)

**TwinCAT 2:**

![TwinCAT 2 project settings](https://example.com/twincat2.png)
[Optional] Step 3: Connecting further runtimes

By default, the TwinCAT OPC UA Server connects to the first PLC runtime on the local system. To make more than one PLC runtime available on the server, or if the PLC runtime is located on another system, corresponding settings are required in the TwinCAT OPC UA Configurator.

Configure all further necessary parameters as described in the section General information [66].

Connecting remote computers

To configure a runtime that is located on a remote Industrial PC or Embedded PC, enter the correct parameters for AmsNetId and AdsPort and provide the corresponding symbol file of the PLC program on this PC. Also, make sure that an ADS route to the remote system has been established.

[Optional] Step 4: Explicit hiding of symbols

In addition to the regular PLC attributes for activating a PLC symbol, you can explicitly exclude PLC symbols from publication in the OPC UA namespace. There may be several reasons for this:

- You want to publish a data structure, but not all its subelements (Sample 1).
- You have enabled a data structure in the definition and want to hide an individual instance of this data structure (Sample 2).

Sample 1:

```plaintext
[attribute 'OPC.UA.DA' := '1']
TYPE ST_TEST :
STRUCT
  a : INT;
  b : DINT;
END_STRUCT
END_TYPE

PROGRAM MAIN
VAR
  instance1 : ST_TEST;
  instance2 : ST_TEST;
END_VAR
```
In this case, the PLC attribute has been added to the structure definition, so that each instance of this structure should be available on the OPC UA Server. Subelement b (and all its subelements, if b is another data structure) will be excluded from publication on the OPC UA Server.

Sample 2:

```plaintext
{attribute 'OPC.UA.DA' := '1'}
TYPE ST_TEST :
   STRUCT
   a : INT;
   b : DINT;
   END_STRUCT
END_TYPE

PROGRAM MAIN
VAR
   instance1 : ST_TEST;
   {attribute 'OPC.UA.DA' := '0'}
   instance2 : ST_TEST;
END_VAR
```

Although the PLC attribute is added to the structure definition, which makes each instance of this structure available on the OPC UA Server, instance2 receives the PLC attribute to disable this inheritance. This means that only instance1 is available in the UA namespace, not instance2.

### 4.1.4.1.1 Arrays

By default arrays are regarded as individual nodes in the UA namespace. This means that if you define, for example, an array `dyn_BOOL[10]` in the PLC (and have also enabled it for OPC UA), it will subsequently appear in the UA namespace as follows:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns=4:s=</td>
<td>dyn_BOOL dyn_BOOL</td>
<td>True, True, True, True, True</td>
</tr>
</tbody>
</table>

The advantage of this approach is a considerable reduction in the complexity of the UA namespace and in memory consumption, since not every position of an array needs to be made available as an individual node in the namespace. However, modern UA Clients can continue to access the individual array positions via the so-called "RangeOffset".

In order to support older UA Clients that don’t offer this feature, however, you can also make the positions of an array available as individual nodes in the UA namespace. It is illustrated as follows:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns=4:s=</td>
<td>dyn_BOOL[0] dyn_BOOL[1]</td>
<td>False</td>
</tr>
<tr>
<td>ns=4:s=</td>
<td>dyn_BOOL[0] dyn_BOOL[1]</td>
<td>False</td>
</tr>
</tbody>
</table>

This setting is available by activating the **Legacy Array Handling** option in the UA Configurator within the respective namespace configuration.

Depending on the scope of the PLC project, the UA namespace can become significantly more complex, which in turn is reflected in an increased memory utilization of the UA Server.

Changes to the settings listed above only become active after restarting the UA Server.
4.1.4.1.2 Enums

Enumerations in OPC UA always have the data type Int32. However, the IEC61131-3 allows to define data types bigger than Int32. In order to treat those enumerations properly, the TwinCAT OPC UA Server provides the configuration option <ImportBigEnumsNumeric> that can be activated in its Data Access configuration file.

Per default this option is set to false. This means that if the enum value falls out of the Int32 range, a status code exception BadOutOfRange is thrown.

If the option is set to true, enumerations with data types bigger than Int32 are treated as regular variables with that particular data type.

Let’s assume that we have the following enum definitions in our PLC code:

```plaintext
TYPE E_Enum_Normal :
{
    enum_member_0 := 0,
    enum_member_1 := 1,
    enum_member_2 := 2
}
END_TYPE

TYPE E_Enum_NotSoBig :
{
    enum_member_0 := 0,
    enum_member_1 := 1,
    enum_member_2 := 2
} UINT;
END_TYPE

TYPE E_Enum_VeryBig :
{
    enum_member_0 := 0,
    enum_member_1 := 1,
    enum_member_2 := 2
} LINT;
END_TYPE
```

When activating the configuration option from above, instances of E_Enum_VeryBig will be treated as a regular variable of data type Int64 in the server’s namespace whereas instances of E_Enum_Normal and E_Enum_NotSoBig are treated as an OPC UA enumeration (with data type Int32):

### Properties

The display of PLC properties in the server namespace has been supported since TwinCAT 3.1 Build 4024. All you need to do is set a special PLC attribute on the Property so that the Property is imported into the namespace and represented there as a UA Property. Sample:

```plaintext
{attribute 'monitoring' := 'call'}
PROPERTY Property_1 : BOOL
```

The function block on which the Property is defined must contain the normal PLC attribute for enabling symbols [165].
StructuredTypes

StructuredTypes allow you to read or write structures without interpreting each byte, because the UA Server returns the information type of each element of the structure. Based on complex functions in modern OPC UA SDKs, OPC UA Clients can search and interpret this structural information.

From version 2.2.x of the OPC UA Server, structures of the TwinCAT 3 runtime (TMC and TMI import only) are generated as a StructuredType in the UA namespace.

Sample:

```plaintext
STRUCT ST_Communication:
    TYPE ST_Communication :
        STRUCT
            a : INT;
            b : INT;
            c : INT;
        END_STRUCT
    END_TYPE

Program MAIN:

PROGRAM MAIN
    VAR
        {attribute 'OPC.UA.DA' := '1'}
        {attribute 'OPC.UA.DA.StructuredType' := '1'}
        stCommunication : ST_Communication;
    END_VAR

Filtered mode

If filters are used to make symbols available via OPC UA, a STRUCT or function block must be fully available in the UA namespace in order to be displayed as a StructuredType.

Pointers and references

If pointers and references are used in the structure, then they cannot be converted into a StructuredType. The OPC UA Server then illustrates these structures as regular FolderTypes with the corresponding member variables.

The instance stCommunication is then displayed in the UA namespace as a StructuredType:
Alternatively, the STRUCT definition can also be assigned the PLC attribute to make all instances of STRUCT available as StructuredType.

```plaintext
{attribute 'OPC.UA.DA.StructuredType' := '1'}

TYPE ST_Communication :
  STRUCT
    a : INT;
    b : INT;
    c : INT;
  END_STRUCT
END_TYPE
```

In order to deactivate StructuredType of a certain instance, use the following attribute:

```plaintext
PROGRAM MAIN
  VAR
    {attribute 'OPC.UA.DA' := '1'}
    stCommunication : ST_Communication;
    END_VAR
```

**Function block StructuredType**

In addition, each function block of the TwinCAT 3 PLC also contains a child node, FunctionBlock, which contains the entire function block as a StructuredType.

**Sample:**

**Function block:**

```plaintext
FUNCTION_BLOCK FB_FunctionBlock
  VAR_INPUT
    Input1 : INT;
    Input2 : LREAL;
  END_VAR
  VAR_OUTPUT
    Output1 : LREAL;
  END_VAR
```

**Instance of the function block:**
Instance of the function block in the OPC UA namespace:

```plaintext
BEGIN_VAR
  VAR
    {attribute 'OPC.UA.DA' := '1'}
    {attribute 'OPC.UA.DA.StructuredType' := '1'}
    fbFunctionBlock : FB_FunctionBlock;
  END_VAR
```

FunctionBlock node with StructuredType:

```plaintext
FUNCTION_BLOCK FB_FunctionBlock
  VAR_INPUT
    Input1 : INT;
    Input2 : LREAL;
  END_VAR
  VAR_OUTPUT
    Output1 : LREAL;
  END_VAR
```

Alternatively, the function block can also receive a PLC attribute to make all instances of the function block available as StructuredType.

```plaintext
BEGIN_VAR
  VAR
    {attribute 'OPC.UA.DA' := '1'}
    {attribute 'OPC.UA.DA.StructuredType' := '0'}
    fbFunctionBlock : FB_FunctionBlock;
  END_VAR
```

Maximum size of the structure

The maximum size of a structure is 16 kByte by default. Each STRUCT constantly exchanges data with the basic ADS device, i.e. a large ADS message is sent with each read/write command of a StructuredType. To prevent the ADS router from being flooded with large messages, the maximum size is limited. You can change this specification in the file ServerConfig.xml. To do this, the key <MaxStructureSize> must be added to OpcServerConfig\UaServerConfig', and a new value for the maximum size of a structure must be set in bytes. If a structure exceeds <MaxStructureSize>, it is imported as FolderType, where each structure item is available as a single node.
4.1.4.1.5 AnalogItemTypes

AnalogItemTypes are part of the OPC UA specification and allow meta information such as units to be attached to a variable. You can define these items of meta information in the form of PLC attributes in the TwinCAT 3 PLC.

The following parameters can be set:

- EngineeringUnits: Units defined by the OPC UA specification
- EURange: Maximum value range of the variables
- InstrumentRange: Normal value range of the variables
- WriteBehavior: Behavior if the value range is exceeded during a write operation.

The following sample shows how the fillLevel variable is configured as an AnalogItemType. The following parameters are hereby set:

- Unit: 20529 ("Percent", defined in the OPC UA specification)
- Max. value range: 0 to 100
- Normal value range: 10 to 90
- Write behavior: 1 (Clamping)

```{attribute 'OPC.UA.DA' := '1'}
{attribute 'OPC.UA.DA.AnalogItemType' := '1'}
{attribute 'OPC.UA.DA.AnalogItemType.EngineeringUnits' := '20529'}
{attribute 'OPC.UA.DA.AnalogItemType.EURange' := '0:100'}
{attribute 'OPC.UA.DA.AnalogItemType.InstrumentRange' := '10:90'}
{attribute 'OPC.UA.DA.AnalogItemType.WriteBehavior' := '1'}
```

fillLevel : UINT;

EngineeringUnits can be configured using the IDs specified in OPC UA (Part 8 of the OPC UA specification). The IDs are based on the widely used and accepted "Codes for Units of Measurement (Recommendation N.20)" published by the "United Nations Center for Trade Facilitation and Electronic Business". CommonCode, which specifies the three-digit alphanumeric ID, is converted by OPC UA according to specification into an Int32 value and referenced (extract from OPC UA specification v1.02, pseudo-code):

```int32 unitId = 0;
int32 c;
for (i=0; i<=3;i++)
{
    c = CommonCode[i];
    if (c == 0)
        break; // end of Common Code
    unitId = unitId << 8; // shift left
    unitId = unitId | c; // OR operation
}
```

Write behavior

When writing an AnalogItemType variable, you can define how the OPC UA Server should handle the new value in relation to the value range. The following options are available:

- 0: All values are allowed and are accepted during a write operation.
- 1: The value to be written is truncated according to the value range.
- 2: The value to be written is rejected if it exceeds the value range.

4.1.4.1.6 Type system

One of the biggest advantages of OPC UA is the meta-model, which can be used to provide base types as well as to extend the type system with custom models. The same mechanism is used to represent real objects (nodes) so that OPC UA Clients can determine an object type.

The OPC UA Server publishes type information from the IEC61131 world in its namespace. This includes not only base types such as BOOL, INT, DINT, or REAL, but also extended type information such as the current class (function block) or structure that represents an object.
Type information

Type information is part of the UA namespace. The OPC UA Server extends the basic type information as follows:

- Local type information that is only valid for one runtime is stored in the same namespace as the runtime symbols.
- Global type information that can be valid for different runtimes is stored in a separate global namespace.

The type system is also virtually available and can be viewed in the Types area of the OPC UA Server:

Every non-standard data type is entered in the BeckhoffCtrlTypes area.

Basic principles

Assuming the TwinCAT 3 PLC consists of a PLC program with different STRUCTs. Each STRUCT is represented as a node in a UA namespace, with each element of the structure as a subordinate node.

In this sample the STRUCT stSampleStruct consists of three subordinate elements: one variable nValue1 of the type INT, one variable bValue2 of the type BOOL and a further STRUCT stSubStruct, which contains only one subordinate element (variable nValue of the type INT).
The structure itself is a regular variable in the UA namespace and has the data type ByteString. The clients can therefore simply be connected to the root element (the structure itself), and its values can be read/written by interpreting the ByteString. To simplify the interpretation of each subordinate element, the type system contains more information about the structure itself, primarily in the instance reference:

![Diagram](image1.png)

In addition, the type system contains more information about ST_SampleStruct:

![Diagram](image2.png)

And in the references of ST_SampleStruct:

![Diagram](image3.png)

Overall, the type system can offer very useful information if a Client wants to interpret the structure further.

**Object-orientated extensions**

Assuming the TwinCAT 3 PLC runtime contains a PLC program whose structure can be visualized as follows:
The two function blocks Scanner and Drive are derived from the base class Device by using object-oriented extensions of IEC61131-3. The MAIN program now contains the following declarations:

```
PROGRAM MAIN
VAR
  {attribute 'OPC.UA.DA':='1'}
  Scanner1 : Scanner;
  {attribute 'OPC.UA.DA':='1'}
  Scanner2 : Scanner;
  {attribute 'OPC.UA.DA':='1'}
  DriveX : Drive;
END_VAR
```

All three objects are of type Device, but also of their special data type. The OPC UA Server imports the objects as follows:

The basic data type can now be determined in the reference of each object, e.g. object Scanner1:
According to the basic IEC61131 program, the object Scanner1 is of the data type Scanner and also shows which variables are contained and what type the variable is: input, output or internal (local) variable. The diagram above shows that not only the variables of the actual function block are displayed here, but also the derived variables of the base class. The entire IEC61131-3 inheritance chain is represented in the UA namespace.

4.1.4.1.7 StatusCode

The OPC UA Server enables a PLC application to change the OPC UA StatusCode.

Perform the following steps to configure and affect the StatusCode of a variable:

- Creating a PLC structure [80]
- Overwriting StatusCode [80]

Creating a PLC structure

So that the data consistency is guaranteed, the concept of changing the OPC UA StatusCode is based on StructuredTypes (see StructuredTypes [73]). Each variable whose UA StatusCode is to be affected must be included in a STRUCT.

Create a new STRUCT and add a PLC attribute before the STRUCT definition. The STRUCT contains the variable itself and a variable of the data type DINT, which represents the StatusCode and to which reference is made in the attribute in front of the STRUCT definition.

```plaintext
{attribute 'OPC.UA.DA.STATUS' := 'quality'}
TYPE ST_StatusCodeOverride :
  STRUCT
    value : REAL;
    quality: DINT;
  END_STRUCT
END_TYPE
```

Now create an instance of this STRUCT, for example in the MAIN program, and add the regular PLC attribute so that this instance becomes available via OPC UA.

```plaintext
PROGRAM MAIN
VAR
  {attribute 'OPC.UA.DA' := '1'}
  stStatusCodeOverride : ST_StatusCodeOverride;
END_VAR
```

This instance is now available inside the OPC UA namespace as a StructuredType.

Overwriting StatusCode

To overwrite the UA StatusCode for the STRUCT, simply edit the value of the variable "quality". If you set this, for example, to "-2147155968", the StatusCode of the STRUCT changes to "BadCommunicationError").
The value must be determined according to the definition in the OPC UA specification.

The following table lists only some of the available StatusCodes and their corresponding decimal representation. Consult the official OPC UA specification for a more comprehensive list of the StatusCodes.

<table>
<thead>
<tr>
<th>StatusCode</th>
<th>Hex</th>
<th>Decimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>BadUnexpectedError</td>
<td>0x80010000</td>
<td>-2147418112</td>
</tr>
<tr>
<td>BadInternalError</td>
<td>0x80020000</td>
<td>-2147352576</td>
</tr>
<tr>
<td>BadCommunicationError</td>
<td>0x80050000</td>
<td>-2147155968</td>
</tr>
<tr>
<td>BadTimeout</td>
<td>0x800A0000</td>
<td>-2146828288</td>
</tr>
<tr>
<td>BadServiceNotSupported</td>
<td>0x800B0000</td>
<td>-2146762752</td>
</tr>
</tbody>
</table>

When calculating the decimal representation of other UA StatusCodes on the basis of their hexadecimal representation, make sure that your computer is set to DWORD, e.g. the Windows computer (“Programmer” view).

4.1.4.1.8 List of attributes and comments

The runtime variables for various OPC UA functions (e.g. data access or historical access) are configured directly in the PLC program or in the TMC code editor (if using TwinCAT 3 C++). The advantage is that PLC developers can decide directly in the program with which they are familiar whether and how a variable is to be enabled for OPC UA. You activate a variable by inserting a comment and the corresponding OPC UA tag in front of the variable, e.g.:

**TwinCAT 3 PLC (TMC):**

```plaintext
[attribute 'OPC.UA.DA' := '1']
bVariable : BOOL;
```

**TwinCAT 2 PLC (TPY):**

```plaintext
bVariable : BOOL; (*~ (OPC:1:available)*)
```

You can find a detailed description of the use of attributes and comments in the sections concerning the corresponding runtime components:

- PLC
- C++
- I/O
- Matlab/Simulink

The following table shows an overview of all definable tags and their meaning. The subsections of the corresponding function contain a detailed description of the functional principle.

**TwinCAT 3 (TMC):**
<table>
<thead>
<tr>
<th>OPC UA function</th>
<th>PLC tag</th>
<th>C++ TMC code editor (Optional features)</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| Data Access (DA) | `{attribute 'OPC.UA.DA' := '0'}` | Name: OPC.UA.DA_DA
Value: 0 | Locks a variable for OPC UA, whereupon it is no longer visible in the UA namespace. |
| Data Access (DA) | `{attribute 'OPC.UA.DA' := '1'}` | Name: OPC.UA.DA_DA
Value: 1 | Enables a variable for OPC UA, whereupon it becomes visible in the UA namespace. This tag must always be set if you want to use a variable for UA. |
| Data Access (DA) | `{attribute 'OPC.UA.DA.Access' := 'x'}` | Name: OPC.UA.DA_DA.Access
Value: see right column | Sets read/write access for a variable, depending on parameter "x".
0 = none
1 = read-only
2 = write access only
3 = read and write access (default if no tag is used) |
| Data Access (DA) | `{attribute 'OPC.UA.DA.Description' := 'x'}` | Name: OPC.UA.DA_Description
Value: see right column | Sets a text for the OPC UA attribute "Description". |
| Data Access (DA) | `{attribute 'OPC.UA.DA.StructuredType' := '0'}` | Name: OPC.UA.DA_StructuredType
Value: 0 | Disables StructuredType for a STRUCT or a function block |
| Data Access (DA) | `{attribute 'OPC.UA.DA.StructuredType' := '1'}` | Name: OPC.UA.DA_StructuredType
Value: 1 | Enables StructuredType for a STRUCT or a function block |
| Data Access | `{attribute 'OPC.UA.DA.Status' := 'quality'}` | Name: OPC.UA.DA_Status
Value: quality | Manually define the StatusCode of a symbol in the UA namespace. Only for data structures. The value "quality" specifies which DINT subelement of the data structure determines the StatusCode. See corresponding article in the documentation for more information. |
| Historical Access (HA) | `{attribute 'OPC.UA.HA' := '1'}` | Name: OPC.UA.HA
Value: 1 | Enables a variable for Historical Access. Must be used with `{attribute 'OPC.UA.DA' := '1'}. |
| Historical Access (HA) | `{attribute 'OPC.UA.HA.Storage' := 'x'}` | Name: OPC.UA.HA_Storage
Value: see right column | Defines the storage location for Historical Access, depending on parameter "x".
1 = RAM
2 = File
3 = SQL Compact Database
4 = SQL Server Database |
<table>
<thead>
<tr>
<th>OPC UA function</th>
<th>PLC tag</th>
<th>C++ TMC code editor (Optional features)</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historical Access (HA)</td>
<td>{attribute 'OPC.UA.HA.Sampling' := 'x'}</td>
<td>Name: OPC.UA.HA.Sampling</td>
<td>Determines the sampling rate at which the variable values are to be stored, in [ms] depending on the parameter &quot;x&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value: see right column</td>
<td></td>
</tr>
<tr>
<td>Historical Access (HA)</td>
<td>{attribute 'OPC.UA.HA.Buffer' := 'x'}</td>
<td>Name: OPC.UA.HA.Buffer</td>
<td>Defines the maximum number of values that remain in the data memory, depending on the parameter &quot;x&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value: see right column</td>
<td></td>
</tr>
</tbody>
</table>

**TwinCAT 2 (TPY):**

<table>
<thead>
<tr>
<th>OPC UA function</th>
<th>PLC tag</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Access (DA)</td>
<td>(*~ (OPC:0: not available) *)</td>
<td>Locks a variable for OPC UA, whereupon it is no longer visible in the UA namespace.</td>
</tr>
<tr>
<td>Data Access (DA)</td>
<td>(*~ (OPC:1: available) *)</td>
<td>Enables a variable for OPC UA, whereupon it becomes visible in the UA namespace. This tag must always be set if you want to use a variable for UA.</td>
</tr>
<tr>
<td>Data Access (DA)</td>
<td>(*~ (OPC_PROP[0005]:1: read-only) *)</td>
<td>Sets the write protection for a variable. Must be used together with (*~ (OPC:1: available) *).</td>
</tr>
<tr>
<td>Data Access (DA)</td>
<td>(*~ (OPC_UA_PROP[5100]: x: Alias name) *)</td>
<td>Specifies x as node name in the UA namespace, so-called alias mapping.</td>
</tr>
<tr>
<td>Historical Access (HA)</td>
<td>(*~ (OPC_UA_PROP[5000]:x:Storage media) *)</td>
<td>Enables a variable for Historical Access. Must be used together with (*~ (OPC:1: available) *). x defines the storage medium for saving the data values: 1 = RAM 2 = File 3 = SQL Compact Database 4 = SQL Server Database</td>
</tr>
<tr>
<td>Historical Access (HA)</td>
<td>(*~ (OPC_UA_PROP[5000][1]:x:SamplingRate) *)</td>
<td>Determines the sampling rate at which the variable values are to be stored, in [ms] depending on the parameter &quot;x&quot;</td>
</tr>
<tr>
<td>Historical Access (HA)</td>
<td>(*~ (OPC_UA_PROP[5000][2]:x:Buffer) *)</td>
<td>Defines the maximum number of values that remain in the data memory, depending on the parameter &quot;x&quot;.</td>
</tr>
</tbody>
</table>

### 4.1.4.2 C++

This section describes how to configure the namespace of the TwinCAT OPC UA Server in order to obtain access to the symbols of a TwinCAT 3 C++ module. For this you can either use the OPC UA Configurator or carry out the configuration directly in the file ServerConfig.xml of the OPC UA Server.

This section contains the following topics:
- Step 1: Project-related settings
- Step 2: Configuring the UA Server
Step 1: Project-related settings

To configure certain symbols contained in an instance of a C++ module in such a way that they are accessible via OPC UA, the following settings are necessary in the corresponding C++ module instance in TwinCAT XAE.

1. The OPC UA Server requires the TMI symbol file, which is not passed to the target runtime by default. Enable the transfer by setting the following options:

   - Enable the transfer by setting the following options:
     - The generated TMI file is named after the Object ID, e.g. "Obj_01010020.tmi" and stored in the TwinCAT boot directory, e.g. C:\TwinCAT\3.1\Boot\Tmi.

2. Select which symbols are to be made accessible to the corresponding variables by checking the Create symbol checkbox in the TMC code generator. Then execute the TMC CodeGenerator.

Step 2: Configuring the UA Server

You can configure and parameterize the access to TwinCAT 3 C++ modules simply with the help of the OPC UA Configurator. To do this, add a new device of the type "CPP TwinCAT 3 (TMI) filtered" in the Data Access area. The SymbolFile field must point to the TMI file created for the C++ module instance. This TMI file is located in the TwinCAT boot directory, e.g. C:\TwinCAT\3.1\Boot\Tmi, and is named after the ObjectID of the TwinCAT 3 C++ module instance.

The configurable parameters describe the following functions:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS Port</td>
<td>Defines the ADS port under which the C++ module instance is accessible. The ADS port can be read in the properties of the C++ task.</td>
<td>351 352 …</td>
</tr>
<tr>
<td>AutoCfg</td>
<td>First defines the type of the target runtime used for communication, e.g. PLC, C++, I/O. A further distinction can then be made within these categories. Each AutoCfg option is available as an unfiltered or filtered option. Filtered means the user can determine which C++ symbols are made publicly accessible via OPC UA. When using an unfiltered option, each C++ symbol is published to OPC UA.</td>
<td>4020 CPP TwinCAT 3 (TMI) 4021 CPP TwinCAT 3 (TMI) filtered</td>
</tr>
<tr>
<td>AutoCfgSymFile</td>
<td>Symbol file (TMI) of the corresponding C++ module instance.</td>
<td>Path to the symbol file. (TMI)</td>
</tr>
<tr>
<td>IoMode</td>
<td>Defines the method for accessing symbols.</td>
<td>1 (access via handle - default)</td>
</tr>
<tr>
<td>ArraySubItemLegacy Support</td>
<td>By default, subelements of an array are not mapped as separate nodes in the UA namespace. Instead, only the array is mapped as a single element. Nonetheless, UA Clients can access subelements via their &quot;IndexRange&quot;. (Some older OPC UA Clients do not yet support this option). The flag was introduced so that access is nevertheless possible for these clients. It ensures that every array position is displayed as a separate node in the UA namespace. This leads to higher memory requirement of the OPC UA Server.</td>
<td>0 (disabled - default) 1 (enabled)</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disables the C++ module instance in the UA namespace, so that the corresponding node is not displayed. It is advisable to enable this parameter if certain C++ runtimes are not yet available at the time of project planning, for example because the corresponding devices are not yet connected to the network.</td>
<td>0 (disabled - default) 1 (enabled)</td>
</tr>
</tbody>
</table>

4.1.4.2.1 Arrays

By default arrays are regarded as individual nodes in the UA namespace. This means that if you define, for example, an array `dyn_BOOL[10]` in the PLC (and have also enabled it for OPC UA), it will subsequently appear in the UA namespace as follows:

![Browser]

The advantage of this approach is a considerable reduction in the complexity of the UA namespace and in memory consumption, since not every position of an array needs to be made available as an individual node in the namespace. However, modern UA Clients can continue to access the individual array positions via the so-called "RangeOffset".

In order to support older UA Clients that don’t offer this feature, however, you can also make the positions of an array available as individual nodes in the UA namespace. It is illustrated as follows:
This setting is available by activating the Legacy Array Handling option in the UA Configurator within the respective namespace configuration.

Depending on the scope of the PLC project, the UA namespace can become significantly more complex, which in turn is reflected in an increased memory utilization of the UA Server.

Changes to the settings listed above only become active after restarting the UA Server.

4.1.4.3 Matlab/Simulink

This section describes how to use TwinCAT 3 TMI files for TcCOM modules to construct the namespace of the OPC UA Server.

This section contains the following topics:

- General Information [\ref{general-information}]
- Generating and importing a TMI file for TcCom modules [\ref{generating-and-importing-a-tmi-file-for-tc-com-modules}]
- Filtered or unfiltered mode [\ref{filtered-or-unfiltered-mode}]

**General Information**

If you use TwinCAT 3 C++ or the Matlab/Simulink integration, you can generate a symbol file (TMI file) for the arising TcCom modules from the TwinCAT 3 XAE.

The OPC UA Server imports this TMI file and generates its namespace using the symbol information contained in the file. The namespace can then consist of variables (= symbols) that are contained in the respective TcCom module.

The import of TMI files is configured in the OPC UA Configurator.

**Generating and importing a TMI file for TcCom modules**

In order for a TMI file to be generated and for TwinCAT to automatically copy the TMI file to the target system, enable the option Copy TMI to Target in the settings of the TcCOM module:
After activating the project, the boot directory of the target system contains the TMI file for the TcCOM module. This file can then be imported into the OPC UA namespace with the help of the OPC UA Configurator.

The configured OPC UA namespace then contains a representation of the Matlab/Simulink block diagram:
Filtered or unfiltered mode

Note that there is currently no filtered mode for generic TcCOM module instances. Filtered mode is only possible for TwinCAT 3 C++ module instances if the TMC Code Editor is used. TwinCAT Matlab/Simulink integration offers several filter options. These are described in the documentation TE1400 in section Data exchange.

If a generic TcCOM module instance (e.g. a Matlab/Simulink module) is to be imported, the unfiltered option must be used and therefore all symbols of the modules are published in the OPC UA namespace.

4.1.4.4 I/O task

This section describes how you can make IO task variables accessible via the data access functions of the TwinCAT OPC UA Server.

This section contains the following topics:
Technical introduction

- General Information [89]
- Step 1: Configure a TwinCAT I/O task to enable symbol handling. [89]
- Step 2: Add the I/O task to the OPC UA namespace [90]

General Information

You can publish the variables of a task with process image via OPC UA.

The way in which the variables are displayed and how they are communicated with is determined by various parameters. You can define these parameters with the help of the OPC UA Configurator or directly in the configuration file ServerConfig.xml.

The following table provides an overview of all parameters that are important when accessing the I/O task.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS Port</td>
<td>Defines the ADS port under which the I/O task is accessible. The ADS port can be read out in the properties of the I/O task.</td>
<td>301, 302, ...</td>
</tr>
<tr>
<td>AutoCfg</td>
<td>Initially defines the type of target runtime used for the communication, e.g. PLC, C++, I/O. A finer distinction can subsequently be made within these categories. Each AutoCfg option is available as an unfiltered or filtered option. Filtered means that users can determine which I/O variables are made publicly available to the OPC UA via comments. When using an unfiltered option, each task variable is published to OPC UA.</td>
<td>107 I/O TwinCAT 2/3, 108 I/O TwinCAT 2/3 filtered</td>
</tr>
<tr>
<td>AutoCfgSymFile</td>
<td>Specifies the path of the CurrentConfig.xml file, which is normally located in the folder C:\TwinCAT\3.1\Boot. Path of CurrentConfig.xml</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>Disables the I/O task in the UA namespace, so that the corresponding node is not displayed. It is advisable to enable this parameter if certain runtimes are not yet available at the time of project planning, for example, because the corresponding devices are not yet connected to the network.</td>
<td>0 (disabled - default), 1 (enabled)</td>
</tr>
</tbody>
</table>

The following steps describe how to import variables from an I/O task into the UA namespace. This requires the OPC UA Server and the runtime to be on the same computer.

**Step 1: Configure a TwinCAT I/O task to enable symbol handling.**

Open the I/O task settings and enable the **Create symbols** option. At this point, note the ADS port of the I/O task (in the example, this is 301).
Step 2: Add the I/O task to the OPC UA namespace

Configure the OPC UA Server so that it offers access to the I/O task. Using the OPC UA Configurator, add a new device of type "IO TwinCAT 2/3" and configure its settings for AdsNetId, AdsPort and SymbolFile (path to the CurrentConfig.xml file).

After setting the corresponding properties, restart the OPC UA Server to enable these settings.

4.1.5 Historical Access

This section describes the steps necessary to configure the variables in the namespace of the OPC UA Server for Historical Access (HA).

Historical Access is an OPC UA function, in which the variable values are either stored permanently on a data storage device (file or database) or in the device RAM, so that they can be retrieved later by the client. The way in which the OPC UA Server reads and stores the variable values can be configured.
Technical introduction

The Historical Access configuration is available for variables from any runtime system (PLC, C++, ...). As a prerequisite, the respective variable must first be enabled for OPC UA. For details on how to do this please refer to the respective document under "Data Access".

Requirements and recommendations

The following prerequisites apply to the use of Historical Access:

- The runtime system whose symbols are to be stored for Historical Access must be configured for Data Access (and the respective variables must be enabled).
- In order to use an SQL Compact database as a storage medium, SQL Compact Runtime 3.5 SP2 must be installed on the computer on which the OPC UA Server is running.
- SQL Compact databases are also supported under Windows CE.
- SQL Server databases are not supported under Windows CE.
- The following MS SQL Server versions are supported: 2014, 2017, 2019
- The following recommendations apply when using the respective memory type:
  - Main memory: Number of entries < 5000
  - File system: Number of entries < 10000
  - Database: Number of entries >= 10000

The following memory types are supported:

<table>
<thead>
<tr>
<th>Memory type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main memory</td>
<td>Saves the values in the RAM of the device on which the OPC UA Server is running. No further parameters are required. After restarting the device, the stored values are no longer available. The storage medium is therefore not persistent. The above requirements and recommendations apply.</td>
</tr>
<tr>
<td>File system</td>
<td>Saves the values in several files, the location of which can be specified. Each symbol configured for this storage medium is assigned its own file in this directory. In addition, there is a backup copy of the file for each symbol, which is created when the buffer size is reached. The contents of the data file are then saved as a backup copy, and a new file is created. The above requirements and recommendations apply.</td>
</tr>
<tr>
<td>SQL Compact database</td>
<td>Saves the values to an SQL Compact database, the location of which can be specified. The above requirements and recommendations apply.</td>
</tr>
<tr>
<td>MS SQL Server database</td>
<td>Saves the values in an SQL Server database that is referenced with various parameters. The above requirements and recommendations apply.</td>
</tr>
</tbody>
</table>

The individual memory types are configured as HistoryAdapters in the server. This is done via the TwinCAT OPC UA Server configurator. Each HistoryAdapter (except for "Volatile" -> RAM) can be used repeatedly, e.g., if the historical values for individual variables are to be stored in different data memories. In the HistoryNodes area, the individual nodes are configured, assigned to a data memory and assigned a SamplingRate and a maximum size for the ring buffer to be used in the data memory.

The attribute HistoryWriteable="true" ensures that the data memory for this node can be filled with values via a HistoryUpdate() call. Such a call is provided, for example, by the TwinCAT OPC UA Client via the function block UA_HistoryUpdate. If you configure a node with this attribute, then the server doesn't normally "sample" the values itself, but receives them from other clients. In such a configuration the SamplingRate is therefore usually 0.

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>
4.1.5.1 Display historical data

Displaying Historical Access values in an OPC UA Client

The following step-by-step instructions describe how to configure the UA Expert software in order to access historical data.

1. Start the UA Expert software and connect to the OPC UA Server.
2. Add a new History Trend View.

3. Browse the PLC1 namespace and use drag & drop to add the PLC variables _HistoryDB, _HistoryDBcompact, _HistoryFast and _HistorySlowPersist.
You can now use the **Start Time** and **End Time** controls to specify the desired time period for which the symbol values are to be displayed, or you can start a **Cyclic Update** for these variables if necessary.

### 4.1.6 Alarms and Conditions

The steps required to configure OPC UA Alarms and Conditions (A&C) on the OPC UA Server are described in this section. The basic concept is independent of TwinCAT runtime, which means the configuration steps for PLC, C++, TcCOM runtime or only I/O task are the same.

OPC UA Alarms and Conditions (Part 9 of the OPC UA specification) describes a model for monitoring process values and outputting alarms and events when a runtime symbol changes its state.

#### Requirements

The following requirements apply to the use of OPC UA Alarms and Conditions:

- The runtime symbol to be monitored must be available in the namespace.
- The OPC UA Client must support Alarms and Conditions. In this section UA Expert (from Unified Automation) is used as the reference UA Client.

#### General Information

Execute the following steps once to release a symbol for Alarms and Conditions:
Technical introduction

- Step 1: Activating runtime symbol for data access [95] (so that the symbol is generally accessible via OPC UA.)
- Step 2: Activating A&C for a symbol [95]
- Step 3: Transferring your own user data with an event [96]
- Step 4: Triggering an event using the FireEvent method [97]
- Step 5: Configuring multilingual alarm texts [99]
- Step 6: Registering A&C with a reference OPC UA Client [99]

These steps are explained in more detail below. At the end of this section you will find information about receiving configured alarms via A&C with the UA Expert Reference Client.

Supported alarm types

The implementation of OPC UA Alarms and Conditions currently supports the following alarm types:

- LimitAlarmType: Define different limits for a symbol. If a limit is reached, the UA Server issues an alarm.
- OffNormalAlarmType: Define a value that is "normal". If the current value deviates from the "normal" value, the UA Server issues an alarm.

Step 1: Activating runtime symbol for data access

A variable must be available in the OPC UA Server in order for it to be configured for A&C. To do this in the case of a PLC variable, provide it with an attribute (see PLC [65]).

Step 2: Activating A&C for a symbol

You can configure a runtime symbol for A&C with the OPC UA Server Configurator. The Configurator has a simple graphical user interface for editing the XML file on which it is based. The configurator is available in two versions, depending on the setup version: Standalone or integrated in Visual Studio [49].

The following program extract shows a sample of this XML file to better understand the general behavior and structure of the A&C implementation.

```
<TcUaAcConfig>
  <ConditionController Name="ConditionController1" />
    <Condition Name="Counter" Severity="200">
      <LimitAlarmType LowLowLimit="-10" LowLimit="0" HighLimit="10" HighHighLimit="20" MessageNormal="100" MessageLowLow="10" MessageLow="11" MessageHigh="12" MessageHighHigh="13" />
      <ItemToMonitor SamplingRate="100" NS="urn:[NodeName]:BeckhoffAutomation:Ua:PLC1" NodeId="s=MAIN.nCounter1" />
    </Condition>
    <Condition Name="Switch" Severity="500">
      <OffNormalAlarmType Normal="0" MessageNormal="100" MessageOffNormal="20" />
      <ItemToMonitor SamplingRate="100" NS="urn:[NodeName]:BeckhoffAutomation:Ua:PLC1" NodeId="s=MAIN.bSwitch" />
    </Condition>
    <Condition Name="Struct" Severity="300">
      <LimitAlarmType LowLowLimit="-10" LowLimit="0" HighLimit="10" HighHighLimit="20" MessageNormal="100" MessageLowLow="10" MessageLow="11" MessageHigh="12" MessageHighHigh="13" />
      <ItemToMonitor SamplingRate="100" NS="urn:[NodeName]:BeckhoffAutomation:Ua:PLC1" NodeId="s=MAIN.stStruct" />
    </Condition>
  </ConditionController>
  <ConditionController Name="ConditionController2" />
    <Condition Name="Counter2" Severity="200">
      <LimitAlarmType LowLowLimit="-10" LowLimit="0" HighLimit="10" HighHighLimit="20" MessageNormal="100" MessageLowLow="10" MessageLow="11" MessageHigh="12" MessageHighHigh="13" />
      <ItemToMonitor SamplingRate="100" NS="urn:[NodeName]:BeckhoffAutomation:Ua:PLC1" NodeId="s=MAIN.nCounter2" />
    </Condition>
  </ConditionController>
</TcUaAcConfig>
```

A "condition" defines the runtime symbol to be monitored and the alarm limits and texts. Each condition is organized in a so-called "ConditionController", the object that the OPC UA Clients subsequently subscribe to.
When creating a condition, you must specify the NamespaceName (NS) and NodeID for referring to the UA node to be monitored. The standalone configurator provides a simple browsing mechanism for selecting a node. The configurator integrated in Visual Studio uses the target browser (Extension - OPC UA). In XML, the placeholder [NodeName] in NamespaceName can be used to switch the XML file between different hardware systems. NamespaceName always contains the host name of the IPC or Embedded PC on which the OPC UA Server is running. If [NodeName] is selected, this tag will be replaced by the host name of the current IPC or Embedded PC on which the UA Server is running.

SamplingRate determines how often the UA Server should request a value from the node to determine whether one of the alarm limits has been reached.

The alarm texts are identified by an ID. The ID uniquely identifies an alarm text from the resource file (see Step 5: Configuring multilingual alarm texts [99]).

**Step 3: Transferring own user data with an alarm**

Alarms can contain fields with their own user data, which complement the data output with the alarm. These user data fields can be created and filled out in the runtime application. To do this, create a STRUCT and name its first element "value". In case of an alarm, all the following elements are then sent in an additional user data field.

**Sample PLC application:**

```plaintext
TYPE ST_CustomStruct :
  STRUCT
    value : INT;
    data  : ST_SomeStruct;
  END_STRUCT
END_TYPE

TYPE ST_SomeStruct :
  STRUCT
    Data1 : INT;
    Data2 : REAL;
    Data3 : LREAL;
  END_STRUCT
END_TYPE
```

The instance of ST_CustomStruct is then enabled for data access via the regular mechanism, e.g. in TwinCAT 3: To do this the STRUCT must be activated as a `StructuredType` [73].

```plaintext
PROGRAM MAIN
VAR
    stCustomStruct : ST_CustomStruct;
END_VAR
```

When logging on to a ConditionController, the OPC UA Clients must subscribe to special AlarmConditionTypes, i.e. "BkUaLimitAlarmType" and "BkUaOffNormalAlarmType", so that they can receive the special user data fields when an alarm is received.
Technical introduction

The OPC UA Client then receives the user data in the fields BkUaEventData and BkUaEventValue of the incoming alarm. In the above sample, these are the value of the PLC variables and the user data represented by the PLC structure ST_SomeStruct.

**Step 4: Triggering an event using the FireEvent method**

Each ConditionController includes a FireEvent method with which the OPC UA Clients can trigger a general event with user-defined EventFields.
If the method is executed, an event is output on the OPC UA Server. Other OPC UA Clients can receive these events when they subscribe to the corresponding ConditionController.

The user-defined EventFields are appended to the event as "UserEventData". This data can be received by OPC UA Clients that are logged on to the SimpleEventType "UserEventType".
Technical introduction

Step 5: Configuring multilingual alarm texts

The A&C implementation in the OPC UA Server supports the use of multilingual alarm texts. The alarm text that is used depends on the language with which the UA Client connects to the Server.

Alarm texts are configured in XML files. There is a separate file for each language. These files are located in the res (Resource) folder on the OPC UA Server. With the configurator you can simply add or remove alarm texts without having to directly edit the XML files. Each alarm text has its own ID, which occurs only once in the file.

Sample:

```xml
<TcOpcUaSvrRes Lang="en">
  <Text ID="0">Text not available</Text>
  <Text ID="1">Some alarm text</Text>
  <Text ID="2">Value is High range</Text>
  <Text ID="3">Value is HighHigh range</Text>
  <Text ID="4">Value is OffNormal</Text>
  ...
</TcOpcUaSvrRes>
```

Step 6: Registering A&C with a reference OPC UA Client

An OPC UA Client must log on to a ConditionController so that it can receive events for conditions that are configured for this particular ConditionController. The UA Expert provides functions for subscribing to and receiving UA events.

After you have started the UA Expert and established a connection with the OPC UA Server, add a new document view, Event View, to your working area.
You can subscribe to a ConditionController by dragging the corresponding object in Event View. The events for this ConditionController are displayed in the Event Window.

<table>
<thead>
<tr>
<th>Events</th>
<th>Alarms</th>
<th>Event History</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>C</td>
<td>Time</td>
</tr>
<tr>
<td>⚠️</td>
<td>⚠️</td>
<td>11:41:54.553</td>
</tr>
<tr>
<td>⚠️</td>
<td>⚠️</td>
<td>11:58:04.415</td>
</tr>
<tr>
<td>⚠️</td>
<td>⚠️</td>
<td>11:41:54.553</td>
</tr>
<tr>
<td>⚠️</td>
<td>⚠️</td>
<td>11:58:04.415</td>
</tr>
<tr>
<td>⚠️</td>
<td>⚠️</td>
<td>12:44:09.875</td>
</tr>
<tr>
<td>⚠️</td>
<td>⚠️</td>
<td>11:41:54.553</td>
</tr>
<tr>
<td>⚠️</td>
<td>⚠️</td>
<td>12:44:09.875</td>
</tr>
</tbody>
</table>

It may be necessary to subscribe to special alarm and/or event types in order to receive all fields of an incoming event or alarm.

4.1.7 Method Call

4.1.7.1 PLC

Method calls are a fundamental part of the OPC UA specification. With the introduction of these functionalities into the PLC world, TwinCAT 3 offers the possibility of efficiently executing RPC calls in the IEC61131 world and thus reduces the classic handshake patterns for communication between devices. The OPC UA Server imports PLC methods such as OPC UA methods via its TMC import.

**IEC61131 method**

Although the PLC method appears to be a normal method in the UA namespace, it is still an IEC61131 method that runs within the real-time context and therefore falls under the context of a real-time task. The PLC developer must therefore take precautions so that the execution time of the method matches the task cycle time.

**Methods in IEC61131-3**

Methods in the IEC61131 world are always configured below a function block. At high-level language level, the function block can be regarded as the surrounding class of the method. You have to declare the method itself with a special PLC attribute so that the TwinCAT system knows that the method is to be activated for a remote method call.
Filtered or unfiltered mode

Depending on the import mode used, you also have to activate the surrounding function block for the OPC UA access. This can be done by using the normal PLC attributes for OPC UA access.

Note that you only need to use the PLC attributes if the filtered mode is used to enable symbols from the PLC to be accessed via OPC UA. This is the default setting of the OPC UA Server.

Sample:

The method M_Sum is located in the function block FB_Mathematics. The declaration of the function block instance uses the PLC attribute that has enabled the function block and thus the method for OPC UA access.

```plaintext
PROGRAM MAIN
VAR
{attribute 'OPC.UA.DA':='1'}
   fbMathematics : FB_Mathematics;
END_VAR
```

4.1.7.2 C++

Method calls are a fundamental part of the OPC UA specification. With the introduction of these functionalities into the PLC world, TwinCAT 3 offers the possibility of efficient execution of RPC calls in the C++ real-time context and thus reduces the classic handshake patterns for communication between devices. The OPC UA Server imports C++ methods such as OPC UA methods via its TMI import.

- **Real-time method**

  Although the C++ method appears to be a normal method in the UA namespace, it is still a real-time method that runs within the real-time context and therefore falls under the context of a real-time task. The TwinCAT C++ developer must therefore take precautions so that the execution time of the method matches the task cycle time.
Methods in TwinCAT 3 C++

TwinCAT modules could implement interfaces with predefined methods (see TcCOM modules). The method itself must be enabled for RPC calls during its definition (see TwinCAT Module Class Wizard documentation) so that the OPC UA Server knows that it is ready for execution.

So that the return value of the method is available, the corresponding option Include Return Value must be activated. Note that the interface under which the method was created must be implemented.
Filtered or unfiltered mode

Depending on the import mode used, you have to declare the method for the access via OPC UA. This can be done by using the TMC Code editor and the usual OPC UA attributes as optional properties.

---

4.1.8 File transfer

4.1.8.1 Access to files and folders via OPC UA

From OPC UA specification version 1.02, OPC UA contains a specialized ObjectType for file transfer, which is described in Appendix C of the specification. This special ObjectType called "FileType" describes the information model for the data transfer. Files can be modeled as simple variables in OPC UA with ByteStrings. FileType is a file with methods for accessing the file. The OPC UA specification provides further information about FileType and the structure and handling of the underlying methods and properties for accessing a file in the OPC UA namespace.

Beckhoff has implemented a generic way to load files and folders from a local hard disk into the OPC UA namespace. Each file is represented by a FileType and allows read and write operations for this file. In addition, each folder contains a CreateFile() method to create new files on the hard disk and a separate FolderPath to specify the actual path to the folder on the OPC UA Server.
Technical introduction

FileTransfer

TwinCAT

3.1

Boot

- CreateFile
- Current.cap
- CurrentConfig.tszip
- CurrentConfig.xml

FolderPath

Plc

- CreateFile
- FolderPath
- Port_851.app
- Port_851.autostart
- Port_851.bootdata-old
- Port_851.cid
- Port_851.crc
- Port_851.occ
- Port_851.tpy
- Port_851_act.tizip
- Port_851_boot.tizip

FileTransfer in the OPC UA Server Device Manager

Only the OPC UA Server of the Beckhoff Device Manager (IPC diagnostics) has this function. The TwinCAT OPC UA Server also provides some parts of this file transfer. However, the general function that enables disclosure of all files and folders is only available in the OPC UA Server, which is part of the device manager that is automatically available on every Beckhoff Industrial PC or Embedded PC. See the Device manager documentation for more information.

Configuration

FileType objects are created in a separate namespace called "FileTransfer". An XML file (files.xml) is used to configure this namespace and to select the files and folders available via OPC UA. The file must be located in the same directory as the executable file of the OPC UA Server. The system must be restarted in order to activate the configuration. The XML file contains information about the folder path and a search mask that defines which files are published in the OPC UA namespace:

```xml
<Files>
  <FolderObject DisplayName="TwinCAT">
    <FolderObject DisplayName="Boot" Path="c:/TwinCAT/3.1/Boot" Search="*.*"/>
    <FolderObject DisplayName="Plc" Path="c:/TwinCAT/3.1/Plc" Search="*.*"/>
    <FolderObject DisplayName="Tmi" Path="c:/TwinCAT/3.1/Tmi" Search="*.*"/>
  </FolderObject>
</Files>
```

Sample: Reading a file with UA Expert

General file handling is described in Appendix C of the OPC UA specification. Reading a file via UA can be divided into the following steps:

- Calling the Open method of a file. This method returns a file handle that must be saved for later access. The mode defines whether the file is read or written to (see File modes [105]).
• Determining the file size with the property "Size". In this way, the entire file can be read when the Read method is called.
• Calling the Read method. Inserting the file handle and file size as inputs. Selecting the destination folder in which the file contents are to be saved AFTER the method call.
• Calling the Close method to enable the file handle.

File modes

The following table shows all available file modes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Bit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>1</td>
<td>The file is opened for reading. If this bit is not set, Read cannot be executed.</td>
</tr>
<tr>
<td>Write</td>
<td>4</td>
<td>The file is opened for writing. If this bit is not set, Write cannot be executed.</td>
</tr>
<tr>
<td>EraseExisting</td>
<td>6</td>
<td>The existing file contents are deleted, and an empty file is made available.</td>
</tr>
<tr>
<td>Append</td>
<td>10</td>
<td>The file is opened and positioned at the end, otherwise it is moved to the beginning. This position can be changed with SetPosition.</td>
</tr>
</tbody>
</table>

4.1.9 Global Discovery Server

The TwinCAT OPC UA Server allows integration of the server application into a Global Discovery Server (GDS), so that it can issue certificates for the server and provide certificate revocation lists (CRL). Two models are supported, push and pull, which are explained in more detail below:

Push

In this model, the server includes a standardized interface that a GDS client can use to connect to a Global Discovery Server at the request of the server, register the server application there and request a server certificate, including the current CRL. The certificate is then activated on the server.

As a prerequisite for using this functionality, the GDS client must authenticate itself on the server with a user account that has administrator rights \( \text{IsRoot} = \text{true} \).

GDS Client

Any client that supports the push model can be used as a GDS Client. Various OPC UA toolkit manufacturers offer corresponding software packages. Alternatively, the OPC Foundation also provides a GDS Sample Client on Github.

GDS Server

In principle, any GDS can be used as a Global Discovery Server. Various OPC UA toolkit manufacturers offer corresponding software packages. Alternatively, the OPC Foundation also provides a GDS Sample Server on Github.
Pull

In this model, the server independently connects to the Global Discovery Server, registers there as a server application and obtains a matching server certificate.

Registration on the Global Discovery Server

In the first step, the TwinCAT OPC UA Server must be registered as an application at the GDS. This is done using the Register() method. By registering with the GDS, a server certificate is automatically requested for the server application. Depending on the implementation of the GDS application, such a certificate is issued either automatically or after manual approval by an administrator. The variables RegistrationState and CertificateState can be used to check whether the server has already been registered with a Global Discovery Server and has received a certificate from it. The variable CrlState indicates the status of the Certificate Revocation List and whether it could be obtained from the GDS.

The method expects the following input parameters:
**Technical introduction**

**Input parameter**  | **Meaning**  
---|---
GdsUrl | The URL of the Global Discovery Server in the format opc.tcp://hostnameOrIpAddress:port  
GdsUser | User name of a GDS user with the right to register new applications.  
GdsPassword | User password  
SaveCredentials | Saves the user password in a configuration file of the TwinCAT OPC UA Server. For security reasons, this setting is not recommended, since it was designed exclusively for Global Discovery Servers, which require user name/password authentication. However, this is usually only required once when registering the application. The issued server certificate is then used for all subsequent connections to the GDS.

---

**Re-initialization of the server endpoints**

After registering the server application with the Global Discovery Server and obtaining a server certificate, the server reinitializes its endpoints once, causing connected clients to momentarily lose connectivity.

After the server application has been registered with a Global Discovery Server, a new file named "TcUaGdsClientConfig.xml" is created in the installation directory of the TwinCAT OPC UA Server. It contains the connection information of the configured GDS and the registration information obtained from there, plus timestamp information for the server application, e.g., when the certificate and CRL were last updated.

**De-registration at the Global Discovery Server**

The Unregister() method can be used to de-register the TwinCAT OPC UA Server application at the GDS. Successful execution of the method causes the server application to be de-registered at the GDS and the contents of the file TcUaGdsClientConfig.xml to be deleted.

The method expects the following input parameters:
Technical introduction

Input parameter | Meaning
---|---
ForceRemove | If the connection to the Global Discovery Server is no longer available, the connection to the GDS can be removed by setting this input parameter. The TwinCAT OPC UA Server removes the GDS from its configuration.

The issued server certificate and the CRL remain valid after the TwinCAT OPC UA Server has been decoupled from the GDS. If you want to delete them and run the server with a self-signed certificate, you have to remove the corresponding files in the PKI directory of the server and restart the server. The server then creates another self-signed certificate.

Updating the server certificate

An update of the server certificate can be requested from the GDS outside the regular update interval by executing the method UpdateCertificate(). The method does not expect any further input parameters.

Setting the update intervals for server certificate and CRL

The update intervals for the server certificate and the certificate revocation list can be set by executing the SetUpdateStrategy() method.

The method expects the following input parameters:
## 4.1.10 Security

### 4.1.10.1 Overview

Security was a central requirement in the development of OPC UA. It is addressed in various areas:

- Encryption
- Integrity
- Authentication

The confidentiality of the exchanged information is secured by the encryption of the exchanged messages. Modern cryptographic algorithms are used for this. In order to be able to cope with future security requirements as well, even stronger and more modern algorithms can subsequently be added to an application without changing the protocol.

Different security levels can be selected according to the requirements of the respective application. In some areas it is sufficient to sign the messages in order to prevent changes being made by third parties, while additional encryption of the messages is necessary in other cases where the data must also not be read by third parties.

TF6100 OPC UA offers the following security levels (security endpoints) that clients can connect to:

- None: No security
- Sign: signed messages
- Sign & Encrypt: signed and encrypted messages

The signing of messages prevents a third party from changing the contents of a message. This prevents, for example, a write statement to open a switch being falsified by a third party and the switch being closed instead.

OPC UA applications identify themselves via so-called software and application instance certificates. With the aid of software certificates it is possible to grant certain client applications extended access to the information on an OPC UA Server, for example for the engineering of an OPC UA Server. Application instance certificates can be used to ensure that an OPC UA Server communicates only with preconfigured clients. A client can ensure by means of the server's application instance certificate that it is speaking to the correct server (similar to the certificates of a Web browser). The taking into account of these certificates is optional, i.e. an OPC UA server can also grant the same access to each client, depending on the user rights.

The TwinCAT OPC UA Client and TwinCAT OPC UA Server generate a self-signed certificate during the first startup process. This certificate consists of a private key and a public key. The private key is saved in the `\PKI\CA\private` directory and the corresponding public key in the `\PKI\CA\certs` directory. Any OPC UA Client wishing to establish a secure connection with the Server via one of the security endpoints (Sign, Sign&Encrypt) must know the public key of the OPC UA Server. Conversely the OPC UA Server must know the Client's public key. This so-called key exchange is described in the following sections:

- Authentication [►.109]
- Certificate exchange [►.110]
- Access rights [►.111]

### 4.1.10.2 Authentication

In addition to certificate exchange, the TwinCAT OPC UA Server offers the option of authentication via user name/password. An OPC UA Client must then use a valid user name/password combination for successful connection to the server.
The TwinCAT OPC UA Server uses mechanisms of the operating system for validating user names and passwords. If the computer on which the TwinCAT OPC UA Server is running is a member of a Windows domain (e.g. Active Directory), a request is made to the corresponding domain controller. If the computer is a single device, the local user database of the operating system is checked.

The configuration of the TwinCAT OPC UA Server allows two settings:

- Enable/Disable anonymous access (without user authentication)
- Enable/Disable user name/password validation

You can make both settings in the OPC UA Server Configurator.

When using the unencrypted end point in conjunction with authentication, the TwinCAT OPC UA Client requires the public certificate from the OPC UA Server to encrypt the password. To this end the certificate must be trusted in the TwinCAT OPC UA Client (see Certificate exchange [110]).

### 4.1.10.3 Certificate exchange

The communication between an OPC UA Client and an OPC UA Server can optionally be secured by communication with a secure endpoint. By default, both the TwinCAT OPC UA Server and the TwinCAT OPC UA Client generate a machine-specific, self-signed certificate for authentication the first time they are started.

If you want to use such an encrypted communication connection in your environment, you need to establish a trust relationship between OPC UA Server and OPC UA Client.

#### Trust settings on the server

If you want to authenticate one or more OPC UA Clients to the OPC UA Server via certificates, the OPC UA Server must trust the public keys of the clients. This can be done via the file system, for example. The server manages the trust settings for certificates via the file system.

- Trusted certificates: %InstallDir%\Server\PKI\CA\trusted\certs
- Rejected certificates: %InstallDir%\Server\PKI\CA\rejected\certs

By moving client certificates between these directories, the trust settings can be adjusted accordingly.

#### Reading a client certificate

A simple way of accessing the client certificate is described below. To do this, you establish a connection to the UA Server using a secure endpoint (for example, Basic128Rsa15/Sign&Encrypt) without first copying the client certificate to the UA Server. This connection is naturally rejected by the UA Server, since it does not trust the UA Client at this point in time. In this case, the TwinCAT OPC UA Client would return the error 0xE4DD0102, for example. However, after rejecting the connection request, the UA Server stores a copy of
the client certificate in the above-mentioned "Rejected" directory. The name of the certificate corresponds to the "Thumbprint" of the certificate and can thus be clearly assigned to the client certificate. You can now move this file directly to the above-mentioned "Trusted" directory so that the UA Server can trust the UA Client and accept the connection for all other connection requests.

**Announcing OPC UA Servers to the OPC UA Client**

Depending on the OPC UA Client employed, different steps may need to be taken so that the OPC UA Client trusts the OPC UA Server. Typically, for client applications with a graphical user interface, a warning message is displayed the first time you connect to the server, whereby the server certificate can then be classified as trustworthy.

The following instruction is therefore only valid for the TwinCAT OPC UA Client.

The public key of the OPC UA Server is located in the following directory as a DER file: \%InstallDir\%
\Server\PKI\CA\own\certs

In the case of the TwinCAT OPC UA Client, copy the file into the corresponding "Trusted" directory: \%InstallDir\%
\Client\PKI\CA\certs

### 4.1.10.4 Access rights

The TwinCAT OPC UA Server enables the configuration of permissions at namespace and node level. This allows you to fine-granulate the access to ADS devices (for example, to different PLC runtimes) as well as variables. These security settings are available for all ADS devices that can be displayed in the server namespace.

The following diagram illustrates the access rights for different user roles:

![Access Rights Diagram]

See also:

Configuration > Setup version 4.x.x. > Configuration of the security settings in the configurator [56].

**Requirements**

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>
4.1.11 Miscellaneous

4.1.11.1 Configuring firewalls

To make OPC UA communication also possible via a NAT device, e.g. an Internet router, this device must be able to forward the UA port used to the TwinCAT OPC UA Server (so-called "port forwarding"). By default the TwinCAT OPC UA Server is configured for UA communication via the TCP port 4840; however, you can adapt this configuration yourself if necessary, either via the server configuration file or using the OPC UA Configurator. The following figure illustrates the relationship between port forwarding and the UA Server.

In this example, the OPC UA Client establishes a UA connection to the NAT device via TCP port 4840, which then forwards this communication connection to the TwinCAT OPC UA Server via port forwarding. The NAT device thus only needs to forward the UA port configured in the TwinCAT OPC UA Server to the target device. The port used by the UA Server can either be viewed in the server configuration file or conveniently through the UA Configurator (in delivery state this is always TCP port 4840). For the appropriate configuration of your NAT device for port forwarding please refer to its documentation.

4.1.11.2 Namespace for configuration of the server

From server version 2.1.x the TwinCAT OPC UA Server provides a configuration namespace that contains the following functionalities:

- Management of the server configuration files
- Management of the certificates
Management of the server configuration files

The server configuration files are published in the namespace as a regular OPC UA FileType and therefore provide the methods and properties required to access the file.

Management of certificates

Each client certificate known to the server is published in the namespace as an OPC UA CertificateType. Certificates are divided into "rejected" and "trusted" certificates, which is represented by a separate folder in the namespace.

A certificate can be moved between the trust lists by calling the Move() method.

In addition, various properties provide additional information about the certificates themselves for easier identification.
Using the configuration namespace

The configuration namespace is enabled by default for ease of use and is available to users. This enables the TwinCAT OPC UA Configurator to connect to a server and apply the corresponding server configuration.

We recommend that you only make the namespace accessible to authenticated users once the server configuration is complete. This means that an OPC UA Client must authenticate itself vis-à-vis the OPC UA Server by providing a valid user name/password combination to access the namespace. Click [here](56) to find out how to do this.

4.1.11.3 DeviceState

Each namespace in the TwinCAT OPC UA Server contains a DeviceState object.

```
typedef enum
{
    UADEV_NOTINIT = 0x0100,
    UADEV_STARTING = 0x0110,
    UADEV_CONNECTED = 0x0120,
    UADEV_SHUTDOWN = 0x0130,
    UADEV_ERROR = 0xF000
} UaDeviceState;
```

If the device is in an ERROR state, the ErrorCode Property returns the following values:

```
#define UA_DEVSTATE_INVALID_STATE 0x80EB0010
#define UA_DEVSTATE_CREATE_NS_FAILED 0x80EB0011
#define UA_DEVSTATE_LOAD_NS_FAILED 0x80EB0012
#define UA_DEVSTATE_INVALID_IO_SETTING 0x80EB0100
```

A corresponding readable error message is then displayed in the ErrorMessage Property.

4.1.11.4 Default port and end points

The TwinCAT OPC UA Server makes various end points available for OPC UA Clients via the default port 4840/tcp. The end points define the connection type between client and server and whether it should be secured or unsecured.

- **Standard port**
  
  Note that the standard port 4840 may be used by other OPC UA Servers, such as the Local Discovery Server (LDS) from the OPC Foundation, which is used by some vendors with OPC UA software packages.

- **Safe end points**
  
  Please note that in order to use the secure end points, a trust relationship must be established between server and client, which is usually done via their certificates. The configuration of such a trust relationship on the server side is explained [here](110).
List of endpoints

The list provides an overview of the endpoints of the OPC UA Server. This includes endpoints that have already been discontinued. The following screenshot shows the endpoints currently contained in the OPC UA Server (version 3.2.0.62). The options are signing only or signing in combination with encryption.

From setup version 4.3.28 (server version 3.2.0.62) or higher, the unencrypted endpoint is disabled by default for security and certification reasons.

The available endpoints are based on the safety of the security mechanisms. If security profiles are classified as potentially unsafe over time, they are no longer used in the TwinCAT OPC UA Server by default and are replaced by newer and more secure encryption algorithms.

<table>
<thead>
<tr>
<th>Security profile</th>
<th>Security mode</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>This is the unencrypted endpoint, which can be used to communicate without security. Disabled by default since version 4.3.28. Can be reactivated if required by configuring the server accordingly.</td>
</tr>
<tr>
<td>Basic128Rsa15 (obsolete)</td>
<td>Sign / Sign &amp; Encrypt</td>
<td>This endpoint is considered obsolete from a security perspective and is disabled by default. Can be re-enabled if required by configuring the server accordingly.</td>
</tr>
<tr>
<td>Basic256 (obsolete)</td>
<td>Sign / Sign &amp; Encrypt</td>
<td>This endpoint is considered obsolete from a security perspective and is disabled by default. Can be re-enabled if required by configuring the server accordingly.</td>
</tr>
<tr>
<td>Basic256Sha256</td>
<td>Sign / Sign &amp; Encrypt</td>
<td>Endpoint currently present in the server for secure signing and encryption.</td>
</tr>
<tr>
<td>Aes256_Sha256_RsaPss</td>
<td>Sign / Sign &amp; Encrypt</td>
<td>Endpoint currently present in the server for secure signing and encryption.</td>
</tr>
<tr>
<td>Aes256_Sha256_RsaOaep</td>
<td>Sign / Sign &amp; Encrypt</td>
<td>Endpoint currently present in the server for secure signing and encryption.</td>
</tr>
</tbody>
</table>

All endpoints in the list can be enabled or disabled via the server configuration. In the following figure, all endpoints are enabled.
A flag (AllowDeprecatedSecurityPolicies) is available that enables the endpoints marked as obsolete in the table to be re-enabled.

### 4.2 Client I/O

#### 4.2.1 Overview

This function requires TwinCAT 3.1 Build 4022.4 or higher.

The TwinCAT OPC UA Client is also integrated as an I/O driver and is available as such in the TwinCAT I/O configuration. This not only shortens the engineering time required to establish the OPC UA connection to a remote server, it also enables the implementation of many application cases, such as the creation of protocol bridges that are simple to configure.

First of all, add a virtual device container to the configuration and then an OPC UA Client object.
After you have created the OPC UA I/O Client object, you can configure its connection to an OPC UA Target Server and add variables, methods and structures to the process image. The process of data exchange with a target server is reduced to a simple method of mapping process variables.

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

4.2.2 Quick start

The following instructions enable you to make a quick start with the OPC UA I/O Client. In the instructions a PLC project will be created that enables a variable via the OPC UA Server (for the simulation of a UA Server) and reads the enabled variable in again via the OPC UA I/O Client. This can of course be divided between two projects and two controllers.

Enabling variables for a server

For simulation, the OPC UA Server should be used in this quick start.

1. Create a new TwinCAT project and add a new PLC project to the project.
2. Create a new variable "nQuickStartOut" of data type INT in the PLC project. This should be the variable that is enabled via the OPC UA Server.
3. Set the OPC UA attribute [65] for this variable in order to be able to enable the variable via the OPC UA Server.
4. Activate the check box for the download of the TMC file.
5. Activate the configuration.
   - The variable is enabled for the server.

Configuring the I/O UA Client

1. In the same PLC project, create another variable "nQuickStartIn" of data type INT and define it as an input variable (AT%I*). This should be the variable that the OPC UA Client I/O device links to the server variable through mapping.
2. Compile the project so that the input variable is available in the PLC process image.
3. Add a new "Virtual OPC UA Device".
4. Add a new "OPC UA Client" to the device and open its settings.
5. Navigate to the **Settings** tab. Enter the server URL of the OPC UA Server. In this sample this is "opc.tcp://localhost:4840".
6. Click **Add Nodes**.
7. Navigate to the shared variable "nQuickStartOut" on the OPC UA Server (located under PLC1 > MAIN) and select it. The variable is now added to the process image of the "Virtual OPC UA Device".

8. Expand the newly added variable in the process image and double-click on **Input > Value**. Link the variable to the variable "nQuickStartIn" from the PLC process image.
9. Activate the configuration.
You should now find the configuration shown below. The two process image variables `nQuickStartIn` and `nQuickStartOut` are linked to each other.
10. After activating the configuration, log in to the PLC program.

You can also view the current value in the process image mapping.

11. You can use the settings on the OPC UA Client to modify parameters such as the sampling rate.

Requirements

<table>
<thead>
<tr>
<th>Products</th>
<th>Setup versions</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>TF6100</td>
<td>4.x.x</td>
<td>IPC or CX (x86, x64, ARM)</td>
</tr>
</tbody>
</table>

4.2.3 Supported data types

The OPC UA Client enables direct access to an OPC UA Server from a real-time logic. For the reading and writing of data, the data type of the OPC UA node must be assigned to the TwinCAT environment (mapping). This assignment is described below.

Basic data types

The assignment of the basic data types is described in PLCopen OPC UA Information Model for IEC 61131-3.
Technical introduction

<table>
<thead>
<tr>
<th>OPC UA data type</th>
<th>PLC data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>BOOL</td>
</tr>
<tr>
<td>SByte</td>
<td>SINT</td>
</tr>
<tr>
<td>Byte</td>
<td>USINT</td>
</tr>
<tr>
<td>Int16</td>
<td>INT</td>
</tr>
<tr>
<td>Int32</td>
<td>DINT</td>
</tr>
<tr>
<td>String</td>
<td>STRING</td>
</tr>
<tr>
<td>USInt</td>
<td>BYTE</td>
</tr>
<tr>
<td>Float</td>
<td>REAL</td>
</tr>
<tr>
<td>Double</td>
<td>LREAL</td>
</tr>
<tr>
<td>UInt16</td>
<td>UINT</td>
</tr>
<tr>
<td>UInt32</td>
<td>UDINT</td>
</tr>
<tr>
<td>Int64</td>
<td>LINT</td>
</tr>
<tr>
<td>UInt64</td>
<td>ULINT</td>
</tr>
<tr>
<td>DateTime</td>
<td>DT</td>
</tr>
</tbody>
</table>

You can use the mapping both on the OPC UA Client PLCopen function block and on the OPC UA I/O Client.

Derived data types

OPC UA defines basic data types. Other data types are derived from these.

On the client side, access to all UA data types is only possible with PLC data types. Data types derived from the basic data types are also supported from TcOpcUaClient version 2.1.0.36 or higher.

Currently supported non-base data types on the client side are:

- Counter (use UDINT in PLC)

In addition, the OPC UA I/O Client supports structured data types (StructuredTypes) if the structured data type does not incorporate any non-supported data type (e.g. in a member variable). The following list provides an overview of the data types that are not currently supported:

- ByteString
- NodeID
- LocalizedText (and thus AnalogItemType, DiscreteItemType)

4.2.4 Adding nodes of a Server

To add nodes of an OPC UA Target Server to the process image of the OPC UA I/O Client, you can use the namespace browser that is integrated in the I/O Client.

Open the Settings tab of the client configuration and click on the Add Nodes button to open the namespace browser.

The namespace browser dialog automatically establishes a connection with the Target Server by using the specified connection parameters.
Within the namespace browser you can activate and deactivate the check boxes in order to add nodes to the process image or remove them from it. Each selected node is shown in the process image as an input or output variable.

4.2.5 Node attributes

If you double-click on a node in the process image, you will see the UA attributes with their current values as they were at the time of opening the window.
Further variables that can be used for diagnostic purposes are added to the process image using the check box **Provide timestamp and status code variables**.

- **Int16 (OPC UA Variable)**
- **Inputs**
  - **TimeStamp**
  - **ErrorCode**
  - **Value**
- **Outputs**
  - **Value**

### 4.2.6 Method call

The OPC UA I/O Client supports the call of server methods. You can add a method to the process image like any other variable. The "input arguments" of the method are then available as output variables in the process image, whereas the "output arguments" are added as input variables. Additional input and output variables, e.g. bExecute, bBusy, bError, are added to the process image so that the method can be called.

**Sample: Method on the server**
You can then create a mapping between the input/output variables and the PLC variables.
Calling of a method

To call a method, set the output variable `bExecute` to TRUE. You can check whether the method call has been completed and whether it was successful via the input variables `nErrorID`, `bDone`, `bBusy` and `bError`.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>LREAL</td>
<td>3</td>
</tr>
<tr>
<td>b</td>
<td>LREAL</td>
<td>42</td>
</tr>
<tr>
<td>result</td>
<td>LREAL</td>
<td>126</td>
</tr>
<tr>
<td>bExecute</td>
<td>BOOL</td>
<td>TRUE</td>
</tr>
<tr>
<td>nErrorID</td>
<td>DINT</td>
<td>0</td>
</tr>
<tr>
<td>bDone</td>
<td>BOOL</td>
<td>TRUE</td>
</tr>
<tr>
<td>bError</td>
<td>BOOL</td>
<td>FALSE</td>
</tr>
<tr>
<td>bBusy</td>
<td>BOOL</td>
<td>FALSE</td>
</tr>
</tbody>
</table>
4.2.7 StructuredTypes

The OPC UA I/O Client supports read/write procedures with structured data types (StructuredTypes). You can also add StructuredTypes to the process image like any other variable. When adding a StructuredType to the process image, the type to be parsed is added to the TwinCAT type system so that, for example, it can simply be used by a PLC application.

Sample: StructuredType on the server

<table>
<thead>
<tr>
<th>Value</th>
<th>Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Fat Boy</td>
</tr>
<tr>
<td>Height</td>
<td>171</td>
</tr>
<tr>
<td>Weight</td>
<td>132.6</td>
</tr>
<tr>
<td>Gender</td>
<td>0 (Male)</td>
</tr>
</tbody>
</table>

Data Type: Person

NamespaceIndex: 2

Identifier Type: Numeric

Identifier: 543210

In this sample the server contains a node of the structured data type "Person", which contains various member variables (Name, Height, Weight, Gender).

Sample: StructuredTypes in the process image

I/O

Devices

Device 1 (OPC UA Virtual)

Image

Inputs

Outputs

Client #1

Inputs

Outputs

Demo (OPC UA Folder)

000_Static (OPC UA Folder)

Scalar (OPC UA Folder)

Structures (OPC UA Folder)

Person1 (OPC UA Variable)

Inputs

Value

Name

Height

Weight

Gender

Outputs

Value

Name

Height

Weight

Gender
After you have added a node to the process image, the process image contains the node and also the structural information of the type, e.g. whether individual member variables of the node should be read or written.

**StructuredTypes in the TwinCAT type system**

The data type is added to the TwinCAT type system. The "Value" tree items then have this data type.

![Variable Table]

You can also view the data type in the TwinCAT type system under SYSTEM > Type System.

![Data Types Table]

To distinguish the data type from other data types you can add a prefix in the settings of the OPC UA Client.

![Data Type Settings]

**Mapping a StructuredType**

Since every StructuredType is added to the TwinCAT type system, the mapping of the variables is simple. Create an input/output variable of this data type and subsequently a mapping.

GVL

```gvl
1 {attribute 'qualified_only'}
2 VAR_GLOBAL
3 Person1 AT*1* : Person;
4 END_VAR
```
Data recording

Data collection is configured on a per-device basis. The configuration can be opened by double-clicking on the OPC UA client device. The Process Data Configuration area shows various parameters for setting the different modes of data collection from a server.

The OPC UA client device offers three different modes for data collection. In addition to cyclical reading of data, this includes reading via a trigger variable and the use of subscriptions.
Cyclic read/write

One of the possible types of data collection is cyclic reading and writing. Time intervals are defined for both reading and writing. You can also specify how many variables are to be read in one read command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Cycle Time</td>
<td>Specifies how fast variables are cyclically read.</td>
</tr>
<tr>
<td>Write Cycle Time</td>
<td>Defines how often a write command is triggered on the OPC UA channel. If a variable value changes several times within a specific cycle time, only the last value is written to the OPC UA channel.</td>
</tr>
<tr>
<td>ReadList</td>
<td>Read commands on the OPC UA channel are bundled to save bandwidth. This parameter specifies how many variables are collected in a single read command on the OPC UA channel. The labeling behind it indicates how many read commands arise from the current configuration.</td>
</tr>
<tr>
<td>Array Single Write</td>
<td>On activation, every write process is executed as a single write command on the OPC UA channel.</td>
</tr>
</tbody>
</table>

**Read and write via trigger variables**

In addition, there is an option to trigger reading and writing via trigger variables. For each OPC UA client device there is a trigger variable (it can be found under Outputs/Control/Execute) that can be connected to a variable from the PLC and set if required. This option is suitable, for example, if data is only to be read from an OPC UA Server when a certain event occurs in the PLC. If the trigger variable remains permanently set, the data collection type behaves in the same way as the cyclic configuration.

**Reading and writing using subscriptions**

The third and last way of data collection is to use subscriptions. The I/O client registers a subscription with the connected OPC UA server. The parameters described below can be specified for Publish Interval, Lifetime Count and Keepalive Count.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish Interval</td>
<td>After the specified time the connected OPC UA Server checks where there are new notification packets for the Client. If several value changes occur in a publishing interval, only the last value is transferred.</td>
</tr>
<tr>
<td>Lifetime Count</td>
<td>The OPC UA Client is responsible for sending a PublishRequest to the server. In the PublishResponse, the server returns the respective notification packages. The Lifetime Count indicates after how many failed PublishRequests from the client the server deletes the subscription. The calculated duration is shown in brackets (in the sample 1200 multiplied by 1000 ms = 20 minutes).</td>
</tr>
<tr>
<td>Keepalive Count</td>
<td>If the server does not have new notification packets for the client, it will not return any data. The Keepalive Count indicates after how many missed messages the server would send an empty message to the client to indicate that it is still active and the subscription is still in place.</td>
</tr>
</tbody>
</table>

### 4.2.9 Writing variables

To enable the writing of variables, several conditions must be met:

1. The flag "Enable Write" must be set for the variable. This can be done either during the adding process via the button **Add Nodes** or afterwards in the parameter settings of the variable.
2. Before a write command, the "Write Enable" output for the I/O client must be enabled globally. Only then are the write commands generated.

#### Setting Enable Write for a variable

In order to add not only an input (Read) but also an output (Write) element for a variable in the process image, it must be enabled explicitly. This can be done by using the **Add Nodes** dialog while adding the variables, for example:

![Select Nodes](image)

Alternatively, this setting can be enabled/disabled at a later stage via the configuration parameters of the variables in the process image.
Enabling write access globally

Before write commands can be sent, they must be enabled globally. This is done by setting the output variable "Write Enable" for the I/O client:

![Image of I/O configuration]

### 4.2.10 Security

#### 4.2.10.1 Overview

Security was a central requirement in the development of OPC UA. It is addressed in various areas:

- Encryption
- Integrity
• Authentication

The confidentiality of the exchanged information is secured by the encryption of the exchanged messages. Modern cryptographic algorithms are used for this. In order to be able to cope with future security requirements as well, even stronger and more modern algorithms can subsequently be added to an application without changing the protocol.

Different security levels can be selected according to the requirements of the respective application. In some areas it is sufficient to sign the messages in order to prevent changes being made by third parties, while additional encryption of the messages is necessary in other cases where the data must also not be read by third parties.

TF6100 OPC UA offers the following security levels (security endpoints) that clients can connect to:

• None: No security
• Sign: signed messages
• Sign & Encrypt: signed and encrypted messages

The signing of messages prevents a third party from changing the contents of a message. This prevents, for example, a write statement to open a switch being falsified by a third party and the switch being closed instead.

OPC UA applications identify themselves via so-called software and application instance certificates. With the aid of software certificates it is possible to grant certain client applications extended access to the information on an OPC UA Server, for example for the engineering of an OPC UA Server. Application instance certificates can be used to ensure that an OPC UA Server communicates only with preconfigured clients. A client can ensure by means of the server’s application instance certificate that it is speaking to the correct server (similar to the certificates of a Web browser). The taking into account of these certificates is optional, i.e. an OPC UA server can also grant the same access to each client, depending on the user rights.

The TwinCAT OPC UA Client and TwinCAT OPC UA Server generate a self-signed certificate during the first startup process. This certificate consists of a private key and a public key. The private key is saved in the \PKI\CA\private directory and the corresponding public key in the \PKI\CA\certs directory. Any OPC UA Client wishing to establish a secure connection with the Server via one of the security endpoints (Sign, Sign&Encrypt) must know the public key of the OPC UA Server. Conversely the OPC UA Server must know the Client’s public key. This so-called key exchange is described in the following sections:

• Authentication [109]
• Certificate exchange [132]
• Access rights [111]

### 4.2.10.2 Certificate exchange

The communication between an OPC UA Client and an OPC UA Server can optionally be secured by communication with a secure endpoint. By default, both the TwinCAT OPC UA Server and the TwinCAT OPC UA Client generate a machine-specific, self-signed certificate for authentication the first time they are started.

If you want to use such an encrypted communication connection in your environment, you need to establish a trust relationship between OPC UA Server and OPC UA Client.
Trust settings on the server

If you want to authenticate one or more OPC UA Clients to the OPC UA Server via certificates, the
OPC UA Server must trust the public keys of the clients. This can be done via the file system, for example.
The server manages the trust settings for certificates via the file system.

- Trusted certificates: %InstallDir%/Server\PKI\CA\trusted\certs
- Rejected certificates: %InstallDir%/Server\PKI\CA\rejected\certs

By moving client certificates between these directories, the trust settings can be adjusted accordingly.

Reading a client certificate

A simple way of accessing the client certificate is described below. To do this, you establish a connection to
the UA Server using a secure endpoint (for example, Basic128Rsa15/Sign&Encrypt) without first copying the
client certificate to the UA Server. This connection is naturally rejected by the UA Server, since it does not
trust the UA Client at this point in time. In this case, the TwinCAT OPC UA Client would return the error
0xE4DD0102, for example. However, after rejecting the connection request, the UA Server stores a copy of
the client certificate in the above-mentioned "Rejected" directory. The name of the certificate corresponds to
the "Thumbprint" of the certificate and can thus be clearly assigned to the client certificate. You can now
move this file directly to the above-mentioned "Trusted" directory so that the UA Server can trust the
UA Client and accept the connection for all other connection requests.

Announcing OPC UA Servers to the OPC UA Client

Depending on the OPC UA Client employed, different steps may need to be taken so that the OPC UA Client
trusts the OPC UA Server. Typically, for client applications with a graphical user interface, a warning
message is displayed the first time you connect to the server, whereby the server certificate can then be
classified as trustworthy.

The following instruction is therefore only valid for the TwinCAT OPC UA Client.

The public key of the OPC UA Server is located in the following directory as a DER file: %InstallDir%
\Server\PKI\CA\own\certs

In the case of the TwinCAT OPC UA Client, copy the file into the corresponding "Trusted" directory:
%InstallDir%/Client\PKI\CA\certs
## 4.3 Client PLCopen

### 4.3.1 Overview

The TwinCAT OPC UA Client offers several options for communicating directly with one or more OPC UA Servers from the control logic. On the one hand, an OPC UA interface is available directly from the PLC, in which a connection to an OPC UA Server can be initiated via PLCopen standardized function blocks. On the other there is an OPC UA Client I/O device that offers a simple mapping-based interface.

**PLC function blocks**

The following table provides an overview of the functionalities offered:

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Description</th>
<th>Relevant function blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect/Disconnect</td>
<td>Establishment and disconnection of connections to OPC UA Servers.</td>
<td>UA_Connect, UA_Disconnect</td>
</tr>
<tr>
<td>Polling (Read/Write)</td>
<td>Reading and writing of variables in the UA namespace in the polling mode.</td>
<td>UA_Connect, UA_Disconnect, UA_Read, UA_Write, UA_GetNamespaceIndex, UA_NodeGetHandle, UA_NodeReleaseHandle</td>
</tr>
<tr>
<td>Method Call</td>
<td>Execution of methods in the UA namespace.</td>
<td>UA_Connect, UA_Disconnect, UA_MethodGetHandle, UA_MethodReleaseHandle, UA_MethodCall</td>
</tr>
<tr>
<td>Security</td>
<td>Establishment of an encrypted connection to an OPC UA Server.</td>
<td>UA_Connect, UA_Disconnect</td>
</tr>
</tbody>
</table>

The interfaces of each function block are described in the section [PLC API](#).

**I/O device**

Further information on the TwinCAT OPC UA Client I/O device can be found in the section I/O > Quick start [117].

### 4.3.2 Supported data types

The OPC UA Client enables direct access to OPC UA Servers from the real-time logic. To read and write data, the data types must be assigned to both environments (mapping). This assignment is described below.

**Basic data types**

The assignment of the basic data types is described in PLCopen OPC UA Information Model for IEC 61131-3.
<table>
<thead>
<tr>
<th>OPC UA data type</th>
<th>PLC data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>BOOL</td>
</tr>
<tr>
<td>SByte</td>
<td>SINT</td>
</tr>
<tr>
<td>Byte</td>
<td>USINT</td>
</tr>
<tr>
<td>Int16</td>
<td>INT</td>
</tr>
<tr>
<td>Int32</td>
<td>DINT</td>
</tr>
<tr>
<td>String</td>
<td>STRING</td>
</tr>
<tr>
<td>USInt</td>
<td>BYTE</td>
</tr>
<tr>
<td>Float</td>
<td>REAL</td>
</tr>
<tr>
<td>Double</td>
<td>LREAL</td>
</tr>
<tr>
<td>UInt16</td>
<td>UINT</td>
</tr>
<tr>
<td>UInt32</td>
<td>UDINT</td>
</tr>
<tr>
<td>Int64</td>
<td>LINT</td>
</tr>
<tr>
<td>UInt64</td>
<td>ULINT</td>
</tr>
<tr>
<td>DateTime</td>
<td>DT</td>
</tr>
</tbody>
</table>

**Derived data types**

OPC UA defines basic data types. Other data types are derived from these.

On the client side, access to all UA data types is only possible with PLC data types. Data types derived from the basic data types are also supported from TcOpcUaClient version 2.1.0.36 or higher.

Currently supported non-base data types on the client side are:

- Counter (use UDINT in PLC)

**Access to arrays**

When creating a node handle, the system checks the possibilities to access the node. Further checks are performed during reading and writing.

To access array nodes and input and output parameters of method calls, certain conditions must be fulfilled.

- For accessing nodes: The array dimension and data length must match the data provided when reading and writing.
- Reading strings: If just one string exceeds the specified length for PLC strings, the read process fails.
- Only array dimensions up to three levels are supported.

**4.3.3 Best practice**

**4.3.3.1 How to determine communication parameters**

In general a graphic OPC UA Client is used to determine the attributes of a node or methods that have to be used together with the PLC function blocks, e.g.:

- Node Identifier [136]
- Node namespace index and corresponding namespace URI [136]
- Node Data Type [137]
- Node ID and Object Node ID methods [138]

The following documentation uses the generic OPC UA Client UA Expert as an example. This client can be purchased from the Unified Automation website: www.unified-automation.com.
Technical introduction

**Node Identifier**

A general task consists of reading or writing variables that are generally referred to as nodes in the context of OPC UA.

Nodes can be marked with the following three attributes:

- **NamespaceIndex**: Namespace in which the node is located, e.g. the PLC runtime
- **Identifier**: Unique identifier of the node within its namespace
- **IdentifierType**: Type of node: String, Guid and Numeric

These attributes represent the so-called NodeID – the representation of a node on an OPC UA Server – and are required by some function blocks.

With the help of UA Expert you can simply determine the attributes of a node by establishing a connection to the OPC UA Server and browsing to the desired node. The attributes are then visible in the Attributes panel.

**Sample:**

<table>
<thead>
<tr>
<th>NodeId</th>
<th>NodeId</th>
</tr>
</thead>
<tbody>
<tr>
<td>NamespaceIndex</td>
<td>5</td>
</tr>
<tr>
<td>IdentifierType</td>
<td>String</td>
</tr>
<tr>
<td>Identifier</td>
<td>MAIN.nCounter</td>
</tr>
</tbody>
</table>

**Node NamespaceIndex and corresponding NamespaceURI**

According to the OPC UA specification, the namespace index (as shown above) can be a dynamically generated value. Therefore, OPC UA Clients must always use the corresponding namespace URI to resolve the NamespaceIndex before a node handle is detected.

Use the UA_GetNamespaceIndex [182] function block to obtain the NamespaceIndex for a NamespaceURI. The NamespaceURI required for this can be determined with the help of UA Expert by establishing a connection to the OPC UA Server and browsing to the NamespaceArray node.

**Sample:**

This node contains information about all namespaces registered on the OPC UA Server. The corresponding NamespaceURIs are visible in the Attributes panel.
A NodeID in which the NamespaceIndex is 5 is shown in the sample in the section Node Identifier [136]. According to the NamespaceArray shown in the figure, the corresponding NamespaceURI is urn://SVENG-NB04/BeckhoffAutomation/Ua/PLC1. This URI can now be used for the function block UA_GetNamespaceIndex. The OPC UA Server ensures that the URI always remains the same, even after a restart. As the NamespaceIndex shown can change, however, the NamespaceURI should always be used in combination with the UA_GetNamespaceIndex function block for later use with other function blocks, e.g. UA_Read [190], UA_Write [192], to resolve the correct NamespaceIndex.

**Node DataType**

The data type of a node is required in order to see which PLC data type needs to be used in order to assign a read value or write it to a node. With the help of UA Expert you can simply determine the data type of a node by establishing a connection to the OPC UA Server and browsing to the desired node. The data type is then visible in the Attributes panel.

**Sample:**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SourceTimestamp</td>
<td>16.02.2015 08:56:06.350</td>
</tr>
<tr>
<td>ServerTimestamp</td>
<td>16.02.2015 09:31:01.945</td>
</tr>
<tr>
<td>SourcePicoseconds</td>
<td>0</td>
</tr>
<tr>
<td>ServerPicoseconds</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sample</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><a href="http://opcfoundation.org/UA/">http://opcfoundation.org/UA/</a></td>
</tr>
<tr>
<td>1</td>
<td>urn://SVENG-NB04/BeckhoffAutomation/UaServer:1</td>
</tr>
<tr>
<td>2</td>
<td><a href="http://opcfoundation.org/Ua/DA/">http://opcfoundation.org/Ua/DA/</a></td>
</tr>
<tr>
<td>3</td>
<td><a href="http://PLCopen.org/OpcUa/IEC61131-3/">http://PLCopen.org/OpcUa/IEC61131-3/</a></td>
</tr>
<tr>
<td>4</td>
<td>urn://SVENG-NB04/BeckhoffAutomation/Ua/Typesystem</td>
</tr>
<tr>
<td>5</td>
<td>urn://SVENG-NB04/BeckhoffAutomation/Ua/PLC1</td>
</tr>
<tr>
<td>6</td>
<td>urn://SVENG-NB04/BeckhoffAutomation/Ua/PLC2</td>
</tr>
<tr>
<td>7</td>
<td><a href="http://www.opcfoundation.org/Energy/DataAcquisition/">http://www.opcfoundation.org/Energy/DataAcquisition/</a></td>
</tr>
</tbody>
</table>

In this case the data type (DataType) is "Int16". This must be assigned to an equivalent data type in the PLC, e.g. "INT".

The PLCopen IEC61131 - to - OPC UA specification describes the defined data type mapping. The following table is an excerpt from this specification:
<table>
<thead>
<tr>
<th>IEC61131 elementary data types</th>
<th>OPC UA built-in data types</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOL</td>
<td>Boolean</td>
</tr>
<tr>
<td>SINT</td>
<td>SByte</td>
</tr>
<tr>
<td>USINT</td>
<td>Byte</td>
</tr>
<tr>
<td>INT</td>
<td>Int16</td>
</tr>
<tr>
<td>UINT</td>
<td>UInt16</td>
</tr>
<tr>
<td>DINT</td>
<td>Int32</td>
</tr>
<tr>
<td>UDINT</td>
<td>UInt32</td>
</tr>
<tr>
<td>LINT</td>
<td>Int64</td>
</tr>
<tr>
<td>UUINT</td>
<td>UInt64</td>
</tr>
<tr>
<td>BYTE</td>
<td>Byte</td>
</tr>
<tr>
<td>WORD</td>
<td>UInt16</td>
</tr>
<tr>
<td>DWORD</td>
<td>UInt32</td>
</tr>
<tr>
<td>LWORD</td>
<td>UInt64</td>
</tr>
<tr>
<td>REAL</td>
<td>Float</td>
</tr>
<tr>
<td>LREAL</td>
<td>Double</td>
</tr>
<tr>
<td>STRING</td>
<td>String</td>
</tr>
<tr>
<td>CHAR</td>
<td>Byte</td>
</tr>
<tr>
<td>WSTRING</td>
<td>String</td>
</tr>
<tr>
<td>WCHAR</td>
<td>UInt16</td>
</tr>
<tr>
<td>DT</td>
<td>DateTime</td>
</tr>
<tr>
<td>DATE_AND_TIME</td>
<td>DateTime</td>
</tr>
<tr>
<td>DATE</td>
<td>DateTime</td>
</tr>
<tr>
<td>TOD</td>
<td>DateTime</td>
</tr>
<tr>
<td>TIME_OF_DAY</td>
<td>DateTime</td>
</tr>
<tr>
<td>TIME</td>
<td>Double</td>
</tr>
</tbody>
</table>

**Method NodeID and Object NodeID**

When calling methods from the OPC UA namespace, two identifiers are required if the method handle is captured using the function block `UA_MethodGetHandle`:

- **ObjectNodeID**: Identifies the UA object that contains the method
- **MethodNodeID**: Identifies the method itself

With the help of UA Expert you can simply determine both NodeIDs by establishing a connection to the OPC UA Server and browsing to the desired method or the desired UA object that contains the method.

**Sample – M_Mul method:**

| ![Image of diagram] |

The method identifier is then visible in the Attributes panel.
Sample – fbMathematics object:

The object identifier is then visible in the Attributes panel.

Overview

The following function blocks are required to establish a connection to an OPC UA Server and to interrupt the session later: UA_Connect [180], UA_Disconnect [181].

First read the section How to determine communication parameters [135] to better understand certain UA functionalities (e.g. how to determine node identifiers).

Schematic workflow

The schematic workflow of each TwinCAT OPC UA Client can be categorized into three different phases: Preparation, Work and Cleanup.

The use case described in this section can be visualized as follows:
General notes

The UA_Connect function block requires the following information in order to be able to establish a connection to a local or remote OPC UA Server:

- Server URL
- Session Connect Information

The server URL basically consists of a prefix, a hostname and a port. The prefix describes the OPC UA transport protocol that should be used for the connection, e.g. "opc.tcp://" for a binary TCP connection (default). The host name or IP address part describes the address information of the OPC UA target server, e.g. "192.168.1.1" or "CX-12345". The port number is the target port of the OPC UA Server, e.g. "4840". Overall the server URL may then look like this: opc.tcp://CX-12345:4840.

Code snippet

Declaration:

```c
/* Declarations for UA_Connect */
fbUA_Connect : UA_Connect;
SessionConnectInfo : ST_UASessionConnectInfo;
nConnectionHdl : DWORD;

/* Declarations for UA_Disconnect */
fbUA_Disconnect : UA_Disconnect;

/* Declarations for state machine and output handling */
iState : INT;
bDone : BOOL;
bBusy : BOOL;
bError : BOOL;
nErrorID : DWORD;
```

Implementation:

```c
CASE iState OF
  0:
    bError := FALSE;
    nErrorID := 0;
    SessionConnectInfo.tConnectTimeout := T#1M;
    SessionConnectInfo.tSessionTimeout := T#1M;
    SessionConnectInfo.sApplicationName := '';
    SessionConnectInfo.sApplicationUri := '';
    SessionConnectInfo.eSecurityMode := eUASecurityMsgMode_None;
    SessionConnectInfo.eSecurityPolicyUri := eUASecurityPolicy_None;
    SessionConnectInfo.eTransportProfileUri := eUATransportProfileUri_UATcp;
    stNodeAddInfo nIndexRangeCount := nIndexRangeCount;
    stNodeAddInfo.stIndexRange := stIndexRange;
    iState := iState + 1;
  1:
    fbUA_Connect(
        Execute := TRUE,
        ServerURL := 'opc.tcp://192.168.1.1:4840',
        SessionConnectInfo := SessionConnectInfo,
        Timeout := T#5S,
        ConnectionHdl := nConnectionHdl);
    IF NOT fbUA_Connect.Busy THEN
      fbUA_Connect(Execute := FALSE);
      IF NOT fbUA_Connect.Error THEN
        iState := iState + 1;
      ELSE
        bError := TRUE;
        nErrorID := fbUA_Connect.ErrorCode;
    ELSE
```

Version: 2.11  TF6100
4.3.3.3 How to read nodes

The following section describes how you use the TcX_PLCopen_OpcUa function block to read out an OPC UA node from a local or remote OPC UA Server.

This section contains the following topics:

- **Overview** [141]
- **Schematic workflow** [141]
- **General notes** [142]
- **Code snippet** [142]

**Overview**

The following function blocks are required to establish a connection to an OPC UA Server, to read UA nodes and to interrupt the session later: **UA_Connect** [180], **UA_GetNamespaceIndex** [182], **UA_NodeGetHandle** [186], **UA_Read** [190], **UA_NodeReleaseHandle** [188], **UA_Disconnect** [181].

First of all, read the section **How to determine communication parameters** [135] so as to be able to understand certain UA functions better (e.g. how NodeIdentifiers can be determined) as well as the section **How to establish a connection** [139].

**Schematic workflow**

The schematic workflow of each TwinCAT OPC UA Client can be categorized into three different phases: Preparation, Work and Cleanup.

The use case described in this section can be visualized as follows:
General notes

- The UA_Connect function block requires the following information to establish a connection to a local or remote OPC UA Server (see also How to establish a connection [139]):
  - Server URL
  - Session Connect Information

- The UA_GetNamespaceIndex function block requires a connection handle (from UA_Connect) and a NamespaceURI for resolution in a NamespaceIndex, which will be used later by UA_NodeGetHandle to obtain a node handle (see also How to determine communication parameters [135]).

- The UA_NodeGetHandle function block requires a connection handle (from UA_Connect) and the NodeID (from a ST_UANodeID) in order to obtain a node handle (see also How to determine communication parameters [135]).

- The UA_Read function block requires a connection handle (from UA_Connect), a node handle (from UA_NodeGetHandle) and a pointer to the target variable (where the read value is to be saved). Make sure that the target variable has the correct data type (see How to determine communication parameters [135]).

- The UA_NodeReleaseHandle function block requires a connection handle (from UA_Connect) and a node handle (from UA_NodeGetHandle).

Code snippet

Declaration:

```plaintext
(* Declarations for UA_GetNamespaceIndex *)
fbUA_GetNamespaceIndex : UA_GetNamespaceIndex;
nNamespaceIndex : UINT;

(* Declarations for UA_NodeGetHandle *)
fbUA_NodeGetHandle : UA_NodeGetHandle;
NodeID : ST_UANodeID;
nNodeHdl : DWORD;

(* Declarations for UA_Read *)
fbUA_Read : UA_Read;
stIndexRange : ARRAY [1..nMaxIndexRange] OF ST_UAIndexRange;
nIndexRangeCount : UINT;
stNodeAddInfo : ST_UANodeAdditionalInfo;
sNodeIdentifier : STRING(MAX_STRING_LENGTH) := 'MAIN.nCounter';
nReadData : INT;
cbDataRead : UDINT;

(* Declarations for UA_NodeReleaseHandle *)
fbUA_NodeReleaseHandle : UA_NodeReleaseHandle;
```

Implementation:

```plaintext
CASE iState OF
  0: [...]
  2: (* GetNS Index *)
```
func fbUA_GetNamespaceIndex(
    Execute := TRUE,
    ConnectionHdl := nConnectionHdl,
    NamespaceUri := sNamespaceUri,
    NamespaceIndex := nNamespaceIndex
); IF NOT fbUA_GetNamespaceIndex.Busy THEN fbUA_GetNamespaceIndex(Execute := FALSE); IF NOT fbUA_GetNamespaceIndex.Error THEN
    iState := iState + 1;
ELSE
    bError := TRUE;
    nErrorID := fbUA_GetNamespaceIndex.ErrorID;
    iState := 6;
END_IF END_IF
3: (* UA_NodeGetHandle *)
    NodeID.eIdentifierType := eUAIdentifierType_String;
    NodeID.nNamespaceIndex := nNamespaceIndex;
    NodeID.sIdentifier := sNodeIdentifier;
    fbUA_NodeGetHandle(
        Execute := TRUE,
        ConnectionHdl := nConnectionHdl,
        NodeID := NodeID,
        NodeHdl := nNodeHdl);
IF NOT fbUA_NodeGetHandle.Busy THEN fbUA_NodeGetHandle(Execute := FALSE);
IF NOT fbUA_NodeGetHandle.Error THEN
    iState := iState + 1;
ELSE
    bError := TRUE;
    nErrorID := fbUA_NodeGetHandle.ErrorID;
    iState := 6;
END_IF END_IF
4: (* UA_Read *)
    fbUA_Read(
        Execute := TRUE,
        ConnectionHdl := nConnectionHdl,
        NodeHdl := nNodeHdl,
        cbData := SIZEOF(nReadData),
        stNodeAddInfo := stNodeAddInfo,
        pVariable := ADR(nReadData));
IF NOT fbUA_Read.Busy THEN fbUA_Read( Execute := FALSE, cbData_R => cbDataRead);
IF NOT fbUA_Read.Error THEN
    iState := iState + 1;
ELSE
    bError := TRUE;
    nErrorID := fbUA_Read.ErrorID;
    iState := 6;
END_IF END_IF
5: (* Release Node Handle *)
    fbUA_NodeReleaseHandle(
        Execute := TRUE,
        ConnectionHdl := nConnectionHdl,
        NodeHdl := nNodeHdl);
IF NOT fbUA_NodeReleaseHandle.Busy THEN fbUA_NodeReleaseHandle(Execute := FALSE);
IF NOT fbUA_NodeReleaseHandle.Error THEN
    iState := iState + 1;
ELSE
    bError := TRUE;
    nErrorID := fbUA_NodeReleaseHandle.ErrorID;
    iState := 6;
END_IF END_IF
6: [...] END_CASE
4.3.3.4 How to write nodes

The following section describes how you use the TcX_PLCopen_OpcUa function block to write values in an OPC UA node from a local or remote OPC UA Server.

This section contains the following topics:

- **Overview** [144]
- **Schematic workflow** [144]
- **General notes** [144]
- **Code snippet** [145]

**Overview**

The following function blocks are required to establish a connection to an OPC UA Server, write UA nodes and subsequently interrupt the session: `UA_Connect` [180], `UA_GetNamespaceIndex` [182], `UA_NodeGetHandle` [186], `UA_Write` [192], `UA_NodeReleaseHandle` [188], `UA_Disconnect` [181].

First of all, read the section *How to determine communication parameters* [135] so as to be able to understand certain UA functions better (e.g. how NodeIdentifiers can be determined) as well as the section *How to establish a connection* [139].

**Schematic workflow**

The schematic workflow of each TwinCAT OPC UA Client can be categorized into three different phases: Preparation, Work and Cleanup.

The use case described in this section can be visualized as follows:

**General notes**

- The `UA_Connect` function block requires the following information to establish a connection to a local or remote OPC UA Server (see also *How to establish a connection* [139]):
  - Server URL
  - Session Connect Information
- The `UA_GetNamespaceIndex` function block requires a connection handle (from `UA_Connect`) and a NamespaceURI for resolution in a NamespaceIndex, which will be used later by `UA_NodeGetHandle` to obtain a node handle (see also *How to determine communication parameters* [135]).
- The `UA_NodeGetHandle` function block requires a connection handle (from `UA_Connect`) and the NodeID (from a ST_UANodeID) in order to obtain a node handle (see also *How to determine communication parameters* [135]).
• The UA_Write function block requires a connection handle (from UA_Connect), a node handle (from UA_NodeGetHandle) and a pointer to a variable containing the value that is to be written. Make sure that the target variable has the correct data type (see How to determine communication parameters [135]).

• The UA_NodeReleaseHandle function block requires a connection handle (from UA_Connect) and a node handle (from UA_NodeGetHandle).

**Code snippet**

**Declaration:**

```c
(* Declarations for UA_GetNamespaceIndex *)
fbUA_GetNamespaceIndex : UA_GetNamespaceIndex;
nNamespaceIndex : UINT;

(* Declarations for UA_NodeGetHandle *)
fbUA_NodeGetHandle : UA_NodeGetHandle;
NodeID : ST_UANodeID;
nNodeHdl : DWORD;

(* Declarations for UA_Write *)
fbUA_Write : UA_Write;
stIndexRange : ARRAY [1..nMaxIndexRange] OF ST_UAIndexRange;
nIndexRangeCount : UINT;
stNodeAddInfo : ST_UANodeAdditionalInfo;
sNodeIdentifier: STRING(MAX_STRING_LENGTH) := 'MAIN.nNumber';
nWriteData: INT := 42;

(* Declarations for UA_NodeReleaseHandle *)
fbUA_NodeReleaseHandle : UA_NodeReleaseHandle;
```

**Implementation:**

```c
CASE iState OF
  0: [...] 
  2: (* GetNS Index *)
      fbUA_GetNamespaceIndex(
        Execute := TRUE,
        ConnectionHdl := nConnectionHdl,
        NamespaceUri := sNamespaceUri,
        NamespaceIndex => nNamespaceIndex
      );
      IF NOT fbUA_GetNamespaceIndex.Busy THEN
        fbUA_GetNamespaceIndex(Execute := FALSE);
        IF NOT fbUA_GetNamespaceIndex.Error THEN
          iState := iState + 1;
        ELSE
          bError := TRUE;
          nErrorID := fbUA_GetNamespaceIndex.ErrorID;
          iState := 6;
        END_IF
      END_IF
  3: (* UA_NodeGetHandle *)
      NodeID.eIdentifierType := eUAIdentifierType_String;
      NodeID.nNamespaceIndex := nNamespaceIndex;
      NodeID.sIdentifier := sNodeIdentifier;
      fbUA_NodeGetHandle(
        Execute := TRUE,
        ConnectionHdl := nConnectionHdl,
        NodeID := NodeID,
        NodeHdl => nNodeHdl);
      IF NOT fbUA_NodeGetHandle.Busy THEN
        fbUA_NodeGetHandle(Execute := FALSE);
        IF NOT fbUA_NodeGetHandle.Error THEN
          iState := iState + 1;
        ELSE
          bError := TRUE;
          nErrorID := fbUA_NodeGetHandle.ErrorID;
          iState := 6;
        END_IF
      END_IF
  4: (* UA_Write *)
      fbUA_Write(
```

```c
```
4.3.3.5 How to call methods

The following section describes how you use the TcX_PLCopen_OpcUa function block to call methods on a local or remote OPC UA Server.

This section contains the following topics:

- **Overview** [→ 146]
- Schematic workflow [→ 146]
- General notes [→ 147]
- Code snippet [→ 147]

**Overview**

The following function blocks are required to connect to an OPC UA Server, call UA methods, and subsequently interrupt the session: **UA_Connect** [→ 180], **UA_GetNamespaceIndex** [→ 182], **UA_MethodGetHandle** [→ 184], **UA_MethodCall** [→ 183], **UA_MethodReleaseHandle** [→ 185], **UA_Disconnect** [→ 181].

First of all, read the section **How to determine communication parameters** [→ 135] so as to be able to understand certain UA functions better (e.g. how MethodIdentifier can be determined) as well as the section **How to establish a connection** [→ 139].

**Schematic workflow**

The schematic workflow of each TwinCAT OPC UA Client can be categorized into three different phases: Preparation, Work and Cleanup.
The use case described in this section can be visualized as follows:

**General notes**

- The UA_Connect function block requires the following information to establish a connection to a local or remote OPC UA Server (see also How to establish a connection:

  - Server URL
  - Session Connect Information

- The UA_GetNamespaceIndex function block requires a connection handle (from UA_Connect) and a NamespaceURI for resolution in a NamespaceIndex, which will be used later by UA_NodeGetHandle to obtain a node handle (see also How to determine communication parameters):

- The UA_MethodGetHandle function block requires a connection handle (from UA_Connect), an ObjectNodeID and a MethodNodeID in order to obtain a method handle (see also How to determine communication parameters:

- The UA_MethodCall function block requires a connection handle (from UA_Connect), a method handle (from UA_MethodGetHandle) and information about the input and output arguments of the method that is to be called. Information about the input arguments is represented by the input parameters pInputArgInfo and pInputArgData of UA_MethodCall. Information about the output parameters is represented by the pOutputArgInfo and pOutputArgData input parameters of UA_MethodCall. The input parameter pOutputArgInfoAndData then represents a pointer to a structure containing the results of the method call, including all output parameters. In the following code snippet the pInputArgInfo and pInputArgData parameters are calculated and created in the M_Init method.

- The UA_NodeReleaseHandle function block requires a connection handle (from UA_Connect) and a method handle (from UA_MethodGetHandle).

**Code snippet**

**M_Init initialization method of the function block containing the UA method call**

```c
MEMSET(ADR(nInputData),0,SIZEOF(nInputData));
nArg := 1;

{"********** Input parameter 1 **********}
InputArguments[nArg].DataType := eUAType_Int16;
InputArguments[nArg].ValueRank := -1; (* Scalar = -1 or Array *)
InputArguments[nArg].ArrayDimensions[1] := 0; (* Number of Dimension in case its an array *)
InputArguments[nArg].nLenData := SIZEOF(numberIn1); (* Length if its a STRING *)
IF nOffset + SIZEOF(numberIn1) > nInputArgSize THEN
  bInputDataError := TRUE;
  RETURN;
ELSE
  MEMCPY(ADR(nInputData)+nOffset,ADR(numberIn1),SIZEOF(numberIn1)); (* VALUE in BYTES FORM *)
  nOffset := nOffset + SIZEOF(numberIn1);
END_IF
nArg := nArg + 1;

{"********** Input parameter 2 **********}
InputArguments[nArg].DataType := eUAType_Int16;
InputArguments[nArg].ValueRank := -1; (* Scalar = -1 or Array *)
InputArguments[nArg].ArrayDimensions[1] := 0; (* Number of Dimension in case its an array *)
InputArguments[nArg].nLenData := SIZEOF(numberIn2); (* Length if its a STRING *)
```
IF nOffset + SIZEOF(numberIn2) > nInputArgSize THEN
    bInputDataError := TRUE;
RETURN;
ELSE
    MEMCPY(ADR(nInputData)+nOffset,ADR(numberIn2),SIZEOF(numberIn2));(* VALUE in BYTES FORM *)
    nOffset := nOffset + SIZEOF(numberIn2);
END_IF

cbWriteData := nOffset;

Declaration:

/* Declarations for UA_GetNamespaceIndex */
fbUA_GetNamespaceIndex : UA_GetNamespaceIndex;
nNamespaceIndex : UINT;

/* Declarations for UA_MethodGetHandle */
fbUA_MethodGetHandle: UA_MethodGetHandle;
ObjectNodeID: ST_UANodeID;
MethodNodeID: ST_UANodeID;
nMethodHdl: DWORD;

/* Declarations for UA_MethodCall */
fbUA_MethodCall: UA_MethodCall;
sObjectNodeIdIdentifier : STRING(MAX_STRING_LENGTH) := 'MAIN.fbMathematics';
sMethodNodeIdIdentifier : STRING(MAX_STRING_LENGTH) := 'MAIN.fbMathematics#M_Mul';
nAdrWriteData: PVOID;
numberIn1: INT := 42; // change according to input value and data type
numberIn2: INT := 42; // change according to input value and data type
numberOutPro: DINT; // result (output parameter of M_Mul())
cbWriteData: UDINT; // calculated automatically by M_Init()
InputArguments: ARRAY[1..2] OF ST_UAMethodArgInfo; // change according to input parameters
stOutputArgInfo: ARRAY[1..1] OF ST_UAMethodArgInfo; // change according to output parameters
stOutputArgInfoAndData: ST_OutputArgInfoAndData;
nInputData: ARRAY[1..4] OF BYTE; // numberIn1(INT16)(2) + numberIn2(INT16)(2)
nOffset: UDINT; // calculated by M_Init()
nArg: INT; // used by M_Init()

/* Declarations for UA_MethodReleaseHandle */
fbUA_MethodReleaseHandle: UA_MethodReleaseHandle;

Implementation:

CASE iState OF
  0:
    [...] 
  2: (* GetNS Index *)
    fbUA_GetNamespaceIndex{
      Execute := TRUE,
      ConnectionHdl := nConnectionHdl,
      NamespaceUri := sNamespaceUri,
      NamespaceIndex => nNamespaceIndex);
    IF NOT fbUA_GetNamespaceIndex.Busy THEN
      fbUA_GetNamespaceIndex(Execute := FALSE);
      IF NOT fbUA_GetNamespaceIndex.Error THEN
        iState := iState + 1;
      ELSE
        bError := TRUE;
        nErrorID := fbUA_GetNamespaceIndex.ErrorID;
        iState := 7;
      END_IF
    END_IF
  END_IF

  3: (* Get Method Handle *)
    ObjectNodeID.eIdentifierType := eUAIdentifierType_String;
    ObjectNodeID.nNamespaceIndex := nNamespaceIndex;
    ObjectNodeID.sIdentifier := sObjectNodeIdIdentifier;
    MethodNodeID.eIdentifierType := eUAIdentifierType_String;
    MethodNodeID.nNamespaceIndex := nNamespaceIndex;
    MethodNodeID.sIdentifier := sMethodNodeIdIdentifier;
    M_Init();
    IF bInputDataError = FALSE THEN
      iState := iState + 1;
    ELSE
      bBusy := FALSE;
      bError := TRUE;
      nErrorID := 16#70A; //out of memory
END_IF

4: (* Method Get Handle *)

fbUA_MethodGetHandle(
  Execute := TRUE,
  ConnectionHdl := nConnectionHdl,
  ObjectNodeID := ObjectNodeID,
  MethodNodeID := MethodNodeID,
  MethodHdl => nMethodHdl);

IF NOT fbUA_MethodGetHandle.Busy THEN
  fbUA_MethodGetHandle(Execute := FALSE);
IF NOT fbUA_MethodGetHandle.Error THEN
  iState := iState + 1;
ELSE
  bError := TRUE;
  nErrorID := fbUA_MethodGetHandle.ErrorID;
  iState := 6;
END_IF
END_IF

5: (* Method Call *)

stOutputArgInfo[1].nLenData := SIZEOF(stOutputArgInfoAndData.pro);

fbUA_MethodCall(
  Execute := TRUE,
  ConnectionHdl := nConnectionHdl,
  MethodHdl := nMethodHdl,
  nNumberOfInputArguments := nNumberOfInputArguments,
  pInputArgInfo := ADR(InputArguments),
  cbInputArgInfo := SIZEOF(InputArguments),
  pInputArgData := ADR(nInputData),
  cbInputArgData := cbWriteData,
  pInputWriteData := 0,
  cbInputWriteData := 0,
  nNumberOfOutputArguments := nNumberOfOutputArguments,
  pOutputArgInfo := ADR(stOutputArgInfo),
  cbOutputArgInfo := SIZEOF(stOutputArgInfo),
  pOutputArgInfoAndData := ADR(stOutputArgInfoAndData),
  cbOutputArgInfoAndData := SIZEOF(stOutputArgInfoAndData));

IF NOT fbUA_MethodCall.Busy THEN
  fbUA_MethodCall(Execute := FALSE);
IF NOT fbUA_MethodCall.Error THEN
  iState := iState + 1;
  numberOutPro := stOutputArgInfoAndData.pro;
ELSE
  bError := TRUE;
  nErrorID := fbUA_MethodCall.ErrorID;
  iState := 6;
END_IF
END_IF

6: (* Release Method Handle *)

fbUA_MethodReleaseHandle(
  Execute := TRUE,
  ConnectionHdl := nConnectionHdl,
  MethodHdl := nMethodHdl);

IF NOT fbUA_MethodReleaseHandle.Busy THEN
  fbUA_MethodReleaseHandle(Execute := FALSE);
ELSE
  bBusy := FALSE;
  bError := TRUE;
  nErrorID := fbUA_MethodReleaseHandle.ErrorID;
  iState := 7;
END_IF
END_IF

7: ([...])

END_CASE
4.3.4 Security

4.3.4.1 Overview

Security was a central requirement in the development of OPC UA. It is addressed in various areas:

- Encryption
- Integrity
- Authentication

The confidentiality of the exchanged information is secured by the encryption of the exchanged messages. Modern cryptographic algorithms are used for this. In order to be able to cope with future security requirements as well, even stronger and more modern algorithms can subsequently be added to an application without changing the protocol.

Different security levels can be selected according to the requirements of the respective application. In some areas it is sufficient to sign the messages in order to prevent changes being made by third parties, while additional encryption of the messages is necessary in other cases where the data must also not be read by third parties.

TF6100 OPC UA offers the following security levels (security endpoints) that clients can connect to:

- None: No security
- Sign: signed messages
- Sign & Encrypt: signed and encrypted messages

The signing of messages prevents a third party from changing the contents of a message. This prevents, for example, a write statement to open a switch being falsified by a third party and the switch being closed instead.

OPC UA applications identify themselves via so-called software and application instance certificates. With the aid of software certificates it is possible to grant certain client applications extended access to the information on an OPC UA Server, for example for the engineering of an OPC UA Server. Application instance certificates can be used to ensure that an OPC UA Server communicates only with preconfigured clients. A client can ensure by means of the server’s application instance certificate that it is speaking to the correct server (similar to the certificates of a Web browser). The taking into account of these certificates is optional, i.e. an OPC UA server can also grant the same access to each client, depending on the user rights.

The TwinCAT OPC UA Client and TwinCAT OPC UA Server generate a self-signed certificate during the first startup process. This certificate consists of a private key and a public key. The private key is saved in the PKI\CA\private directory and the corresponding public key in the PKI\CA\certs directory. Any OPC UA Client wishing to establish a secure connection with the Server via one of the security endpoints (Sign, Sign&Encrypt) must know the public key of the OPC UA Server. Conversely the OPC UA Server must know the Client’s public key. This so-called key exchange is described in the following sections:

- Authentication [109]
- Certificate exchange [150]
- Access rights [111]

4.3.4.2 Certificate exchange

The communication between an OPC UA Client and an OPC UA Server can optionally be secured by communication with a secure endpoint. By default, both the TwinCAT OPC UA Server and the TwinCAT OPC UA Client generate a machine-specific, self-signed certificate for authentication the first time they are started.

If you want to use such an encrypted communication connection in your environment, you need to establish a trust relationship between OPC UA Server and OPC UA Client.
Trust settings on the server

If you want to authenticate one or more OPC UA Clients to the OPC UA Server via certificates, the OPC UA Server must trust the public keys of the clients. This can be done via the file system, for example. The server manages the trust settings for certificates via the file system.

- Trusted certificates: `%InstallDir%\Server\PKI\CA\trusted\certs`
- Rejected certificates: `%InstallDir%\Server\PKI\CA\rejected\certs`

By moving client certificates between these directories, the trust settings can be adjusted accordingly.

Reading a client certificate

A simple way of accessing the client certificate is described below. To do this, you establish a connection to the UA Server using a secure endpoint (for example, Basic128Rsa15/Sign&Encrypt) without first copying the client certificate to the UA Server. This connection is naturally rejected by the UA Server, since it does not trust the UA Client at this point in time. In this case, the TwinCAT OPC UA Client would return the error 0xE4DD0102, for example. However, after rejecting the connection request, the UA Server stores a copy of the client certificate in the above-mentioned "Rejected" directory. The name of the certificate corresponds to the "Thumbprint" of the certificate and can thus be clearly assigned to the client certificate. You can now move this file directly to the above-mentioned "Trusted" directory so that the UA Server can trust the UA Client and accept the connection for all other connection requests.

Announcing OPC UA Servers to the OPC UA Client

Depending on the OPC UA Client employed, different steps may need to be taken so that the OPC UA Client trusts the OPC UA Server. Typically, for client applications with a graphical user interface, a warning message is displayed the first time you connect to the server, whereby the server certificate can then be classified as trustworthy.

The following instruction is therefore only valid for the TwinCAT OPC UA Client.

The public key of the OPC UA Server is located in the following directory as a DER file: `%InstallDir%\Server\PKI\CA\own\certs`

In the case of the TwinCAT OPC UA Client, copy the file into the corresponding "Trusted" directory: `%InstallDir%\Client\PKI\CA\certs`
4.4 Gateway

4.4.1 Overview

The TwinCAT OPC UA Gateway is the latest addition to the TS6100/TF6100 software product. It not only includes a conventional OPC DA interface for connecting older OPC COM DA applications to the TwinCAT OPC UA Server and can therefore be regarded as the successor of the old TwinCAT OPC DA Server (TS6120/TF6120), it also offers an OPC UA interface for converting several basic TwinCAT OPC UA Servers to a central OPC UA Server.

4.4.2 Quick start

The TS6100/TF6100 setup automatically installs the TwinCAT OPC UA Gateway and registers the application as a Windows service. The setup automatically configures access to a TwinCAT OPC UA Server running on the same computer as the gateway.

If more than one OPC UA Server is added to the gateway, or if the server is running on a different computer, the standard configuration has to be modified. Use the Configurator to configure these settings.

**Configuration of the TwinCAT OPC UA Server**

Check the configuration of the OPC UA Server and make sure that it is operating as expected before continuing.

For further information regarding the configuration of the OPC UA Server, read the Quick start in the section "OPC UA Server".

**Quick start – OPC COM DA**

To connect an OPC COM DA Client to the gateway, start the client and establish a connection to the following ProgId:
When browsing the gateway, one or more OPC UA Servers will be visible in the namespace of the gateway.

Quick start – OPC UA

The gateway not only offers an OPC COM DA interface, but also allows the aggregation of one or more OPC UA Servers. The gateway also opens an OPC UA interface for this purpose. The gateway can be accessed via the following OPC UA Server URL:
The namespace of the gateway then contains all underlying TwinCAT OPC UA Servers.

4.4.3 Licensing

The TwinCAT OPC UA Gateway is supplied free of charge. No further license purchase is required.

Note that the gateway component can only be used for connecting to TwinCAT OPC UA Servers. The software prevents connections to third-party UA Servers. The Unified Automation UA Gateway is recommended where the environment necessitates the connection with a UA Server from a third party. It can be purchased from [http://www.unified-automation.com](http://www.unified-automation.com).

4.4.4 Scenarios

On account of the open and flexible PC-based automation technology from Beckhoff, the OPC UA Gateway can be operated and installed in different ways. The following section describes the various setup scenarios and explains the advantages and disadvantages of each configuration.
Gateway and UA Server on the same computer

In this scenario, the gateway and the UA Server are installed on the same computer. The gateway is configured with the standard settings in order to establish a connection with the local OPC UA Server with the following Server URL: opc.tcp://localhost:4840.

This scenario only works on non-Windows CE devices.

The TwinCAT OPC UA Server is also available for Windows CE, but the gateway is only available for "big" Windows platforms.

Gateway and UA Server on different computers

In this scenario, the gateway and the UA Server are installed on different computers. The gateway is configured for the establishment of a connection with the remote OPC UA Server by defining the latter's corresponding Server URL, e.g. opc.tcp://192.168.1.1:4840.

The OPC UA Server may be installed on a small embedded device (e.g. a CX8090 with Windows CE), while the gateway component is installed on a separate big Windows platform, e.g. a central server device.

Gateway connected to multiple UA Server devices

Please note that, regardless of the scenarios described above, it is also possible to connect other TwinCAT OPC UA Servers to the gateway. For example, the gateway can be configured to access the following servers:

- the local TwinCAT OPC UA Server (e.g. opc.tcp://localhost:4840)
- a remote TwinCAT OPC UA Server (e.g. opc.tcp://192.168.1.1:4840)
- another remote TwinCAT OPC UA Server (e.g. opc.tcp://192.168.1.21:4841)
- ...
4.4.5 Configurator

4.4.5.1 Overview

The UA Gateway Administration Tool is a graphic user interface for the configuration of the gateway.

The tool is opened via the context menu of the gateway symbol in the Windows taskbar. After starting the administration tool via the command Administrate UaGateway, the graphic user interface appears.

The interface offers several configuration options:

- General settings [156]
- Additional UA Servers [158]
- Additional endpoints [159]
- OPC COM DA settings [160]

4.4.5.2 General settings

The General tab displays general settings of the UA Gateway.
Autostart
In this area you can configure the autostart behavior of the UA Gateway.

Activate **UaGateway Runtime Process** to start the UA Gateway Service automatically when the computer is switched on.

Activate the **Notification Area Icon** to start the symbol of the notification area when a user logs on.

Launching User
The UA Gateway is executed as a Windows NT service. This service is assigned a specific user context so that COM/DCOM can be properly configured. The user you select is assigned to the UA Gateway service. In addition, the user is granted a LogOnAsService right (so he/she can start the service) and is added to a local
user group ("UaGatewayUsers"). This group is added to the Access Control List (ACL) of the local machine. For proper COM/DCOM configuration you must add to this group all the users who are permitted to start and access the UA Gateway.

**Configuration Permissions**

It is possible to allow only certain users to change the configuration of the UA Gateway, i.e. to add or remove connections to basic servers. You can choose from the following settings:

<table>
<thead>
<tr>
<th>Everyone</th>
<th>Any user (including users anonymously logged on to UA) who can contact the UA Gateway can change the configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit to operating system users</td>
<td>Only local users and users within the same domain can change the configuration.</td>
</tr>
<tr>
<td>Limit to users of this group</td>
<td>Only users within a specific group to change the configuration. If not all available groups are displayed in the Group drop-down list (or a newly created group is missing), use the Refresh button to read this group again.</td>
</tr>
</tbody>
</table>

**Remote DCOM Access**

When Allow Remote Connection to UaGateway OPC COM Server is enabled, DCOM port 135 and the executable UA Gateway are added to the firewall exception list.

If Allow starting UaGateway by DCOM Clients is disabled, DCOM clients cannot start the UA Gateway. In this case, UA Gateway can still be started or stopped using the Notification Area Icon or the Start menu entries.

**UA Discovery Registration (UA Local Discovery Server)**

Activate Register at Local Discovery Server if the UA Gateway is to be registered with the OPC UA LDS (Local Discovery Server), if one is installed.

**4.4.5.3 Additional UA Servers**

The Configured UA Servers tab offers options for the configuration of the underlying OPC UA Servers. By default the gateway already establishes a connection with the local OPC UA Server (which is running on the same computer).
To configure or remove further OPC UA Servers from the configuration, click on the Plus and Minus buttons in the lower right-hand corner and then Apply to save the changes.

### 4.4.5.4 Additional endpoints

The UA Endpoints tab shows the settings for the UA endpoint configuration.

The UA endpoint is the connection information that a UA Client requires to connect to the gateway.

**General**

Use the checkboxes to specify the logon methods that a client can use to connect to your UA Gateway.
Endpoints

Here you can define all settings required for different UA endpoints. The endpoint is configured with default settings as standard. These represent a single UA endpoint offering two security options: None and Basic128RSsa15.

The None security option allows every UA Client to connect to the UA Gateway. This configuration is only recommended during commissioning and testing. In a production environment this configuration should be switched off.

The various configuration elements are described in the following sections.

Network configuration

<table>
<thead>
<tr>
<th>Endpoint URL</th>
<th>This is the endpoint URL of the UA Gateway as seen in FindServers and GetEndpoint calls.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>This is the protocol used for this endpoint.</td>
</tr>
<tr>
<td>Host name/IP</td>
<td>This is the host name of the UA Gateway (it can also be the IP address of the PC running the UA Gateway).</td>
</tr>
<tr>
<td>Network adapter</td>
<td>This is the network adapter to be used for binding. The available options are:</td>
</tr>
<tr>
<td>All</td>
<td>Binding is to be applied to all IP addresses of the computer. The endpoint will be accessible via the given port on all IP addresses.</td>
</tr>
<tr>
<td>Local only</td>
<td>With this selection, the UA Gateway only establishes a binding with the loopback adapter. The endpoint can only be reached by clients running on the same machine as the UA Gateway.</td>
</tr>
<tr>
<td>Port</td>
<td>This is the TCP port of the endpoint (normally 48050).</td>
</tr>
</tbody>
</table>

Security

In this area you can configure the supported security settings of the endpoint. Select the checkboxes for the security options you want to apply to a specific endpoint. For options other than "None", the available message security mode(s) must be specified. Signing ensures that messages cannot be changed and that they are exchanged between applications that have established a connection. Encryption guarantees that no one can read the messages.

4.4.5.5 OPC COM DA settings

The OPC DA (COM) tab shows the settings for the configuration of the COM DA Server of the UA Gateway.

The following section describes how to configure the COM DA Server of the UA Gateway using the administration tool.

General

ItemIDs of the COM DA Server are formed from the URI namespace and the identifier of the variable node in the OPC UA address space. The namespace part can be omitted in the case of a single namespace.

In the Default Name Space drop-down field you can specify the default namespace with the namespace of a basic OPC server. The ItemIDs of this particular namespace can then be reached by specifying the identifier only, because the default namespace is automatically added internally when an element is accessed. This feature can be used to reconfigure all ItemIDs in the client that accesses the UA Gateway server, if the latter serves as a tunnel solution for a basic COM DA Server, while maintaining the ItemIDs of the original COM DA Server.

In the second drop-down field the Timestamp Source can be defined. The following options are available:
Properties mapping from UA to COM DA

When connecting to the UA Gateway's OPC COM DA Server, all six standard properties (DataType, Value, Quality, TimeStamp, AccessRights and ScanRate) are automatically assigned. Underlying OPC Servers can provide further properties (e.g. user-defined properties, DI properties, etc.). These properties can be assigned to vendor-specific properties (PropertyID ≥ 5000) in the COM DA Server of the UA Gateway.

These vendor-specific PropertyIDs are automatically assigned when the properties are requested for the first time. This dialog allows you to change the assigned PropertyIDs or configure how the OPC UA properties in the UA Gateway address space are assigned to the vendor-specific COM DA properties. You have to define the property name on the UA side and the namespace of the property in the UA Gateway and assign it to the COM DA PropertyIDs. When connecting to the UA Gateway's COM DA server, you can navigate through the available properties (QueryAvailableProperties) of a single OPCItem and then you will be able to see the associated properties as they have been configured (in the range of vendor-specific PropertyIDs above 5000).

Press the [+] or [-] key respectively to add or remove a certain property. To change the contents of a particular field, double-click it and enter the required values. Double-clicking a value in the UA Property NameSpace URI column displays a drop-down menu where you can make a selection.

If you add a new property by pressing [+], the values of the last entry are copied to the new line and the PropertyID is automatically incremented.

4.4.6 Migrating from Tx6120

One of the primary purposes of the UA Gateway is to provide a sustainable connectivity in order to replace the Tx6120 OPC DA supplement/function. Observe the following notes if you wish to migrate Tx6120 OPC DA to UA Gateway.

Standard configuration

The standard configuration of the UA Gateway automatically establishes a connection with the local OPC UA Server and offers the OPC DA Clients an OPC DA interface. For a connection based on this standard configuration, the OPC DA clients must consider the following points:

- The default ProgID of the UA Gateway is "UnifiedAutomation.Gateway.1". The TwinCAT OPC DA Server uses a different ProgID ("Beckhoff.TwinCATOpcServerDA").
- The UA Gateway always uses a ProgID instead of multiple clones.
- The ItemIdentifier of an OPC symbol is generated differently in the UA Gateway. This behavior can be changed.

Changing the syntax of an ItemIdentifier

The syntax used by the UA Gateway for ItemIdentifier can be changed so that the latter corresponds more to the type of the TwinCAT OPC DA Server. By default, the UA Gateway uses a different syntax to that of the TwinCAT OPC DA Server when creating its identifiers.
UA Gateway sample:

Sample TwinCAT OPC DA Server:

The UA Gateway uses a prefix so that the underlying OPC UA Client from which the variable originates can be clearly identified.

The following steps are required to configure the UA Gateway so that it forms its identifiers in roughly the same way as the TwinCAT OPC DA Server. The functionality has been implemented to simplify the migration process.

1. Open the UA Gateway configuration file
   
   \`C:\Program Files (x86)\UnifiedAutomation\UaGateway\bin\uagateway.config.xml\`

2. Look for the following XML tags in the XML file:

   \`<OpcServerConfig>
   <ComDaServerConfig>
   <ComDaNamespaceUseAlias>false</ComDaNamespaceUseAlias>
   </ComDaServerConfig>
   </OpcServerConfig>\`

3. If the XML tag ComDaNamespaceUseAlias is set to "true", user-defined prefixes can be specified. To do this, look for the following XML tag in the same XML file:

   \`<OpcServerConfig>
   <UaServerConfig>
   <ConfiguredNamespaces>
   ...
   </ConfiguredNamespaces
   </UaServerConfig>
   </OpcServerConfig>\`

4. In this XML structure, identify the TwinCAT OPC UA Server namespace. By default, it should read as follows:

   \`<OpcServerConfig>
   <UaServerConfig>
   <ConfiguredNamespaces>
   ...
   <Namespace>
   <Index>\`...
   <Uri>TcOpcUaServer/urn:Hostname:BeckhoffAutomation:Ua:PLC1</Uri>
   <AllowRenameUri>false</AllowRenameUri>\`

   \`</Namespace>\`

\`</ConfiguredNamespaces>
\`</UaServerConfig>
\`</OpcServerConfig>\`
5. On your computer, the placeholder "..." may look different. Set <ComAlias> to your preferred prefix, for example "PLC1". The identifiers are then created with the prefix "PLC1".

4.4.7 Security

4.4.7.1 Overview

Security was a central requirement in the development of OPC UA. It is addressed in various areas:

- Encryption
- Integrity
- Authentication

The confidentiality of the exchanged information is secured by the encryption of the exchanged messages. Modern cryptographic algorithms are used for this. In order to be able to cope with future security requirements as well, even stronger and more modern algorithms can subsequently be added to an application without changing the protocol.

Different security levels can be selected according to the requirements of the respective application. In some areas it is sufficient to sign the messages in order to prevent changes being made by third parties, while additional encryption of the messages is necessary in other cases where the data must also not be read by third parties.

TF6100 OPC UA offers the following security levels (security endpoints) that clients can connect to:

- None: No security
- Sign: signed messages
- Sign & Encrypt: signed and encrypted messages

The signing of messages prevents a third party from changing the contents of a message. This prevents, for example, a write statement to open a switch being falsified by a third party and the switch being closed instead.

OPC UA applications identify themselves via so-called software and application instance certificates. With the aid of software certificates it is possible to grant certain client applications extended access to the information on an OPC UA Server, for example for the engineering of an OPC UA Server. Application instance certificates can be used to ensure that an OPC UA Server communicates only with preconfigured clients. A client can ensure by means of the server’s application instance certificate that it is speaking to the correct server (similar to the certificates of a Web browser). The taking into account of these certificates is optional, i.e. an OPC UA server can also grant the same access to each client, depending on the user rights.
The TwinCAT OPC UA Client and TwinCAT OPC UA Server generate a self-signed certificate during the first startup process. This certificate consists of a private key and a public key. The private key is saved in the \PKI\CA\private directory and the corresponding public key in the \PKI\CA\certs directory. Any OPC UA Client wishing to establish a secure connection with the Server via one of the security endpoints (Sign, Sign&Encrypt) must know the public key of the OPC UA Server. Conversely the OPC UA Server must know the Client’s public key. This so-called key exchange is described in the following sections:

- Authentication [109]
- Certificate exchange [164]
- Access rights [111]

4.4.7.2 Certificate exchange

The communication between an OPC UA Client and an OPC UA Server can optionally be secured by communication with a secure endpoint. By default, both the TwinCAT OPC UA Server and the TwinCAT OPC UA Client generate a machine-specific, self-signed certificate for authentication the first time they are started.

If you want to use such an encrypted communication connection in your environment, you need to establish a trust relationship between OPC UA Server and OPC UA Client.

**Trust settings on the server**

If you want to authenticate one or more OPC UA Clients to the OPC UA Server via certificates, the OPC UA Server must trust the public keys of the clients. This can be done via the file system, for example. The server manages the trust settings for certificates via the file system.

- Trusted certificates: %InstallDir%\Server\PKI\CA\trusted\certs
- Rejected certificates: %InstallDir%\Server\PKI\CA\rejected\certs

By moving client certificates between these directories, the trust settings can be adjusted accordingly.

**Reading a client certificate**

A simple way of accessing the client certificate is described below. To do this, you establish a connection to the UA Server using a secure endpoint (for example, Basic128Rsa15/Sign&Encrypt) without first copying the client certificate to the UA Server. This connection is naturally rejected by the UA Server, since it does not trust the UA Client at this point in time. In this case, the TwinCAT OPC UA Client would return the error 0xE4DD0102, for example. However, after rejecting the connection request, the UA Server stores a copy of the client certificate in the above-mentioned “Rejected” directory. The name of the certificate corresponds to
the "Thumbprint" of the certificate and can thus be clearly assigned to the client certificate. You can now move this file directly to the above-mentioned "Trusted" directory so that the UA Server can trust the UA Client and accept the connection for all other connection requests.

**Announcing OPC UA Servers to the OPC UA Client**

Depending on the OPC UA Client employed, different steps may need to be taken so that the OPC UA Client trusts the OPC UA Server. Typically, for client applications with a graphical user interface, a warning message is displayed the first time you connect to the server, whereby the server certificate can then be classified as trustworthy.

The following instruction is therefore only valid for the TwinCAT OPC UA Client.

The public key of the OPC UA Server is located in the following directory as a DER file: `%InstallDir%\Server\PKI\CA\own\certs`

In the case of the TwinCAT OPC UA Client, copy the file into the corresponding "Trusted" directory: `%InstallDir%\Client\PKI\CA\certs`

### 4.5 Sample Client

#### 4.5.1 Overview

As of version 1.6.80 of the TwinCAT OPC UA Server, a small "UA Sample Client" program is automatically installed. The program enables you to browse the OPC UA namespace and to test the UA Server installation. It is located in the Windows Start menu and in the installation directory of the Supplement/Function. You can run the program both directly on the UA Server and on a computer in your network.

The UA Sample Client currently offers the following features:

- Connecting to the OPC UA Server
- Establishing a secure connection with OPC UA Server (see Establishing a secure connection to OPC UA Server [166])
- Browsing the UA namespace of an OPC UA Server (see Browsing the UA namespace [169])
- Adding a UA node from the namespace to the watchlist, which reads the value of the node regularly (see Using the Watchlist [170])

This application is only an OPC UA Sample Client. It does not offer any sophisticated functionalities, but has been developed to provide users with an easy-to-use interface for carrying out initial tests on the OPC UA Server.

To start the application, run the `UA SampleClient.exe` file with the Run as Admin option.

**Endpoints of the OPC UA Server**

The UA Sample Client first connects itself to a specified server URL. The client acquires all endpoints of the OPC UA Server (see Endpoints drop-down list). The list returned to the server then contains more information about all the available endpoints the client can connect to. Each endpoint can contain the host name of the OPC UA Server instead of the IP address. The client then uses the information from the endpoint to connect to the server.

If the name solution does not work on the user’s network, the client cannot connect. If the endpoint to which you want the client to connect contains the host name of the server, make sure that the name solution works on your network and that the host name is accessible on the server.
4.5.2 Establishing a secure connection to OPC UA Server

1. Enter the URL of an OPC UA Server in the upper text field of the UA Sample Client.
2. Click the Get Endpoints button.
The endpoints provided by the UA Server are then displayed in the Endpoints drop-down list.

3. In this sample, select the entry "<SomeName>/Beckhoff/TcOpcUaServer/1[Basic128Rsa15, SignAndEncrypt] [opc.tcp://<SomeName>:4840]" and click Connect. You must copy the public key from the certificate of the UA Sample Client to the UA Server so that it "trusts" the Sample Client. Otherwise, the connection attempt is rejected by the UA Server via the secure
Technical introduction

channel ("BadSecureChannelClosed"). Further information on the certificate management with the OPC UA Server can be found in the section Certificate exchange [164].
You can now use the **Browser** in the left half of the window to navigate through the UA namespace.

### 4.5.3 Browsing the UA namespace

When a successful connection has been established you can use the **Browser** in the left half of the UA Sample Client to navigate through the UA namespace. Below the node **PLC1** you will find the currently running PLC program, and you can display the variables declared there and released for UA.
4.5.4 Using the Watchlist

You can insert PLC variables from the UA namespace into a watchlist, for example to have their values read cyclically by the UA Sample Client. To do this, open the context menu of a variable and select **Add to Watchlist**. The variable is then transferred to the watchlist and its values are automatically read out cyclically from the PLC.
5 PLC API

5.1 Tc2_OpcUa

5.1.1 Data types

5.1.1.1 ST_OpcUAServerInfo

TYPE ST_OpcUAServerInfo :
  STRUCT
    nReserved : UDINT;
    nCummulatedSessionCount : UDINT;
    nCurrentSessionCount : UDINT;
    nRejectedSessionCount : UDINT;
    nSecurityRejectedSessionCount : UDINT;
    nSessionTimeoutCount : UDINT;
    nCurrentSubscriptionCount : UDINT;
    nRejectedRequestCount : UDINT;
    nSecurityRejectedRequestCount : UDINT;
  END_STRUCT
END_TYPE

ST_OpcUAServerInfo contains session information of a TwinCAT OPC UA Server.

5.1.1.2 E_OpcUAServerOption

TYPE E_OpcUAServerOption
{
  eOPCUAServerOption_None,
  eOPCUAServerOption_Restart,
  eOPCUAServerOption_Shutdown,
  eOPCUAServerOption_RefreshCfg,
  eOPCUAServerOption_ServerInfo
};
END_TYPE

E_OpcUAServerOption determines which command is to be sent to the TwinCAT OPC UA Server.

5.1.1.3 E_OpcUAServerStatus

TYPE E_OpcUAServerStatus
{
  eOPCUAServerStatus_None,
  eOPCUAServerStatus_Alive,
  eOPCUAServerStatus_NotResponding
};
END_TYPE

E_OpcUAServerStatus represents the runtime status of a TwinCAT OPC UA Server.

5.1.2 Function blocks

5.1.2.1 FB_OpcUAServer

The function block enables status information to be read out and a TwinCAT OPC UA Server to be restarted.

Syntax

Definition:
FUNCTION_BLOCK FB_OpcUAServer
VAR_INPUT
  sNetId : T_AmsNetId;
  bExecute : BOOL;
  eOpcUAServerOption : E_OpcUAServerOption;
  tTimeout : TIME;
END_VAR
VAR_OUTPUT
  stOpcUAServerInfo : ST_OpcUAServerInfo;
  bBusy : BOOL;
  bError : BOOL;
  nErrorId : UDINT;
END_VAR

Inputs

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sNetId</td>
<td>T_AmsNetId</td>
<td>AmsNetId of the system on which the TwinCAT OPC UA Server runs.</td>
</tr>
<tr>
<td>bExecute</td>
<td>BOOL</td>
<td>A rising edge activates processing of the function block.</td>
</tr>
<tr>
<td>eOpcUAServerOption</td>
<td>E_OpcUAServerOption [172]</td>
<td>Specifies the operation to be performed.</td>
</tr>
<tr>
<td>tTimeout</td>
<td>TIME</td>
<td>ADS Timeout</td>
</tr>
</tbody>
</table>

Outputs

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stOpcUAServerInfo</td>
<td>ST_OpcUAServerInfo [172]</td>
<td>Contains status information from the server when ServerInfo is selected at the eOpcUAServerOption input.</td>
</tr>
<tr>
<td>bBusy</td>
<td>BOOL</td>
<td>TRUE as long as processing of the function block is in progress.</td>
</tr>
<tr>
<td>bError</td>
<td>BOOL</td>
<td>Becomes TRUE as soon as an error situation occurs.</td>
</tr>
<tr>
<td>nErrorId</td>
<td>UDINT</td>
<td>Contains the error code when an error (bError) occurs.</td>
</tr>
</tbody>
</table>

5.1.2.2 FB_OpcUAServerGetStatus

The function block enables the current status (Running, NotResponding) of a TwinCAT OPC UA Server to be read.

Syntax

Definition:

FUNCTION_BLOCK FB_OpcUAServerGetStatus
VAR_INPUT
  sNetId : T_AmsNetId;
  bGetStatus : BOOL;
  tTimeout : TIME;
END_VAR
VAR_OUTPUT
  eOpcUAServerStatus : E_OPCUAServerStatus;
  bDone : BOOL;
  bBusy : BOOL;
  bError : BOOL;
  nErrorId : UDINT;
END_VAR
## Inputs

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sNetId</td>
<td>T_AmsNetId</td>
<td>AmsNetId of the system on which the TwinCAT OPC UA Server runs.</td>
</tr>
<tr>
<td>bGetStatus</td>
<td>BOOL</td>
<td>A rising edge activates processing of the function block.</td>
</tr>
<tr>
<td>tTimeout</td>
<td>TIME</td>
<td>ADS Timeout</td>
</tr>
</tbody>
</table>

## Outputs

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eOpcUAserverStatus</td>
<td>E_OpcUAserverStatus</td>
<td>Contains status information from the server when ServerInfo is selected at the eOpcUAserverOption input.</td>
</tr>
<tr>
<td>bDone</td>
<td>BOOL</td>
<td>TRUE when processing of the function block is complete.</td>
</tr>
<tr>
<td>bBusy</td>
<td>BOOL</td>
<td>TRUE as long as processing of the function block is in progress.</td>
</tr>
<tr>
<td>bError</td>
<td>BOOL</td>
<td>Becomes TRUE as soon as an error situation occurs.</td>
</tr>
<tr>
<td>nErrorId</td>
<td>UDINT</td>
<td>Contains the error code when an error (bError) occurs.</td>
</tr>
</tbody>
</table>

### 5.2 Tc3_PLCopen_OpcUa

#### 5.2.1 Data types

##### 5.2.1.1 E_UAAttributeID

```plaintext
TYPE E_UAAttributeID:
{
    eUAI_NodeID    := 1, 
    eUAI_NodeClass := 2, 
    eUAI_BrowseName := 3, 
    eUAI_DisplayName := 4, 
    eUAI_Description := 5, 
    eUAI_WriteMask := 6, 
    eUAI_UserWriteMask := 7, 
    eUAI_IsAbstract := 8, 
    eUAI_Symmetric := 9, 
    eUAI_InverseName := 10, 
    eUAI_ContainsNoLoops := 11, 
    eUAI_EventNotifier := 12, 
    eUAI_Value := 13, 
    eUAI_DataType := 14, 
    eUAI_ValueRank := 15, 
    eUAI_ArrayDimensions := 16
} DINT;
END_TYPE
```

### Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

##### 5.2.1.2 E_UADataType

```plaintext
TYPE E_UADataType:
{
    eUAType_Undefined := -1, 
    eUAType_Null := 0, 
}
```
eUAType_Boolean := 1,
eUAType_SByte := 2,
eUAType_Byte := 3,
eUAType_Int16 := 4,
eUAType_UInt16 := 5,
eUAType_Int32 := 6,
eUAType_UInt32 := 7,
eUAType_Int64 := 8,
eUAType_UInt64 := 9,
eUAType_Float := 10,
eUAType_Double := 11,
eUAType_String := 12,
eUAType_DateTime := 13,
eUAType_Guid := 14,
eUAType_ValidString := 15,
eUAType_XmlElement := 16,
eUAType_Numeric := 17,
eUAType_ExpandedNodeId := 18,
eUAType_StatusCode := 19,
eUATypeQualifiedName := 20,
eUAType_LocalizedText := 21,
eUAType_ExtensionObject := 22,
eUAType_DataValue := 23,
eUAType_Variant := 24,
eUAType_DiagnosticInfo := 25
)DINT;
END_TYPE

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.1.3 E_UAIdentifierType

TYPE E_UAIdentifierType:
{
   eUAIdentifierType_String := 1,
   eUAIdentifierType_Numeric := 2,
   eUAIdentifierType_GUID := 3,
   eUAIdentifierType_Opaque := 4
)DINT;
END_TYPE

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.1.4 E_UASecurityMsgMode

TYPE E_UASecurityMsgMode:
{
   eUASecurityMsgMode_BestAvailable := 0,
   eUASecurityMsgMode_None := 1,
   eUASecurityMsgMode_Sign := 2,
   eUASecurityMsgMode_Sign_Encrypt := 3
}DINT;
END_TYPE

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>
5.2.1.5  **E_UASecurityPolicy**

TYPE E_UASecurityPolicy:
{
    eUASecurityPolicy_BestAvailable := 0,
    eUASecurityPolicy_None := 1,
    eUASecurityPolicy_Basic128 := 2,
    eUASecurityPolicy_Basic128Rsa15 := 3,
    eUASecurityPolicy_Basic256 := 4
} DINT;
END_TYPE

None: Guideline for configurations with minimal security requirements.

Basic128: Guideline for configurations with low to medium security requirements.

Basic128Rsa15: Defines a security guideline for configurations with moderate to high security requirements.

Basic256: Defines a security policy for configurations with high security requirements.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.1.6  **E_UATransportProfile**

TYPE E_UATransportProfile:
{
    eUATransportProfileUri_UATcp := 1,
    eUATransportProfileUri_WSHttpBinary := 2,
    eUATransportProfileUri_WSHttpXmlOrBinary := 3,
    eUATransportProfileUri_WSHttpXml := 4
} DINT;
END_TYPE

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.1.7  **ST_UASessionConnectInfo**

TYPE ST_UASessionConnectInfo:
STRUCT
    sApplicationUri : STRING(MAX_STRING_LENGTH);
    sApplicationName : STRING(MAX_STRING_LENGTH);
    eSecurityMode : E_UASecurityMsgMode;
    eSecurityPolicyUri : E_UASecurityPolicy;
    eTransportProfileUri : E_UATransportProfile;
    tSessionTimeout : TIME;
    tConnectTimeout : TIME;
END_STRUCT
END_TYPE

sApplicationUri: Application Uri maximum string length 255.
From TcUAClient 2.0.0.14 or higher this is automatically specified by the certificate, as defined in the PLCOpen specification.

sApplicationName: Application name with a maximum string length of 255.

eSecurityMode: Security message mode. For available modes see E_UASecurityMsgMode [175].

eSecurityPolicyUri: Security policy Uri. For available security policy Uri see E_UASecurityPolicy [176].
eTransportProfileUri: Transport profile Uri. For available transport profile Uri see E_UATransportProfile [176];

nSessionTimeout: Session timeout value.

nConnectTimeout: Value for the connection timeout. This must be set at the UA_Connect function block to match the ADS timeout. The following rule of thumb applies: ADS Timeout > 2 * ConnectionTimeout.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.1.8 ST_UAIndexRange

TYPE ST_UAIndexRange:

  STRUCT
    nStartIndex : UDIINT;
    nEndIndex   : UDIINT;
  END_STRUCT
END_TYPE

nStartIndex: Start index of the data.
nEndIndex: End index of the data.

For all dimensions:

- StartIndex and EndIndex must be assigned.
- StartIndex must be smaller than EndIndex.
- To be able to access all elements in a dimension, StartIndex and EndIndex must be assigned in the dimension depending on the total number of elements.
- Individual elements of a dimension can be selected by specifying the same StartIndex and EndIndex.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.1.9 ST_UAMethodArgInfo

TYPE ST_UAMethodArgInfo:

  STRUCT
    DataType        : E_UADataType := -1;
    ValueRank       : DINT := 2147483647;
    ArrayDimensions : ARRAY[1..3] OF UDIINT := [0,0,0];
    nLenData        : DINT;
  END_STRUCT
END_TYPE

DataType: Defines the UA data type for the method parameter. (Type: E_UADataType [174])

ValueRank: Determines whether the parameter is scalar (-1) or array.

ArrayDimensions: If the parameter is an array, it specifies the dimensions of the array. Each element determines the length per dimension.

nLenData: Specifies the length of the argument. For output information STRUCT only requests this element.
### Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

**5.2.1.10 ST_UANodeID**

```
TYPE ST_UANodeID:
  STRUCT
    nNamespaceIndex : UINT;
    nReserved       : ARRAY [1..2] OF BYTE; // fill bytes
    sIdentifier     : STRING(MAX_STRING_LENGTH);
    eIdentifierType : E_UAIdentifierType;
  END_STRUCT
END_TYPE
```

- **nNamespaceIndex**: Namespace index under which the node is available. Can be determined with the function block `UA_GetNamespaceIndex`.
- **sIdentifier**: Identifier as shown in the UA namespace (attribute 'Identifier').
- **eIdentifierType**: Variable type, described by `E_UAIdentifierType`.

### Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

**5.2.1.11 ST_UANodeAdditionalInfo**

```
TYPE ST_UANodeAdditionalInfo:
  STRUCT
    eAttributeID     : E_UAAttributeID;
    nIndexRangeCount : UINT;
    nReserved        : ARRAY [1..2] OF BYTE; // fill bytes
    stIndexRange     : ARRAY [1..nMaxIndexRange] OF ST_UAIndexRange;
  END_STRUCT
END_TYPE
```

- **eAttributeID**: Specifies the ID of the OPC UA attribute. `eUAAI_Value` is used by default. (Type: `E_UAAttributeID`)
- **nIndexRangeCount**: Determines how many index ranges are used in `stIndexRange`.
- **stIndexRange**: Specifies an index range for reading values from an array. (Type: `ST_UAIndexRange`)

### Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

**5.2.1.12 UAHADataValue**

This function block acts as a data object. An instance represents a value for the OPC UA Historical Access function. A whole field of these values is transferred to the UA_HistoryUpdate function block on calling.

### Declaration

```
aDataValues : ARRAY [1..50] OF UAHADataValue(ValueSize:=SIZEOF(LREAL));
```
Each data object is initialized with the expected size (in bytes) of the value.

**Properties**

**Value (PVOID):** Specifies the address of a variable containing the desired value. This is usually assigned with the help of the operator ADR(). The value itself is hereby assigned at the same time and copied into the data object.

**StatusCode (UAHAUpdateStatusCode [179]):** Indicates the status code of the value.

**SourceTimeStamp (ULINT):** Indicates the time stamp of the source in UTC format. This can be determined with the help of the function F_GetSystemTime (Tc2_System PLC library).

**ServerTimeStamp (ULINT):** Indicates the time stamp of the OPC UA Server in UTC format. This function is not currently supported.

---

**Data type size of the value**

The size of the data type used is already indicated and thus defined in the declaration of the data object. This size is taken as the basis when assigning a value later.

Values of the type STRING are accordingly also saved and transmitted with a fixed initialized size. An indication of the current text length cannot be made.

---

**Sample**

```plaintext
{attribute 'OPC.UA.DA' := '1'}

fMyValue : LREAL;       // Variable for HistorcalAccess
aDataValues : ARRAY [1..50] OF UAHADataValue(ValueSize:=SIZEOF(LREAL));

fMyValue := 27.75;
aDataValues[1].Value := ADR(fMyValue);
aDataValues[1].StatusCode := UAHAUpdateStatusCode.HistorianRaw;
aDataValues[1].SourceTimeStamp := F_GetSystemTime();
```

In this sample a field of 50 values is defined, of which each is represented by a data object. The current content of the variable fMyValue (= 27.75) is assigned to the first value.

The field can now be filled by means of further assignments in subsequent PLC cycles.

---

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1 &gt;= 4024.1</td>
<td>Win32, Win64, WinCE-x86</td>
<td>Tc3_PLCopen_OpcUa &gt;= v3.1.9.0</td>
</tr>
</tbody>
</table>

---

**5.2.1.13 UAHAUpdateStatusCode**

A status code is assigned to each data value transferred using the OPC UA Historical Access function. This is a property of the object UAHADataValue [178].

---

**Enumeration**

```plaintext
{attribute 'qualified_only')

TYPE UAHAUpdateStatusCode :
{
    HistorianRaw := 0, // A raw data value.
    HistorianCalculated := 1, // A data value which was calculated.
    HistorianInterpolated := 2, // A data value which was interpolated.
    Reserved := 3, // Undefined.
    HistorianPartial := 4, // A data value which was calculated with an incomplete interval.
    HistorianExtraData := 8, // A raw data value that hides other data at the same timestamp.
    HistorianMultiValue := 16 // Multiple values match the Aggregate criteria (i.e. multiple minimum values at different timestamps within the same interval).
}) UDINT;
END_TYPE
```
Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1 &gt;= 4024.1</td>
<td>Win32, Win64, WinCE-x86</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt;= v3.1.9.0</td>
</tr>
</tbody>
</table>

5.2.2 Function blocks

5.2.2.1 UA_Connect

This function block establishes an OPC UA Remote connection to another OPC UA Server, which is specified via ServerUrl and SessionConnectInfo. The function block returns a connection handle that can be used for other function blocks, such as UA_Read.

VAR_INPUT

<table>
<thead>
<tr>
<th>VAR_INPUT</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute</td>
<td>BOOL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServerUrl</td>
<td>STRING(MAX_STRING_LENGTH)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SessionConnectInfo</td>
<td>ST_UASessionConnectInfo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeout</td>
<td>TIME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

END_VAR

Execute: The command is triggered by a positive edge at this input.

ServerUrl: OPC UA Server URL, i.e. 'opc.tcp://172.16.3.207:4840' or 'opc.tcp://CX_0193BF:4840'.

SessionConnectInfo: Connection information (see ST_UASessionConnectInfo[176])

Timeout: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds. The value must be set to match the ST_UASessionConnectInfo.tConnectionTimeout. The following rule of thumb applies: ADS Timeout > 2 * ConnectionTimeout.

VAR_OUTPUT

<table>
<thead>
<tr>
<th>VAR_OUTPUT</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionHdl</td>
<td>DWORD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Done</td>
<td>BOOL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Busy</td>
<td>BOOL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>BOOL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ErrorID</td>
<td>DWORD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

END_VAR

ConnectionHdl: OPC UA connection handle.

Done: Switches to TRUE if the function block was executed successfully.

Busy: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

Error: Switches to TRUE if an error occurs while executing a command. The command-specific error code is included in ErrorID.

ErrorID: Contains the command-specific error code of the most recently executed command.
Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.2.2 UA_Disconnect

This function block closes an OPC UA Remote connection to another OPC UA Server. The connection is specified via its connection handle.

VAR_INPUT

<table>
<thead>
<tr>
<th>Input</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute</td>
<td>BOOL</td>
</tr>
<tr>
<td>ConnectionHdl</td>
<td>DWORD</td>
</tr>
<tr>
<td>Timeout</td>
<td>TIME</td>
</tr>
</tbody>
</table>

Execute: The command is triggered by a positive edge at this input.

ConnectionHdl: Connection handle previously output by the function block UA_Connect [180].

Timeout: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

VAR_OUTPUT

<table>
<thead>
<tr>
<th>Output</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Done</td>
<td>BOOL</td>
</tr>
<tr>
<td>Busy</td>
<td>BOOL</td>
</tr>
<tr>
<td>Error</td>
<td>BOOL</td>
</tr>
<tr>
<td>ErrorID</td>
<td>DWORD</td>
</tr>
</tbody>
</table>

Done: Switches to TRUE if the function block was executed successfully.

Busy: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

Error: Switches to TRUE if an error occurs while executing a command. The command-specific error code is contained in nErrID.

ErrorID: Contains the command-specific error code of the most recently executed command.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>
This function block collects the namespace index for a namespace URI. The namespace index is required for identifying symbols, for example, if the function blocks UA_Read [190] or UA_Write [192] are used.

**VAR_INPUT**

```
VAR_INPUT
  Execute : BOOL;
  ConnectionHdl : DWORD;
  NamespaceUri : STRING(MAX_STRING_LENGTH);
  Timeout : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR
```

- **Execute**: The command is triggered by a positive edge at this input.
- **ConnectionHdl**: Connection handle previously output by the function block UA_Connect [180].
- **NamespaceUri**: Namespace URI to be resolved. For the TwinCAT OPC UA Server, this is "urn:BeckhoffAutomation:Ua:PLC1" for the first PLC runtime.
- **Timeout**: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

**VAR_OUTPUT**

```
VAR_OUTPUT
  NamespaceIndex : UINT;
  Done : BOOL;
  Busy : BOOL;
  Error : BOOL;
  ErrorID : DWORD;
END_VAR
```

- **NamespaceIndex**: Namespace Index of the given namespace URI. This can be used in other function blocks, e.g. UA_NodeGetHandle or UA_MethodGetHandle.
- **Done**: Switches to TRUE if the function block was executed successfully.
- **Busy**: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.
- **Error**: Switches to TRUE if an error occurs while executing a command. The command-specific error code is included in ErrorID.
- **ErrorID**: Contains the command-specific error code of the most recently executed command.

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>
This function block calls a method on a remote UA Server. The method is determined by a connection and a method handle. The former can be queried by `UA_Connect`, the latter by `UA_MethodGetHandle`.

**VAR_INPUT**

```plaintext
VAR_INPUT
  Execute : BOOL;
  ConnectionHdl : DWORD;
  MethodHdl : DWORD;
  nNumberOfInputArguments : UDINT;
  pInputArgInfo : POINTER TO ST_UAMethodArgInfo;
  cbInputArgInfo : UDINT;
  pInputArgData : PVOID;
  cbInputArgData : UDINT;
  pInputWriteData : PVOID;
  cbInputWriteData : UDINT;
  nNumberOfOutputArguments : UDINT;
  pOutputArgInfo : POINTER TO ST_UAMethodArgInfo;
  cbOutputArgInfo : UDINT;
  pOutputArgInfoAndData : PVOID;
  cbOutputArgInfoAndData : UDINT;
  Timeout : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR
```

**Execute**: The command is triggered by a positive edge at this input.

**ConnectionHdl**: Connection handle previously output by the function block `UA_Connect`.

**MethodHdl**: Method handle, previously output by the function block `UA_MethodGetHandle`.

**nNumberOfInputArguments**: Number of input parameters.

**pInputArgInfo**: Points to the buffer address where input parameter information is stored in the form of an array `ST_UAMethodArgInfo`.

**cbInputArgInfo**: Size of the buffer where the input parameter information is stored.

**pInputArgData**: Points to the buffer address where input parameters (constant length) are stored.

**cbInputArgData**: Size of the input buffer where input parameters (with constant length) are stored.

**pInputWriteData**: Pointer to buffer address where input parameters (dynamic length) are stored.

**cbInputWriteData**: Size of the input buffer where input parameters (with dynamic length) are stored.

**nNumberOfOutputArguments**: Number of output parameters.
pOutputArgInfo: Points to the buffer address where output parameter information is stored as array ST_UAMethodArgInfo.

nLenData is required to determine the target memory of the individual output parameters. The other elements can be set in such a way that a type check of the returned parameters takes place or remains undefined.

cbOutputArgInfo: Size of the buffer where the input parameter information is stored.

pOutputArgInfoAndData: Points to the buffer address where the output parameters are to be saved as a BYTE array. The BYTE array contains the number of output parameters as DINT, four reserved bytes and parameter information as ARRAY OF ST_UAMethodArgInfo [177] (with the length of the output parameters), followed by pure data. Note that the data is packed as 1-byte alignment.

cbOutputArgInfoAndData: Size of the buffer in which the output parameters are to be saved as a BYTE array.

Timeout: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

VAR_OUTPUT

| cbRead_R | UDINT |
| Done      | BOOL  |
| Busy      | BOOL  |
| Error     | BOOL  |
| ErrorID   | UDINT |

cbRead_R: Counts all the bytes received.

Done: Switches to TRUE if the function block was executed successfully.

Busy: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

Error: Switches to TRUE if an error occurs while executing a command. The command-specific error code is contained in nErrID.

ErrorID: Contains the command-specific error code of the most recently executed command.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.2.5 UA_MethodGetHandle

This function block collects a handle for a UA method, which can then be used to call a method using UA_MethodCall [183].
VAR_INPUT

Execute : BOOL;
ConnectionHdl : DWORD;
ObjectNodeID : ST_UANodeID;
MethodNodeID : ST_UANodeID;
Timeout : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR

Execute: The command is triggered by a positive edge at this input.

ConnectionHdl: Connection handle previously output by the function block [UA_Connect](#).

ObjectNodeID: Object node ID of the method to be called. (Type: [ST_UANodeID](#))

MethodNodeID: Method node ID of the method to be called. Corresponds to the ID attribute in the UA namespace. (Type: [UA_Connect](#))

Timeout: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

VAR_OUTPUT

MethodHdl : DWORD;
Done : BOOL;
Busy : BOOL;
Error : BOOL;
ErrorID : UDINT;
END_VAR

MethodHdl: Returns a method handle that can be used to call a method via [UA_MethodCall](#).

Done: Switches to TRUE if the function block was executed successfully.

Busy: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

Error: Switches to TRUE if an error occurs while executing a command. The command-specific error code is contained in nErrID.

ErrorID: Contains the command-specific error code of the most recently executed command.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.2.6 UA_MethodReleaseHandle

This function block releases the specified method handle.

VAR_INPUT

| Execute : BOOL;
| ConnectionHdl : DWORD; |
MethodHdl : DWORD;
Timeout : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR

**Execute**: The command is triggered by a positive edge at this input.

**ConnectionHdl**: Connection handle previously output by the function block **UA_Connect**[180].

**MethodHdl**: Method handle previously output by the function block **UA_MethodGetHandle**[184].

**Timeout**: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

**VAR_OUTPUT**

VAR_OUTPUT
- Done : BOOL;
- Busy : BOOL;
- Error : BOOL;
- ErrorID : UDINT;
END_VAR

**Done**: Switches to TRUE if the function block was executed successfully.

**Busy**: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

**Error**: Switches to TRUE if an error occurs while executing a command. The command-specific error code is contained in nErrID.

**ErrorID**: Contains the command-specific ADS error code of the most recently executed command.

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

**5.2.2.7 UA_NodeGetHandle**

This function block retrieves a node handle for a given symbol in UA namespace. The symbol will be specified by a connection handle and its node ID.

**VAR_INPUT**

VAR_INPUT
- Execute : BOOL;
- ConnectionHdl : DWORD;
- NodeID : ST_UANodeID;
- Timeout : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR

**Execute**: The command is triggered by a positive edge at this input.

**ConnectionHdl**: Connection handle previously output by the function block **UA_Connect**[180].

**Node ID**: Unique addressing of the UA node, consisting of Identifier, IdentifierType and NamespacelIndex, which are resolved from a NamespaceName, e.g. by means of the method **UA_GetNamespacelIndex**[182].
Timeout: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

VAR OUTPUT

VAR_OUTPUT
  NodeHdl1 : DWORD;
  Done     : BOOL;
  Busy     : BOOL;
  Error    : BOOL;
  ErrorID  : DWORD;
END_VAR

NodeHdl: Node handle that can be used for other function blocks, such as UA_Read or UA_Write.

Done: Switches to TRUE if the function block was executed successfully.

Busy: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs do not accept new commands as long as Busy is TRUE. It is not the connection time that is monitored but the reception time.

Error: Switches to TRUE if an error occurs while executing a command. The command-specific error code is included in ErrorID.

ErrorID: Contains the command-specific ADS error code of the most recently executed command.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.2.8 UA_NodeGetHandleList

This function block queries node handles for nodes in the UA namespace.

VAR_INPUT

VAR_INPUT
  Execute    : BOOL;
  ConnectionHdl : DWORD;
  NodeIDCount : UINT;
  NodeIDs     : ARRAY[1..nMaxNodeIDsInList] OF ST_UANodeID;
  Timeout     : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR

Execute: The command is triggered by a positive edge at this input.

ConnectionHdl: Connection handle previously output by the function block UA_Connect.[180]

NodeIDCount: Number of nodes for which a node handle is required.

NodeIDs: Array of NodeIDs created with struct ST_UANodeID.[178]

Timeout: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.
**VAR_OUTPUT**

VAR_OUTPUT

- **NodeHdls**: Array of requested node handles.
- **NodeErrorIDs**: Array of error IDs if no node handles are available.
- **cbData_R**: Size of the data read.
- **Done**: Switches to TRUE if the function block was executed successfully.
- **Busy**: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.
- **Error**: Switches to TRUE if an error occurs while executing a command. The command-specific error code is in nErrID.
- **ErrorID**: Contains the error ID if an error occurs.

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

### 5.2.2.9 **UA_NodeReleaseHandle**

This function block releases a node handle.

**VAR_INPUT**

VAR_INPUT

- **Execute**: The command is triggered by a positive edge at this input.
- **ConnectionHdl**: Connection handle previously output by the function block **UA_Connect** [180].
- **NodeHdl**: Node handle to be released.
- **Timeout**: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.
**VAR_OUTPUT**

```plaintext
VAR_OUTPUT
  Done : BOOL;
  Busy : BOOL;
  Error : BOOL;
  ErrorID : DWORD;
END_VAR
```

**Done**: Switches to TRUE if the function block was executed successfully.

**Busy**: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

**Error**: Switches to TRUE if an error occurs while executing a command. The command-specific error code is included in ErrorID.

**ErrorID**: Contains the command-specific ADS error code of the most recently executed command.

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

### 5.2.2.10 UA_NodeReleaseHandleList

This function block releases several node handles.

**VAR_INPUT**

```plaintext
VAR_INPUT
  Execute    : BOOL;
  ConnectionHdl : DWORD;
  NodeHdlCount : UINT;
  NodeHdls    : ARRAY[1..nMaxNodeIDsInList] OF DWORD;
  Timeout     : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR
```

**Execute**: The command is triggered by a positive edge at this input.

**ConnectionHdl**: Connection handle previously output by the function block UA_Connect [180].

**NodeHdlCount**: Number of node handles.

**NodeHdls**: Array of node handles to be released.

**Timeout**: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

**VAR_OUTPUT**

```plaintext
VAR_OUTPUT
  NodeErrorIDs : ARRAY[1..nMaxNodeIDsInList] OF DWORD;
  Done         : BOOL;
  Busy         : BOOL;
  Error        : BOOL;
  ErrorID      : DWORD;
END_VAR
```
NodeErrorIDs: Array of error IDs if a node handle could not be released.

Done: Switches to TRUE if the function block was executed successfully.

Busy: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

Error: Switches to TRUE if an error occurs while executing a command. The command-specific error code is in nErrID.

ErrorID: Contains the error ID if an error occurs.

Requirements

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

5.2.2.11 UA_Read

This function block reads values from a given node and connection handle.

VAR_INPUT

<table>
<thead>
<tr>
<th>VAR_INPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute   : BOOL;</td>
</tr>
<tr>
<td>ConnectionHdl : DWORD;</td>
</tr>
<tr>
<td>NodeHdl : DWORD;</td>
</tr>
<tr>
<td>stNodeAddInfo : ST_UANodeAdditionalInfo;</td>
</tr>
<tr>
<td>pVariable : PVOID;</td>
</tr>
<tr>
<td>cbData : UDINT;</td>
</tr>
<tr>
<td>Timeout : TIME := DEFAULT_ADS_TIMEOUT;</td>
</tr>
</tbody>
</table>

Execute: The command is triggered by a positive edge at this input.

ConnectionHdl: Connection handle previously output by the function block UA_Connect [§ 180].

NodeHdl: Node handle previously output by the function block UA_NodeGetHandle [§ 186].

stNodeAddInfo: Defines additional information, such as which attribute is read from the UA namespace (default: 'Value' attribute) or which index range is to be used. Specified by STRUCT ST_UANodeAdditionalInfo [§ 178].

pVariable: Pointer to data memory, where the read data should be stored.

cbData: Determines the size of the data to be read.

Timeout: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.
**VAR_OUTPUT**

- **Done**: Switches to TRUE if the function block was executed successfully.
- **Busy**: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.
- **Error**: Switches to TRUE if an error occurs while executing a command. The command-specific error code is contained in nErrID.
- **ErrorID**: Contains the command-specific ADS error code of the most recently executed command.
- **cbData_R**: Number of bytes to be read.

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

**5.2.2.12 UA_ReadList**

This function block reads values from several given node and connection handles.

**VAR_INPUT**

- **Execute**: The command is triggered by a positive edge at this input.
- **ConnectionHdl**: Connection handle previously output by the function block `UA_Connect [180].`
- **NodeHdlCount**: Number of node handles stored in the input variable `NodeHdls`.
- **NodeHdls**: Array of node handles previously received by the function block `UA_NodeGetHandle [186]` or `UA_NodeGetHandleList [187].`
**stNodeAddInfo**: Defines additional information, such as which attribute is read from the UA namespace (default: 'Value' attribute) or which index range is to be used. Specified by STRUCT ST_UANodeAdditionalInfo [178].

**pVariable**: Pointer to data memory, where the read data should be stored.

**cbData**: Determines the size of the data to be read.

**cbDataTotal**: Total size of the data to be received.

**Timeout**: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

**VAR_OUTPUT**

```plaintext
VAR_OUTPUT
  Done : BOOL;
  Busy : BOOL;
  Error : BOOL;
  ErrorID : UDINT;
  cbData_R : UDINT;
END_VAR
```

**Done**: Switches to TRUE if the function block was executed successfully.

**Busy**: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

**Error**: Switches to TRUE if an error occurs while executing a command. The command-specific error code is in nErrID.

**ErrorID**: Contains the command-specific ADS error code of the most recently executed command.

**cbData_R**: Number of bytes read

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>

### 5.2.2.13 UA_Write

This function block writes values to a given node and connection handle.

**VAR_INPUT**

```plaintext
VAR_INPUT
  Execute : BOOL;
  ConnectionHdl : DWORD;
  NodeHdl : DWORD;
  stNodeAddInfo : ST_UANodeAdditionalInfo;
  pVariable : PVOID;
  Timeout : TIME;
END_VAR
```

This function block writes values to a given node and connection handle.
cbData : UDINT;
Timeout : TIME := DEFAULT_ADS_TIMEOUT;
END_VAR

**Execute**: The command is triggered by a positive edge at this input.

**ConnectionHdl**: Connection handle previously output by the function block UA_Connect [180].

**NodeHdl**: Node handle previously output by the function block UA_NodeGetHandle [186].

**stNodeAddInfo**: Defines additional information, e.g. which IndexRange or which attribute is to be written (by default, the 'Value' attribute is used). Specified by STRUCT ST_UANodeAdditionalInfo [178].

**pVariable**: Pointer to data to be written.

**cbData**: Sets the size of the values to be written.

**Timeout**: Time until the function is aborted. DEFAULT_ADS_TIMEOUT is a global constant, set to 5 seconds.

**VAR_OUTPUT**

<table>
<thead>
<tr>
<th>VAR_OUTPUT</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Done</td>
<td>BOOL;</td>
</tr>
<tr>
<td></td>
<td>Busy</td>
<td>BOOL;</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td>BOOL;</td>
</tr>
<tr>
<td></td>
<td>ErrorID</td>
<td>DWORD;</td>
</tr>
<tr>
<td>END_VAR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Done**: Switches to TRUE if the function block was executed successfully.

**Busy**: TRUE until the function block has executed a command, at the most for the duration of the "Timeout" at the input. The inputs accept no new command as long as Busy = TRUE. It is not the connection time that is monitored but the reception time.

**Error**: Switches to TRUE if an error occurs while executing a command. The command-specific error code is included in ErrorID.

**ErrorID**: Contains the command-specific ADS error code of the most recently executed command.

**Requirements**

<table>
<thead>
<tr>
<th>Development environment</th>
<th>Target platform</th>
<th>PLC libraries to include</th>
</tr>
</thead>
<tbody>
<tr>
<td>TwinCAT 3.1</td>
<td>Win32, Win64, CE-X86, CE-ARM</td>
<td>Tc3_PLCopen_OpcUa</td>
</tr>
<tr>
<td>TwinCAT 2.11 R3 Build 2245</td>
<td>Win32, CE-X86, CE-ARM</td>
<td>Tc2_PLCopen_OpcUa</td>
</tr>
</tbody>
</table>
6 Samples

Sample code and configurations for this product can be obtained from the corresponding repository on GitHub: https://github.com/Beckhoff/TF6100_Samples. There you have the option to clone the repository or download a ZIP file containing the sample.
Appendix

7.1 Error diagnosis

In the following sections, possible errors for all components of the OPC UA setup are shown in the form of a table. In addition, helpful troubleshooting hints are provided for the respective errors.
7.1.1 Server
<table>
<thead>
<tr>
<th>Behavior</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>An OPC UA Client does not see the PLC namespace</td>
<td>TF6100 Setup version 3.x and lower: This status indicates a missing license. Check whether you have activated a valid TF6100 license.</td>
</tr>
<tr>
<td>An OPC UA Client is assigned the StatusCode 0x810e0000 when reading nodes.</td>
<td>TF6100 Setup version 4.x: This status indicates a missing license. Check whether you have activated a valid TF6100 license.</td>
</tr>
<tr>
<td>The variables released via comments/attributes are not displayed in the OPC UA Server.</td>
<td>Check whether the symbol file has been correctly transferred to the controller (e.g., check boxes in the PLC project), verify that it exists in the boot directory and that the path to the symbol file in the configuration file of the server refers to the correct symbol file. You can also use the DeviceState Node in the respective namespace to check any error messages that may have occurred. An entry is made here if the symbol file was not found. Also check that the comments/attributes are spelled correctly.</td>
</tr>
<tr>
<td>The server does not comply with the sampling rate/publishing interval required by the OPC UA Client.</td>
<td>OPC UA Client/Server is not a real-time protocol, i.e., there is no guarantee that the server will always meet 100% of the sampling rate or publishing interval required by the client. The available sampling rates and publishing intervals can be viewed in the server configuration file and modified if required (&lt;AvailableSamplingRates&gt; and &lt;MinPublishingInterval&gt;).</td>
</tr>
<tr>
<td>An OPC UA Client cannot connect to the server although the server is displayed in the Windows Task Manager. The error message &quot;Host unreachable&quot; (or similar) appears.</td>
<td>Check whether firewall settings prevent communication with the server. The server port must be open for incoming TCP communication so that a client can connect.</td>
</tr>
<tr>
<td>An OPC UA Client sees the server's endpoints, but a connection with them fails with the error message &quot;Host unreachable&quot;.</td>
<td>Check that the name resolution in your network is working properly and that the server is accessible under its host name. Even if the OPC UA Client apparently connects to the IP address of the server (e.g., opc.tcp://192.168.0.1:4840) to access the server's endpoints, the server always returns its own host name in its endpoints. If the client connects directly to one of the endpoints, it will use the host name of the server again. If the name resolution does not work, the connection fails.</td>
</tr>
<tr>
<td>An OPC UA Client sees the endpoints of the server, but a connection to a secure endpoint fails. The error message &quot;BadSecurityChecksFailed&quot; appears.</td>
<td>Check whether the server trusts the client certificate. The required configuration steps can be found in section Certificate exchange [p. 110].</td>
</tr>
<tr>
<td>When using an SQL server to store Historical Access information, the values are not added to the SQL database.</td>
<td>Check the access data to the SQL Server and verify that the SQL Server is also accessible in the network. Also make sure that you are using a &quot;Big Windows&quot; operating system on the TwinCAT OPC UA Server, since SQL Server cannot be used for Historical Access under Windows CE (although SQL Compact is OK).</td>
</tr>
<tr>
<td>When reading variables, an OPC UA Client receives the error message &quot;BadDeviceFailure&quot;.</td>
<td>This is an indication that the associated ADS device cannot be reached, for example if no PLC program has been started. Check the connectivity with the ADS device and make sure that the appropriate runtime is active.</td>
</tr>
</tbody>
</table>
### 7.1.2 Client I/O

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>When creating a new I/O client by specifying the server URL with the host name of the server, no connection can be established subsequently via the AddNodes dialog.</td>
<td>Please check if name resolution is operational in your network. Alternatively try again via the IP address of the server.</td>
</tr>
<tr>
<td>Some configuration items from the I/O client are not present, although they should be according to the documentation.</td>
<td>In this case, the system manager description file (TMC) was probably not updated after a TF6100 update. Please execute the command &quot;Reload TMC&quot; from the context menu of the I/O client to reload the description file.</td>
</tr>
<tr>
<td>Write commands to a variable are not executed or do not arrive at the server.</td>
<td>Please check whether the &quot;Write Enable&quot; output has been enabled on the I/O client.</td>
</tr>
</tbody>
</table>

### 7.1.3 Client PLCopen

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The attempt to read or write a Structured Data Type from a server fails.</td>
<td>Structured Data Types are not supported by the PLCopen-based client. Please use the I/O client for this purpose.</td>
</tr>
</tbody>
</table>

### 7.1.4 Gateway

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The gateway cannot connect to the server.</td>
<td>One of the possible causes is that an old configuration is being used. For example, if there is a new server certificate, the gateway only notices this when the configured endpoint is deleted and reinserted under a different name. With the same endpoint or a new endpoint with the same name, the gateway would use the connection information from a cache and as a result would no longer be able to connect to the server.</td>
</tr>
</tbody>
</table>

### 7.2 Status codes

#### 7.2.1 ADS Return Codes

Grouping of error codes: 0x000 [198], ..., 0x500 [199], ..., 0x700 [200], ..., 0x1000 [202], ...

Global error codes
<table>
<thead>
<tr>
<th>Hex</th>
<th>Dec</th>
<th>HRESULT</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>0</td>
<td>0x9811 0000</td>
<td>ERR_NOERROR</td>
<td>No error.</td>
</tr>
<tr>
<td>0x1</td>
<td>1</td>
<td>0x9811 0001</td>
<td>ERR_INTERNAL</td>
<td>Internal error.</td>
</tr>
<tr>
<td>0x2</td>
<td>2</td>
<td>0x9811 0002</td>
<td>ERR_NORTIME</td>
<td>No real-time.</td>
</tr>
<tr>
<td>0x3</td>
<td>3</td>
<td>0x9811 0003</td>
<td>ERR_ALLOCCLOCKEDMEM</td>
<td>Allocation locked – memory error.</td>
</tr>
<tr>
<td>0x4</td>
<td>4</td>
<td>0x9811 0004</td>
<td>ERR_INSERTMAILBOX</td>
<td>Mailbox full – the ADS message could not be sent. Reducing the number of ADS messages per cycle will help.</td>
</tr>
<tr>
<td>0x5</td>
<td>5</td>
<td>0x9811 0005</td>
<td>ERR_WRONGRECEIVEHMSG</td>
<td>Wrong HMSG.</td>
</tr>
<tr>
<td>0x6</td>
<td>6</td>
<td>0x9811 0006</td>
<td>ERR_TARGETPORTNOTFOUND</td>
<td>Target port not found – ADS server is not started or is not reachable.</td>
</tr>
<tr>
<td>0x7</td>
<td>7</td>
<td>0x9811 0007</td>
<td>ERR_TARGETMACHINEFNOTFOUND</td>
<td>Target computer not found – AMS route was not found.</td>
</tr>
<tr>
<td>0x8</td>
<td>8</td>
<td>0x9811 0008</td>
<td>ERR_UNKNOWNCMDID</td>
<td>Unknown command ID.</td>
</tr>
<tr>
<td>0x9</td>
<td>9</td>
<td>0x9811 0009</td>
<td>ERR_BADTASKID</td>
<td>Invalid task ID.</td>
</tr>
<tr>
<td>0xA</td>
<td>10</td>
<td>0x9811 000A</td>
<td>ERR_NOIO</td>
<td>No IO.</td>
</tr>
<tr>
<td>0xB</td>
<td>11</td>
<td>0x9811 000B</td>
<td>ERR_UNKNOWNAMSCMD</td>
<td>Unknown AMS command.</td>
</tr>
<tr>
<td>0xC</td>
<td>12</td>
<td>0x9811 000C</td>
<td>ERR_WIN32ERROR</td>
<td>Win32 error.</td>
</tr>
<tr>
<td>0xD</td>
<td>13</td>
<td>0x9811 000D</td>
<td>ERR_PORTNOTCONNECTED</td>
<td>Port not connected.</td>
</tr>
<tr>
<td>0xE</td>
<td>14</td>
<td>0x9811 000E</td>
<td>ERR_INVALIDAMSLength</td>
<td>Invalid AMS length.</td>
</tr>
<tr>
<td>0xF</td>
<td>15</td>
<td>0x9811 000F</td>
<td>ERR_INVALIDAMSNETID</td>
<td>Invalid AMS Net ID.</td>
</tr>
<tr>
<td>0x10</td>
<td>16</td>
<td>0x9811 0010</td>
<td>ERR_LOWINSTLEVEL</td>
<td>Installation level is too low – TwinCAT 2 license error.</td>
</tr>
<tr>
<td>0x11</td>
<td>17</td>
<td>0x9811 0011</td>
<td>ERR_NODEBUGINTAVAILABLE</td>
<td>No debugging available.</td>
</tr>
<tr>
<td>0x12</td>
<td>18</td>
<td>0x9811 0012</td>
<td>ERR_PORTDISABLED</td>
<td>Port disabled – TwinCAT system service not started.</td>
</tr>
<tr>
<td>0x13</td>
<td>19</td>
<td>0x9811 0013</td>
<td>ERR_PORTALREADYCONNECTED</td>
<td>Port already connected.</td>
</tr>
<tr>
<td>0x14</td>
<td>20</td>
<td>0x9811 0014</td>
<td>ERR_AMSSYNC_W32ERROR</td>
<td>AMS Sync Win32 error.</td>
</tr>
<tr>
<td>0x15</td>
<td>21</td>
<td>0x9811 0015</td>
<td>ERR_AMSSYNC_TIMEOUT</td>
<td>AMS Sync Timeout.</td>
</tr>
<tr>
<td>0x16</td>
<td>22</td>
<td>0x9811 0016</td>
<td>ERR_AMSSYNC_AMSERROR</td>
<td>AMS Sync error.</td>
</tr>
<tr>
<td>0x17</td>
<td>23</td>
<td>0x9811 0017</td>
<td>ERR_AMSSYNC_NOINDEXINMAP</td>
<td>No index map for AMS Sync available.</td>
</tr>
<tr>
<td>0x18</td>
<td>24</td>
<td>0x9811 0018</td>
<td>ERR_INVALIDAMSPORT</td>
<td>Invalid AMS port.</td>
</tr>
<tr>
<td>0x19</td>
<td>25</td>
<td>0x9811 0019</td>
<td>ERR_NOMEMORY</td>
<td>No memory.</td>
</tr>
<tr>
<td>0x1A</td>
<td>26</td>
<td>0x9811 001A</td>
<td>ERR_TCPSEND</td>
<td>TCP send error.</td>
</tr>
<tr>
<td>0x1B</td>
<td>27</td>
<td>0x9811 001B</td>
<td>ERR_HOSTUNREACHABLE</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>0x1C</td>
<td>28</td>
<td>0x9811 001C</td>
<td>ERR_INVALIDAMSFRAgment</td>
<td>Invalid AMS fragment.</td>
</tr>
<tr>
<td>0x1D</td>
<td>29</td>
<td>0x9811 001D</td>
<td>ERR_TLSSEND</td>
<td>TLS send error – secure ADS connection failed.</td>
</tr>
<tr>
<td>0x1E</td>
<td>30</td>
<td>0x9811 001E</td>
<td>ERR_ACCESSDENIED</td>
<td>Access denied – secure ADS access denied.</td>
</tr>
</tbody>
</table>

## Router error codes

<table>
<thead>
<tr>
<th>Hex</th>
<th>Dec</th>
<th>HRESULT</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x500</td>
<td>1280</td>
<td>0x9811 0500</td>
<td>ROUTERERR_NOLOCKEDMEMORY</td>
<td>Locked memory cannot be allocated.</td>
</tr>
<tr>
<td>0x501</td>
<td>1281</td>
<td>0x9811 0501</td>
<td>ROUTERERR_RESIZEMEMORY</td>
<td>The router memory size could not be changed.</td>
</tr>
<tr>
<td>0x502</td>
<td>1282</td>
<td>0x9811 0502</td>
<td>ROUTERERR_MAILBOXFULL</td>
<td>The mailbox has reached the maximum number of possible messages.</td>
</tr>
<tr>
<td>0x503</td>
<td>1283</td>
<td>0x9811 0503</td>
<td>ROUTERERR_DEBUGBOXFULL</td>
<td>The Debug mailbox has reached the maximum number of possible messages.</td>
</tr>
<tr>
<td>0x504</td>
<td>1284</td>
<td>0x9811 0504</td>
<td>ROUTERERR_UNKNOWNPORTTYPE</td>
<td>The port type is unknown.</td>
</tr>
<tr>
<td>0x505</td>
<td>1285</td>
<td>0x9811 0505</td>
<td>ROUTERERR_NOTINITIALIZED</td>
<td>The router is not initialized.</td>
</tr>
<tr>
<td>0x506</td>
<td>1286</td>
<td>0x9811 0506</td>
<td>ROUTERERR_PORTALREADYINUSE</td>
<td>The port number is already assigned.</td>
</tr>
<tr>
<td>0x507</td>
<td>1287</td>
<td>0x9811 0507</td>
<td>ROUTERERR_NOTREGISTERED</td>
<td>The port is not registered.</td>
</tr>
<tr>
<td>0x508</td>
<td>1288</td>
<td>0x9811 0508</td>
<td>ROUTERERR_NOMOREQUEUES</td>
<td>The maximum number of ports has been reached.</td>
</tr>
<tr>
<td>0x509</td>
<td>1289</td>
<td>0x9811 0509</td>
<td>ROUTERERR_INVALIDPORT</td>
<td>The port is invalid.</td>
</tr>
<tr>
<td>0x50A</td>
<td>1290</td>
<td>0x9811 050A</td>
<td>ROUTERERR_NOTACTIVATED</td>
<td>The router is not active.</td>
</tr>
<tr>
<td>0x50B</td>
<td>1291</td>
<td>0x9811 050B</td>
<td>ROUTERERR_FRAGMENTBOXFULL</td>
<td>The mailbox has reached the maximum number for fragmented messages.</td>
</tr>
<tr>
<td>0x50C</td>
<td>1292</td>
<td>0x9811 050C</td>
<td>ROUTERERR_FRAGMENTTIMEOUT</td>
<td>A fragment timeout has occurred.</td>
</tr>
<tr>
<td>0x50D</td>
<td>1293</td>
<td>0x9811 050D</td>
<td>ROUTERERR_TOBEREMOVED</td>
<td>The port is removed.</td>
</tr>
</tbody>
</table>
General ADS error codes
<table>
<thead>
<tr>
<th>Hex</th>
<th>Dec</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x700</td>
<td>1792</td>
<td>0x9811 0700 ADSERR_DEVICE_ERROR</td>
<td>General device error.</td>
</tr>
<tr>
<td>0x701</td>
<td>1793</td>
<td>0x9811 0701 ADSERR_DEVICE_SRVNOTSUPP</td>
<td>Service is not supported by the server.</td>
</tr>
<tr>
<td>0x702</td>
<td>1794</td>
<td>0x9811 0702 ADSERR_DEVICE_INVALIDGRP</td>
<td>Invalid group.</td>
</tr>
<tr>
<td>0x703</td>
<td>1795</td>
<td>0x9811 0703 ADSERR_DEVICE_INVALIDOFFSET</td>
<td>Invalid offset.</td>
</tr>
<tr>
<td>0x704</td>
<td>1796</td>
<td>0x9811 0704 ADSERR_DEVICE_INVALIDACCESS</td>
<td>Reading or writing not permitted.</td>
</tr>
<tr>
<td>0x705</td>
<td>1797</td>
<td>0x9811 0705 ADSERR_DEVICE_INVALIDSIZE</td>
<td>Parameter size not correct.</td>
</tr>
<tr>
<td>0x706</td>
<td>1798</td>
<td>0x9811 0706 ADSERR_DEVICE_INVALIDDATA</td>
<td>Invalid data values.</td>
</tr>
<tr>
<td>0x707</td>
<td>1799</td>
<td>0x9811 0707 ADSERR_DEVICE_NOTREADY</td>
<td>Device is not ready to operate.</td>
</tr>
<tr>
<td>0x708</td>
<td>1800</td>
<td>0x9811 0708 ADSERR_DEVICE_BUSY</td>
<td>Device is busy.</td>
</tr>
<tr>
<td>0x709</td>
<td>1801</td>
<td>0x9811 0709 ADSERRDEVICE_INVALIDCONTEXT</td>
<td>Invalid operating context. This can result from use of ADS function blocks in different tasks. It may be possible to resolve this through multitasking synchronization in the PLC.</td>
</tr>
<tr>
<td>0x70A</td>
<td>1802</td>
<td>0x9811 070A ADSERR_DEVICE_NOMEMORY</td>
<td>Insufficient memory.</td>
</tr>
<tr>
<td>0x70B</td>
<td>1803</td>
<td>0x9811 070B ADSERR_DEVICE_INVALIDPARM</td>
<td>Invalid parameter values.</td>
</tr>
<tr>
<td>0x70C</td>
<td>1804</td>
<td>0x9811 070C ADSERR_DEVICE_NOTFOUND</td>
<td>Not found (files,...).</td>
</tr>
<tr>
<td>0x70D</td>
<td>1805</td>
<td>0x9811 070D ADSERR_DEVICE_SYNTAX</td>
<td>Syntax error in file or command.</td>
</tr>
<tr>
<td>0x70E</td>
<td>1806</td>
<td>0x9811 070E ADSERR_DEVICE_INCOMPATIBLE</td>
<td>Objects do not match.</td>
</tr>
<tr>
<td>0x70F</td>
<td>1807</td>
<td>0x9811 070F ADSERR_DEVICE_EXISTS</td>
<td>Object already exists.</td>
</tr>
<tr>
<td>0x710</td>
<td>1808</td>
<td>0x9811 0710 ADSERR_DEVICE_SYMBOLNOTFOUND</td>
<td>Symbol not found.</td>
</tr>
<tr>
<td>0x711</td>
<td>1809</td>
<td>0x9811 0711 ADSERR_DEVICE_SYMBOLVERSIONINVALID</td>
<td>Invalid symbol version. This can occur due to an online change. Create a new handle.</td>
</tr>
<tr>
<td>0x712</td>
<td>1810</td>
<td>0x9811 0712 ADSERR_DEVICE_INVALIDSTATE</td>
<td>Device (server) is in invalid state.</td>
</tr>
<tr>
<td>0x713</td>
<td>1811</td>
<td>0x9811 0713 ADSERR_DEVICE_TRANSMODENOTSUPP</td>
<td>AdsTransMode not supported.</td>
</tr>
<tr>
<td>0x714</td>
<td>1812</td>
<td>0x9811 0714 ADSERR_DEVICE_NOTIFYHWNDINVALID</td>
<td>Notification handle is invalid.</td>
</tr>
<tr>
<td>0x715</td>
<td>1813</td>
<td>0x9811 0715 ADSERR_DEVICE_CLIENTUNKNOWN</td>
<td>Notification client not registered.</td>
</tr>
<tr>
<td>0x716</td>
<td>1814</td>
<td>0x9811 0716 ADSERR_DEVICE_NOMOREHDLS</td>
<td>No further notification handle available.</td>
</tr>
<tr>
<td>0x717</td>
<td>1815</td>
<td>0x9811 0717 ADSERR_DEVICE_INVALIDWATCHSIZE</td>
<td>Notification size too large.</td>
</tr>
<tr>
<td>0x718</td>
<td>1816</td>
<td>0x9811 0718 ADSERR_DEVICE_NOTINIT</td>
<td>Device not initialized.</td>
</tr>
<tr>
<td>0x719</td>
<td>1817</td>
<td>0x9811 0719 ADSERR_DEVICE_TIMEOUT</td>
<td>Device has a timeout.</td>
</tr>
<tr>
<td>0x71A</td>
<td>1818</td>
<td>0x9811 071A ADSERR_DEVICE_NOINTERFACE</td>
<td>Interface query failed.</td>
</tr>
<tr>
<td>0x71B</td>
<td>1819</td>
<td>0x9811 071B ADSERR_DEVICE_INVALIDINTERFACE</td>
<td>Wrong interface requested.</td>
</tr>
<tr>
<td>0x71C</td>
<td>1820</td>
<td>0x9811 071C ADSERR_DEVICE_INVALIDCLSID</td>
<td>Class ID is invalid.</td>
</tr>
<tr>
<td>0x71D</td>
<td>1821</td>
<td>0x9811 071D ADSERR_DEVICE_INVALIDOBJID</td>
<td>Object ID is invalid.</td>
</tr>
<tr>
<td>0x71E</td>
<td>1822</td>
<td>0x9811 071E ADSERR_DEVICE_PEND</td>
<td>Request pending.</td>
</tr>
<tr>
<td>0x71F</td>
<td>1823</td>
<td>0x9811 071F ADSERR_DEVICE_ABORTED</td>
<td>Request is aborted.</td>
</tr>
<tr>
<td>0x720</td>
<td>1824</td>
<td>0x9811 0720 ADSERR_DEVICE_WARNING</td>
<td>Signal warning.</td>
</tr>
<tr>
<td>0x721</td>
<td>1825</td>
<td>0x9811 0721 ADSERR_DEVICE_INVALIDARRAYIDX</td>
<td>Invalid array index.</td>
</tr>
<tr>
<td>0x722</td>
<td>1826</td>
<td>0x9811 0722 ADSERR_DEVICE_SYMBOLNOTACTIVE</td>
<td>Symbol not active.</td>
</tr>
<tr>
<td>0x723</td>
<td>1827</td>
<td>0x9811 0723 ADSERR_DEVICE_ACCESSDENIED</td>
<td>Access denied.</td>
</tr>
<tr>
<td>0x724</td>
<td>1828</td>
<td>0x9811 0724 ADSERR_DEVICE_LICENSENOTFOUND</td>
<td>Missing license.</td>
</tr>
<tr>
<td>0x725</td>
<td>1829</td>
<td>0x9811 0725 ADSERR_DEVICE_LICENSEEXPIRED</td>
<td>License expired.</td>
</tr>
<tr>
<td>0x726</td>
<td>1830</td>
<td>0x9811 0726 ADSERR_DEVICE_LICENSEEXCEEDED</td>
<td>License exceeded.</td>
</tr>
<tr>
<td>0x727</td>
<td>1831</td>
<td>0x9811 0727 ADSERR_DEVICE_LICENSEINVALID</td>
<td>Invalid license.</td>
</tr>
<tr>
<td>0x728</td>
<td>1832</td>
<td>0x9811 0728 ADSERR_DEVICE_LICENSESYSTEMID</td>
<td>License problem: System ID is invalid.</td>
</tr>
<tr>
<td>0x729</td>
<td>1833</td>
<td>0x9811 0729 ADSERR_DEVICE_LICENSENOTLIMIT</td>
<td>License not limited in time.</td>
</tr>
<tr>
<td>0x72A</td>
<td>1834</td>
<td>0x9811 072A ADSERR_DEVICE_LICENSEFUTUREISSUE</td>
<td>License problem: Time in the future.</td>
</tr>
<tr>
<td>0x72B</td>
<td>1835</td>
<td>0x9811 072B ADSERR_DEVICE_LICENSEMETERLONG</td>
<td>License period too long.</td>
</tr>
<tr>
<td>0x72C</td>
<td>1836</td>
<td>0x9811 072C ADSERR_DEVICE_EXCEPTION</td>
<td>Exception at system startup.</td>
</tr>
<tr>
<td>0x72D</td>
<td>1837</td>
<td>0x9811 072D ADSERR_DEVICE_LICENSEEDUPPLICATED</td>
<td>License file read twice.</td>
</tr>
<tr>
<td>0x72E</td>
<td>1838</td>
<td>0x9811 072E ADSERR_DEVICE_SIGNATUREINVALID</td>
<td>Invalid signature.</td>
</tr>
<tr>
<td>0x72F</td>
<td>1839</td>
<td>0x9811 072F ADSERR_DEVICE_CERTIFICATEINVALID</td>
<td>Invalid certificate.</td>
</tr>
<tr>
<td>0x730</td>
<td>1840</td>
<td>0x9811 0730 ADSERR_DEVICE_LICENSEOEMNOTFOUND</td>
<td>Public key not known from OEM.</td>
</tr>
<tr>
<td>0x731</td>
<td>1841</td>
<td>0x9811 0731 ADSERR_DEVICE_LICENSERESTRICTED</td>
<td>License not valid for this system ID.</td>
</tr>
<tr>
<td>0x732</td>
<td>1842</td>
<td>0x9811 0732 ADSERR_DEVICE_LICENSEDEDEMENDED</td>
<td>Demo license prohibited.</td>
</tr>
<tr>
<td>0x733</td>
<td>1843</td>
<td>0x9811 0733 ADSERR_DEVICE_INVALIDFNCID</td>
<td>Invalid function ID.</td>
</tr>
<tr>
<td>0x734</td>
<td>1844</td>
<td>0x9811 0734 ADSERR_DEVICE_OUTOFRANGE</td>
<td>Outside the valid range.</td>
</tr>
<tr>
<td>0x735</td>
<td>1845</td>
<td>0x9811 0735 ADSERR_DEVICE_INVALIDALIGNMENT</td>
<td>Invalid alignment.</td>
</tr>
</tbody>
</table>
### Appendix

<table>
<thead>
<tr>
<th>Hex</th>
<th>Dec</th>
<th>HRESULT</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x736</td>
<td>1846</td>
<td>0x9811 0736</td>
<td>ADSERR_DEVICE_LICENSEPLATFORM</td>
<td>Invalid platform level.</td>
</tr>
<tr>
<td>0x737</td>
<td>1847</td>
<td>0x9811 0737</td>
<td>ADSERR_DEVICE_FORWARD_PL</td>
<td>Context – forward to passive level.</td>
</tr>
<tr>
<td>0x738</td>
<td>1848</td>
<td>0x9811 0738</td>
<td>ADSERR_DEVICE_FORWARD_DL</td>
<td>Context – forward to dispatch level.</td>
</tr>
<tr>
<td>0x739</td>
<td>1849</td>
<td>0x9811 0739</td>
<td>ADSERR_DEVICE_FORWARD_RT</td>
<td>Context – forward to real-time.</td>
</tr>
<tr>
<td>0x740</td>
<td>1856</td>
<td>0x9811 0740</td>
<td>ADSERR_CLIENT_ERROR</td>
<td>Client error.</td>
</tr>
<tr>
<td>0x741</td>
<td>1857</td>
<td>0x9811 0741</td>
<td>ADSERR_CLIENT_INVALIDPARAM</td>
<td>Service contains an invalid parameter.</td>
</tr>
<tr>
<td>0x742</td>
<td>1858</td>
<td>0x9811 0742</td>
<td>ADSERR_CLIENT_LISTEMPTY</td>
<td>Polling list is empty.</td>
</tr>
<tr>
<td>0x743</td>
<td>1859</td>
<td>0x9811 0743</td>
<td>ADSERR_CLIENT_VARUSED</td>
<td>Var connection already in use.</td>
</tr>
<tr>
<td>0x744</td>
<td>1860</td>
<td>0x9811 0744</td>
<td>ADSERR_CLIENT_DUPINVOKED</td>
<td>The called ID is already in use.</td>
</tr>
<tr>
<td>0x745</td>
<td>1861</td>
<td>0x9811 0745</td>
<td>ADSERR_CLIENT_SYNCTIMEOUT</td>
<td>Timeout has occurred – the remote terminal is not responding in the specified ADS timeout. The route setting of the remote terminal may be configured incorrectly.</td>
</tr>
<tr>
<td>0x746</td>
<td>1862</td>
<td>0x9811 0746</td>
<td>ADSERR_CLIENT_W32ERROR</td>
<td>Error in Win32 subsystem.</td>
</tr>
<tr>
<td>0x747</td>
<td>1863</td>
<td>0x9811 0747</td>
<td>ADSERR_CLIENT_TIMEOUTINVALID</td>
<td>Invalid client timeout value.</td>
</tr>
<tr>
<td>0x748</td>
<td>1864</td>
<td>0x9811 0748</td>
<td>ADSERR_CLIENT_PORTNOTOPEN</td>
<td>Port not open.</td>
</tr>
<tr>
<td>0x749</td>
<td>1865</td>
<td>0x9811 0749</td>
<td>ADSERR_CLIENT_NOAMSSADR</td>
<td>No AMS address.</td>
</tr>
<tr>
<td>0x750</td>
<td>1872</td>
<td>0x9811 0750</td>
<td>ADSERR_CLIENT_SYNCHINTERNAL</td>
<td>Internal error in Ads sync.</td>
</tr>
<tr>
<td>0x751</td>
<td>1873</td>
<td>0x9811 0751</td>
<td>ADSERR_CLIENT_ADDHASH</td>
<td>Hash table overflow.</td>
</tr>
<tr>
<td>0x752</td>
<td>1874</td>
<td>0x9811 0752</td>
<td>ADSERR_CLIENT_REMOVEHASH</td>
<td>Key not found in the table.</td>
</tr>
<tr>
<td>0x753</td>
<td>1875</td>
<td>0x9811 0753</td>
<td>ADSERR_CLIENT_NOMORESYM</td>
<td>No symbols in the cache.</td>
</tr>
<tr>
<td>0x754</td>
<td>1876</td>
<td>0x9811 0754</td>
<td>ADSERR_CLIENT_SYNCRESINVALID</td>
<td>Invalid response received.</td>
</tr>
<tr>
<td>0x755</td>
<td>1877</td>
<td>0x9811 0755</td>
<td>ADSERR_CLIENT_SYNCPORTLOCKED</td>
<td>Sync Port is locked.</td>
</tr>
</tbody>
</table>

### RTime error codes

<table>
<thead>
<tr>
<th>Hex</th>
<th>Dec</th>
<th>HRESULT</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1000</td>
<td>4096</td>
<td>0x9811 1000</td>
<td>RTERR_INTERNAL</td>
<td>Internal error in the real-time system.</td>
</tr>
<tr>
<td>0x1001</td>
<td>4097</td>
<td>0x9811 1001</td>
<td>RTERR_BDTIMERPERIODS</td>
<td>Timer value is not valid.</td>
</tr>
<tr>
<td>0x1002</td>
<td>4098</td>
<td>0x9811 1002</td>
<td>RTERR_INVALIDASKPTR</td>
<td>Task pointer has the invalid value 0 (zero).</td>
</tr>
<tr>
<td>0x1003</td>
<td>4099</td>
<td>0x9811 1003</td>
<td>RTERR_INVALIDSTACKPTR</td>
<td>Stack pointer has the invalid value 0 (zero).</td>
</tr>
<tr>
<td>0x1004</td>
<td>4100</td>
<td>0x9811 1004</td>
<td>RTERR_PRIEXISTS</td>
<td>The request task priority is already assigned.</td>
</tr>
<tr>
<td>0x1005</td>
<td>4101</td>
<td>0x9811 1005</td>
<td>RTERR_NOMORETCB</td>
<td>No free TCB (Task Control Block) available. The maximum number of TCBs is 64.</td>
</tr>
<tr>
<td>0x1006</td>
<td>4102</td>
<td>0x9811 1006</td>
<td>RTERR_NOMORESEMAS</td>
<td>No free semaphore available. The maximum number of semaphores is 64.</td>
</tr>
<tr>
<td>0x1007</td>
<td>4103</td>
<td>0x9811 1007</td>
<td>RTERR_NOMOREQUEUES</td>
<td>No free space available in the queue. The maximum number of positions in the queue is 64.</td>
</tr>
<tr>
<td>0x100D</td>
<td>4109</td>
<td>0x9811 100D</td>
<td>RTERR_EXTIRQALREADYDEF</td>
<td>An external synchronization interrupt is already applied.</td>
</tr>
<tr>
<td>0x100E</td>
<td>4110</td>
<td>0x9811 100E</td>
<td>RTERR_EXTIRQNOTDEF</td>
<td>No external sync interrupt applied.</td>
</tr>
<tr>
<td>0x100F</td>
<td>4111</td>
<td>0x9811 100F</td>
<td>RTERR_EXTIRQINSTALLFAILED</td>
<td>Application of the external synchronization interrupt has failed.</td>
</tr>
<tr>
<td>0x1010</td>
<td>4112</td>
<td>0x9811 1010</td>
<td>RTERR_RQLNOTLESSOREQUAL</td>
<td>Call of a service function in the wrong context</td>
</tr>
<tr>
<td>0x1017</td>
<td>4119</td>
<td>0x9811 1017</td>
<td>RTERR_VMXNOTSUPPORTED</td>
<td>Intel VT-x extension is not supported.</td>
</tr>
<tr>
<td>0x1018</td>
<td>4120</td>
<td>0x9811 1018</td>
<td>RTERR_VMXDISABLED</td>
<td>Intel VT-x extension is not enabled in the BIOS.</td>
</tr>
<tr>
<td>0x1019</td>
<td>4121</td>
<td>0x9811 1019</td>
<td>RTERR_VMXCONTROLSMISSING</td>
<td>Missing function in Intel VT-x extension.</td>
</tr>
<tr>
<td>0x101A</td>
<td>4122</td>
<td>0x9811 101A</td>
<td>RTERR_VMXENABLEFAILS</td>
<td>Activation of Intel VT-x fails.</td>
</tr>
</tbody>
</table>

### TCP Winsock error codes

<table>
<thead>
<tr>
<th>Hex</th>
<th>Dec</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x274C</td>
<td>10060</td>
<td>WSAETIMEOUT</td>
<td>A connection timeout has occurred - error while establishing the connection, because the remote terminal did not respond properly after a certain period of time, or the established connection could not be maintained because the connected host did not respond.</td>
</tr>
<tr>
<td>0x274D</td>
<td>10061</td>
<td>WSAECONNREFUSED</td>
<td>Connection refused - no connection could be established because the target computer has explicitly rejected it. This error usually results from an attempt to connect to a service that is inactive on the external host, that is, a service for which no server application is running.</td>
</tr>
<tr>
<td>0x2751</td>
<td>10065</td>
<td>WSAEHOSTUNREACH</td>
<td>No route to host - a socket operation referred to an unavailable host.</td>
</tr>
</tbody>
</table>

More Winsock error codes: Win32 error codes
7.2.2 Client I/O

The OPC UA Client modules that belong to a virtual OPC UA device offer different status variables as well as control variables. These variables are explained below.

- Reading the status codes

Please note that the status code of the state machine is listed here in hexadecimal notation. If the code is displayed as a decimal number in TwinCAT, it must be converted for interpretation.

---

Fig. 1: OPCUAClientModulesStatusCodes
<table>
<thead>
<tr>
<th>Variable</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>BIT</td>
<td>1 TRUE</td>
</tr>
<tr>
<td>ReadBusy</td>
<td>BIT</td>
<td>1 TRUE</td>
</tr>
<tr>
<td>KeepAlives</td>
<td>BIT4</td>
<td>Shows the number of KeepAlive messages counted. Only active when reading and writing using subscriptions.</td>
</tr>
<tr>
<td>StmState</td>
<td>BYTE</td>
<td>Can be read in the table above.</td>
</tr>
<tr>
<td>ResetStm</td>
<td>BIT</td>
<td>The client is reset when this bit is set to 1.</td>
</tr>
<tr>
<td>Execute</td>
<td>BIT</td>
<td>1 TRUE</td>
</tr>
</tbody>
</table>

## 7.2.3 Client PLCopen

The function blocks of the TwinCAT OPC UA Client have their own error codes, which indicate the occurrence of an error and use an ErrorID to display further information about the problem that has occurred. TwinCAT ADS error messages (ADS Return Codes [198]) with the HighWord 0x0000 and custom error messages from the client or the PLC library with the HighWord 0xE4DD can occur.
Possible TwinCAT ADS errors include the following:

<table>
<thead>
<tr>
<th>Hex</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x 0000 0705</td>
<td>DEVICE_INVALIDSIZE</td>
<td>Parameter size not correct</td>
</tr>
<tr>
<td>0x 0000 0706</td>
<td>DEVICE_INVALIDDATA</td>
<td>Invalid parameter values</td>
</tr>
<tr>
<td>0x 0000 070A</td>
<td>DEVICE_NOMEMORY</td>
<td>Not enough memory</td>
</tr>
</tbody>
</table>

This error code list shows the possible custom error values:
<table>
<thead>
<tr>
<th>Hex</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x E4DD 0001</td>
<td>UAC_E_FAIL</td>
<td>UA service call failed</td>
</tr>
<tr>
<td>0x E4DD 0100</td>
<td>UAC_E_CONNECTED</td>
<td>Server already connected</td>
</tr>
<tr>
<td>0x E4DD 0101</td>
<td>UAC_E_CONNECT</td>
<td>General error when establishing a connection</td>
</tr>
<tr>
<td>0x E4DD 0102</td>
<td>UAC_E_UASECURITY</td>
<td>UA security could not be set up</td>
</tr>
<tr>
<td>0x E4DD 0103</td>
<td>UAC_E_ITEMEXISTS</td>
<td>Element ID already exists</td>
</tr>
<tr>
<td>0x E4DD 0104</td>
<td>UAC_E_ITEMNOTFOUND</td>
<td>Element does not exist</td>
</tr>
<tr>
<td>0x E4DD 0105</td>
<td>UAC_E_ITEMTYPE</td>
<td>Invalid or unsupported item type</td>
</tr>
<tr>
<td>0x E4DD 0106</td>
<td>UAC_E_CONVERSION</td>
<td>Variable types cannot be converted</td>
</tr>
<tr>
<td>0x E4DD 0107</td>
<td>UAC_E_SUSPENDED</td>
<td>Device hangs. Please try again later...</td>
</tr>
<tr>
<td>0x E4DD 0108</td>
<td>UAC_E_TYPE_NOT_SUPPORTED</td>
<td>Conversion variable type is not supported.</td>
</tr>
<tr>
<td>0x E4DD 0109</td>
<td>UAC_E_NSNAME_NOTFOUND</td>
<td>No namespace with the specified name found.</td>
</tr>
<tr>
<td>0x E4DD 0110</td>
<td>UAC_E_CONNECT_NOTFOUND</td>
<td>Connection failed: Target host could not be found.</td>
</tr>
<tr>
<td>0x E4DD 0111</td>
<td>UAC_E_TIMEOUT</td>
<td>Timeout: i.e. target host does not respond.</td>
</tr>
<tr>
<td>0x E4DD 0112</td>
<td>UAC_E_INVALIDHDL</td>
<td>Session handle invalid</td>
</tr>
<tr>
<td>0x E4DD 0113</td>
<td>UAC_E_INVALIDNODEID</td>
<td>UA node ID unknown</td>
</tr>
<tr>
<td>0x E4DD 0114</td>
<td>UAC_E_INVALID_IDENTIFIER_TYPE</td>
<td>Identifier type of UaNodeID invalid</td>
</tr>
<tr>
<td>0x E4DD 0115</td>
<td>UAC_E_IDENTIFIER_NOTSUPP</td>
<td>Identifier type UaNodeID is not supported.</td>
</tr>
<tr>
<td>0x E4DD 0116</td>
<td>UAC_E_INVAL_NODE_HDL</td>
<td>Invalid node handle</td>
</tr>
<tr>
<td>0x E4DD 0117</td>
<td>UAC_E_UAREADFAILED</td>
<td>UA read failed for unknown reasons</td>
</tr>
<tr>
<td>0x E4DD 0118</td>
<td>UAC_E_UAWRITEFAILED</td>
<td>UA write failed for unknown reasons</td>
</tr>
<tr>
<td>0x E4DD 0119</td>
<td>UAC_E_INVAL_NODEMETHOD_HDL</td>
<td>Invalid method handle</td>
</tr>
<tr>
<td>0x E4DD 011A</td>
<td>UAC_E_CALL_FAILED</td>
<td>Call failed, cause unknown</td>
</tr>
<tr>
<td>0x E4DD 011B</td>
<td>UAC_E_CALLEDCODE_FAILED</td>
<td>Successful call, decoding return value failed</td>
</tr>
<tr>
<td>0x E4DD 011C</td>
<td>UAC_E_NOTMAPPEDTYPE</td>
<td>Unassigned data type in return value</td>
</tr>
<tr>
<td>0x E4DD 011D</td>
<td>UAC_E_CALL_FAILED_BADINTERNAL</td>
<td>Call failed with UA_BadInternal</td>
</tr>
<tr>
<td>0x E4DD 011E</td>
<td>UAC_E_METHODIDINVALID</td>
<td>Unknown MethodID (returned on call, even if provided by GetMethodHdl)</td>
</tr>
<tr>
<td>0x E4DD 011F</td>
<td>UAC_E_TOOMUCHDIM</td>
<td>Method call has returned parameters with more than 3 dimensions; not supported.</td>
</tr>
<tr>
<td>0x E4DD 0120</td>
<td>UAC_E_CALL_FAILED_INVALIDARG</td>
<td>Call failed with OpcUa_BadInvalidArgument</td>
</tr>
<tr>
<td>0x E4DD 0121</td>
<td>UAC_E_CALL_FAILED_TYPEMISMATCH</td>
<td>Call failed with UAC_E_CALL_FAILED_TYPEMISMATCH</td>
</tr>
<tr>
<td>0x E4DD 0122</td>
<td>UAC_E_CALL_FAILED_OUTOFRANGE</td>
<td>Call failed with UAC_E_CALL_FAILED_OUTOFRANGE</td>
</tr>
<tr>
<td>0x E4DD 0123</td>
<td>UAC_E_CALL_FAILED_BADSTRUCTURE</td>
<td>Call failed with OpcUa_BadStructureMissing</td>
</tr>
<tr>
<td>0x E4DD 0124</td>
<td>UAC_E_CALL_TYPEMISMATCH_OUTPARAM</td>
<td>Call successful, but type of output information provided does not match</td>
</tr>
<tr>
<td>0x E4DD 0125</td>
<td>UAC_E_INVALIDTYPEINFO</td>
<td>Node has insufficient type information</td>
</tr>
<tr>
<td>0x E4DD 0126</td>
<td>UAC_E_INVALIDATTRIBID</td>
<td>Access to invalid node attribute</td>
</tr>
<tr>
<td>0x E4DD 0128</td>
<td>UAC_E_NOTSUPPORTED</td>
<td>The command is not supported by the connected UaServer, e.g. when calling UA_HistoryUpdate.</td>
</tr>
<tr>
<td>0x E4DE 0100</td>
<td>UAC_E_INVALID_ARRAY_LENGTH</td>
<td>An invalid array length not matching DataValueCount was assigned to UA_HistoryUpdate.</td>
</tr>
<tr>
<td>0x E4DE 0101</td>
<td>UAC_E_INVALID_DATASIZE</td>
<td>A data value with an invalid data type size was assigned to UA_HistoryUpdate. All assigned DataValues must be of the same data type.</td>
</tr>
</tbody>
</table>
### Appendix

<table>
<thead>
<tr>
<th>Hex</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x E4DE 0102</td>
<td>UAC_E_SUBERROR</td>
<td>A lower-level error was output for at least one of the transferred data values. See ValueErrorIDs at UA_HistoryUpdate.</td>
</tr>
</tbody>
</table>

# 7.3 Support and Service

Beckhoff and their partners around the world offer comprehensive support and service, making available fast and competent assistance with all questions related to Beckhoff products and system solutions.

### Beckhoff’s branch offices and representatives

Please contact your Beckhoff branch office or representative for [local support and service](http://www.beckhoff.com) on Beckhoff products!

The addresses of Beckhoff’s branch offices and representatives round the world can be found on her internet pages: [http://www.beckhoff.com](http://www.beckhoff.com)

You will also find further documentation for Beckhoff components there.

### Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

<table>
<thead>
<tr>
<th>Phone</th>
<th>Fax</th>
<th>e-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>+49(0)5246/963-0</td>
<td>+49(0)5246/963-198</td>
<td><a href="mailto:info@beckhoff.com">info@beckhoff.com</a></td>
</tr>
</tbody>
</table>

### Beckhoff Support

Support offers you comprehensive technical assistance, helping you not only with the application of individual Beckhoff products, but also with other, wide-ranging services:

- support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

<table>
<thead>
<tr>
<th>Hotline</th>
<th>Fax</th>
<th>e-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>+49(0)5246/963-157</td>
<td>+49(0)5246/963-9157</td>
<td><a href="mailto:support@beckhoff.com">support@beckhoff.com</a></td>
</tr>
</tbody>
</table>

### Beckhoff Service

The Beckhoff Service Center supports you in all matters of after-sales service:

- on-site service
- repair service
- spare parts service
- hotline service

<table>
<thead>
<tr>
<th>Hotline</th>
<th>Fax</th>
<th>e-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>+49(0)5246/963-460</td>
<td>+49(0)5246/963-479</td>
<td><a href="mailto:service@beckhoff.com">service@beckhoff.com</a></td>
</tr>
</tbody>
</table>
More Information:
www.beckhoff.com/tf6100